Cogent E Services Private Limited

Asset Management Policy & Procedure

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 INTRODUCTION 5
2. POLICY STATEMENT 5
3. OBJECTIVE 6
4. SCOPE 6
5. APPLICABILITY 6
6. BREACHES OF POLICY 6
7. ENFORCEMENT 7
8. FRAMEWORK 7
A 8 ASSET MANAGEMENT 7
A 8.1 RESPONSIBILITY FOR ASSETS 7
A 8.1.1 INVENTORY OF ASSETS 7
A 8.1.2 OWNERSHIP OF ASSETS 12
A 8.1.3 ACCEPTABLE USE OF ASSETS 15
A 8.1.4 RETURN OF ASSETS 19
A 8.2 INFORMATION CLASSIFICATION 21
A 8.2.1 CLASSIFICATION OF INFORMATION 21
A 8.2.2 LABELING OF INFORMATION 29
A 8.2.3 HANDLING OF ASSETS 31
A 8.3 MEDIA HANDLING 35
A 8.3.1 MANAGEMENT OF REMOVABLE MEDIA 35
A 8.3.2 DISPOSAL OF MEDIA 37
A 8.3.3 PHYSICAL MEDIA TRANSFER 39
9. ROLES AND RESPONSIBILITIES 44
10. RELATED DOCUMENTS 44

1 Introduction

Overview

This document details The Cogent E Services Private Limited (hereafter referred to as "Cogent") Asset Management Policy & Procedure. Cogent shall identify all assets and document the importance of these assets. The Cogent asset inventory shall include all information necessary in order to recover from a disaster, including type of asset, format, location, backup information, license information, and a business value. The Cogent asset inventory shall not duplicate other inventories unnecessarily, but it shall be ensured that the content is aligned.

In addition, ownership and classification shall be agreed and documented for each of the assets in the Cogent asset inventory. Based on the importance of the asset, its business value and its security classification, levels of protection commensurate with the importance of the assets shall be identified. Cogent systems, including hardware and software, must be managed in accordance with the information asset protection objectives established throughout the life cycle from acquisition to disposal.

Cogent systems will establish and maintain Asset Register in accordance with the information asset protection objectives established in the Asset Management Policy for each system represented in the Cogent production environment.

All systems, networks, and applications used in the Cogent production environment and in virtual premises, such as hosting sites, must follow the documented change control process and procedures to ensure that only authorized updates or changes are made.

All production systems and applications developed by the Cogent or on behalf of the Cogent must adhere to the documented process of analyzing, designing, developing, testing, and enhancing information systems security to ensure the integration of appropriate security controls.

2. Policy Statement

"Policy Statement

"*Cogent is mindful to ensure all information assets which it manages and owns are accounted for, maintained and controlled through the implementation of best practice, recording mechanisms, processes and procedures. It recognizes the importance of ensuring that all its information assets are identified, recorded and protected.*

Cogent will establish an asset management policy to keep all information assets managed, organized and maintain appropriate protection of its information assets."

- Information Asset is defined as any data, or an aggregate of data, that has value to the organization. This includes all data, whether in the form of electronic media or physical records that are used by Cogent or in support of Cogent business processes, including all data maintained or accessed through systems owned or administered by or on the behalf of the Cogent.
- Information Assets include all personal, private, or financial data about employees, clients, contractors, or other organizations that must be protected in accordance with relevant legislative, regulatory, or contractual requirements.
- Customer refers to an entity that is paying for service.
- Customer Information refers to an Information Asset that is owned by a Customer.

3. Objective

The objectives of this Cogent policy is

a) To identify organizational assets and define appropriate protection responsibilities.

b) To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.

c) To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.

To fulfill the above listed objectives Cogent shall ensure that all

a) Information assets shall be clearly identified and an inventory of all important Cogent assets is drawn up, recorded and maintained in an Information Asset Register to establish professional good practice in the maintenance, protection and classification of all its assets.

b) Define information classifications based on the sensitivity, criticality, confidentiality/privacy requirements, and value of the information.

c) Provide specific instructions and requirements for labeling information assets. These instructions must address labeling requirements for printed and electronically stored information.

d) Rules for the acceptable use of information and assets associated with information processing facilities shall be identified, documented, and implemented.

Non-compliance with this policy could have a significant effect on the efficient operation of Cogent and may result in financial loss and an inability to provide necessary services to our customers.

4. Scope

The document outlines the policy and procedures to identify, classify, label and handle the Information Assets of Cogent , and to apply protection mechanisms commensurate to the level of confidentiality and sensitivity.

The policy applies to all Cogent information resources and will apply to all equipment, buildings and other assets purchased by Cogent.

5. Applicability

This policy and its associated procedures and guidelines applies to all employees, consultants, temporaries, and others not mentioned who access Cogent information assets and information processing facilities

This policy and its associated procedures and guidelines applies at all times and shall be adhered to whenever accessing Cogent information in any format, and on any device.

6. Breaches of Policy

Breaches of this policy and its associated procedures and guidelines and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to Cogent assets, or an event which is in breach of the Cogent security procedures and policies.

All Cogent employees, elected members, partner agencies, contractors and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through the Cogent ' Incident Reporting Procedure. This obligation also extends to any

external organisations contracted to support or access the Information Systems of the Cogent

Cogent will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks in place. In the case of an individual then the matter may be dealt with under the disciplinary process.

7. Enforcement

It is the responsibility of Information Security Team to ensure that the controls described in this document are implemented. IT administrators understand that appropriate asset management procedures are a critical part of Cogent overall information security strategy.

Cogent departments undergo periodic internal and external audits. These audits typically include an analysis of the processes and controls used by departments to secure and manage servers. The Internal Audit team carries out internal audits. The initiation of an internal audit is based on a risk analysis, also performed by the Information Security and Internal Audits Team. A requirement for an external audit may be recommended as a result of the internal audit, or be requested independently by a department's management. The department is responsible for remediation of any findings of non-compliance with this standard within the time frame agreed to with the auditors.

8. Framework

Policy Statement

A 8 Asset management

"The asset management policy and its associated procedures and guidelines guide Cogent how to identify organizational assets and define appropriate protection responsibilities."

Implementation Guide Lines

A 8.1 Responsibility for assets

Assets associated with information and information processing facilities should be identified and an inventory of these assets should be drawn up and maintained, Ownership of assets recorded and maintained, guidelines for acceptable use of assets defined and procedure for return of assets established within Cogent.

A 8.1.1 Inventory of assets

The first stage of asset management is to gather information for every single asset within the organization. An information asset is a definable piece of information, stored in any manner which is recognized as "valuable" to the organization.

1.1. **Asset Inventory**

1.1.1. All Cogent information assets associated with information and information processing facilities shall be identified and must be listed in an Information Asset Inventory.

1.1.2. Each Asset must be clearly identified individually and (if appropriate) collectively in combination with other Assets to form an identifiable Information Asset.

1.2. **Information Asset Category**

Cogent must take steps to ensure all assets are appropriately identified, recorded and maintained in an Information Asset Register to track all information assets within its premise. All Information Assets are grouped into seven asset categories for ease of identification and maintenance.

The categories are as follows:

#	Asset Group	Examples of Assets
1.	**Physical Hardware**	Like Computer Equipments including Computers, Servers, magnetic media, other equipment, cabinets, safes, UPS, DG, CCTV, Access Card Readers, , Communication Network devices : E.g. routers, L3, switches, firewalls, IDS, IPS, communication equipment etc.
2.	**Software**	Like application s/w, development tools, system s/w, utilities, etc. Email, Operating systems, Anti-virus, web server software, utilities, automation tools MS Office, ERP ,Financial Accounting ,Time Sheet Applications , Custom applications e.g. securities tracking system
3.	**Digital Information**	Like any records, data files, system documentation, user manuals, etc. (i.e. mainly in electronic form) Database, data files, system documentation, user manuals, training material, operational and support procedures, ISMS, business continuity policies, email data, source codes, etc
4.	**Printed Information**	Like hard copy personal files, SLA agreements, contracts, guidelines, company documents, business results, Legal documents, HR Records, Purchase documents, Invoices. etc.
5.	**Services /Facilities**	Like Internet services, house- keeping, security services, telephony services, Computing, telecommunications, Power supply, Server rooms. fire controls, CCTV, heating, ventilation and air conditioning etc.
6.	**Human Resources**	Like developers, PMs, etc. (Hierarchy-Wise) Personnel, employees, contract employees, consultants, customers, subscribers
7.	**Intangibles and Intellectual Property**	Like Brand , Reputation ,Knowledge , intellectual property

1. Physical Hardware

Cogent most visible assets are those which are physically located throughout the organization such as computers, printers and phones etc. Offices and buildings must also be considered as ICT assets – providing location for the housing and installation of the Cogent ICT Data and Communications Network infrastructure and physically stored documents and information.

- **Computer equipment** – A large number of computing devices - which includes PDAs, laptops, monitors etc., are in use across the Cogent. Computers are one of the most costly single items of equipment and must be subject to controls from procurement to disposal. Cogent must be able to track all activity and use relating to all Cogent computing devices using various means such as via the computer network and/or using logging systems such as signing in and out and

other such recording mechanisms. All computers must be allocated a unique asset tag number which is recorded against the manufacturer's serial number and model which shall never be altered or exchanged with any other computer. Each computer must have the tag number securely located and easily visible on its outer casing .Throughout its life, a computer may be subject to hardware upgrades, new software installations, configuration changes and maintenance.

- **Communications equipment** – Mobile phones, office IP phones are widely used communications devices in use across the Cogent. Other network and communications devices identified as assets include routers, switches, video conferencing equipment etc. Along with computing equipment, these devices must be allocated an asset tag number which is securely located and easily visible on the device. All communications equipment must be identified and recorded in the Information asset Register and management database
- **Media storage and recording** – Media such as CD/DVDs, Magnetic tape, flash/portable hard disks are valuable assets because they are used to save and retrieve Cogent information and data. The portable nature of this type of media requires responsible use and adherence to all Cogent policies, procedures and processes which are in place for the protection of information and data. Appropriate labeling and recording mechanisms shall be in place to ensure the safety and integrity of media - enabling tracking of essential media such as for data backups e.g. media required to carry out data/file restores must be signed in and out from a secure location. Portable media must be used in accordance with the Cogent Encryption Policy, Laptop and Mobile Device Security Procedures and Data Protection and Media Handling Procedures:
  - **Property and accommodation** – Cogent information systems are housed in its buildings and property. ICT equipment along with Data and Network Communications infrastructure equipment is housed in many buildings and property occupied by it and is therefore vital for maintaining information security. All physical computer, communications and storage media/devices must go through agreed purchasing procedures and must be recorded in the Information Asset Register

2. Software

Computer and IT systems software is widely used across the Cogent and is vital to the day to day running of the Cogent and in providing essential services to its customers. The use of software has continued to change the way the Cogent works. Substantial investment has been made in Software along with accompanying ongoing costs and expenditure such as annual software/systems support, licensing and staff training.

- **Applications** – *Software used by the Cogent must be appropriately sourced using Cogent approved supplier(s) and must be evaluated for business need, suitability, efficiency, ease of use, cost effectiveness and integration into existing Cogent systems. All software approved for use by the Cogent must be recorded on the **Approved Software List**. Appropriate numbers of software licenses must be purchased to cover volume of use and to satisfy legal requirements. Software media must be stored (physically and electronically) in a secure, centralised location **(DML – Definitive Media Library)** along with software installation codes and registration numbers. Access to Software media/DML by employees must be controlled and limited to authorised employees only. A record must be maintained of all installations of software, licensing volumes SLA documentation and references in a centralized location (database) where access is provided to authorized employees only. A signing in/out system shall be used for controlling the use of physical media.
- **System software** – Server/system software such as Operating Systems, must be evaluated for business need, suitability, efficiency, cost effectiveness and

integration into existing Cogent systems. Operating System installation media must be stored in a secure, centralized location (DML) along with installation codes. Access to Server/system software media by employees must be controlled and limited to authorised employees only. A record must be maintained of all installations of software, licensing volumes SLA documentation and references in a centralised location (database) where access is provided to authorised employees only. A signing in/out system shall be used for controlling the use of physical media. Backups of complete Server/systems installations must be routinely carried out for disaster recovery purposes. Installation, configuration and maintenance of Server/system software must only be undertaken by employees who are trained and qualified to do so

- **Development software** – such as RAD (Rapid Application Development) software for the support of existing systems and for the development of in-house solutions must follow the same processes for procurement and use as for the Applications and Server/systems software. Development software shall only be used by employees who are trained or who are undergoing training to use the Development software

All types of software (with the exception of routine security updates and patches verified by software vendors) must go through agreed purchasing procedures and must be recorded in the Cogent Approved Software list.

3. Digital Information

Data and information held and maintained by the Cogent can either be in hardcopy form stored in physical locations, filing systems, office locations or stored electronically using software and electronic backup systems.

Types of Information and Information Systems assets:

- **Databases** – Access to these must be given to authorised employees only and logs shall be maintained to record all access to and changes made to any data held within any database system
- **Data files** – Access to any data file(s) must be given to authorised employees only and logs must be maintained to record all access to and changes made to any data held within database systems
- **Policies, Procedures** – All Cogent Policies and Procedures shall be made available and disseminated internally in a digital format on its servers. All original copies of Policies and Procedures documents whether electronic or hardcopy must be safely stored, regularly reviewed and a version history control record must be maintained for each document to ensure they are up to date
- **Business Continuity plans** – All Business Continuity plans must be regularly reviewed, disseminated to appropriate employees and stored safely for easy retrieval as and when necessary

4. Printed Information

- **Hardcopy documents –** All hardcopy documents containing sensitive and personal identifiable data must be accessed, processed, maintained and securely stored in accordance with the Cogent Information Safe Haven guidance. Restricted hardcopy documents requiring controlled access must have a signing in/out record maintained wherever appropriate
- **User guides** – All user guides which assist and aid in the understanding of processes, procedures or systems shall be safely stored and shall be easily and readily accessible to all relevant employees – wherever possible. Guides which exist only in physical form shall be digitised to include an electronic version which can be stored electronically on the Cogent ICT Network and disseminated wherever possible on the Cogent intranet

- **Training material** – All relevant training material(s) must be stored and made readily accessible to all relevant employees. Duplication or physical reproduction of training manuals must be kept to a minimum and avoided wherever possible
- **Financial Data** – Data and Information relating to Cogent financial data must be restricted to authorised employees only. Recording mechanisms must be in place for logging access, changes and use of financial data and information

5 Services/Facilities

- **Communications** – It is vital for the Cogent to maintain its ability to communicate in many different forms. Communications equipment must be maintained and clear processes, policies and procedures for the provision of this service must be in place. E-mail is also a vital means of communication and as such, requires a robust, reliable infrastructure to enable the Cogent to communicate effectively and reliably, both internally and externally
- **Utilities (power. lighting, environmental controls**) – These services are assets as they provide fundamental requirements for the Cogent to function appropriately, safely and effectively. It is essential that property maintenance and inspections are routinely carried out and that employees are proactive in reporting faults, whenever noted, to the Cogent Property Services division.

6. Human Resources.

- **Personnel -** Cogent cannot function without its workforce – it is its largest asset. The provision of good public services requires Cogent employees to have the necessary skills, knowledge and ability to work within many different areas and departments across Cogent. The number of unique functions and specialism's across Cogent requires a varied knowledge and skills base which must be supported by robust recruitment processes, appropriate training provision and good management of employee skill identification, work placement and allocation
    - **Knowledge and Experience** – Cogent has a great pool of employees who have a wide knowledge and experience base to draw on and is a valuable asset.
    - **Skills** – All Cogent employees must possess the necessary skills and ability to do their jobs.

7.Intangibles

- **Reputation** – Cogent is very aware that public perception and confidence in its ability to deliver effective, efficient public services is of the utmost importance. Reputation is an asset which promotes confidence and generates support in what Cogent is trying to achieve. Cogent takes its reputation seriously and proactively engages to develop policies and procedures along with a consistent approach in maintaining and presenting the right image.

1.3. Asset Inventory

1.3.1. An inventory of all information, software and applications, hardware, services and assets shall be maintained in an Asset Register

1.3.2. Physical assets should be labelled with an asset number that identifies the asset in the asset register.

1.3.3. The respective Asset Owners shall be responsible for maintaining and updating the Asset Inventory of the assets they own.

1.3.4. Asset Inventory should be verified on a half yearly basis.

1.3.5. The Information Asset Inventory must contain the following information as a minimum:

1.3.5.1. Asset Classification

1.3.5.2. Asset Identification

1.3.5.3. Asset Description

1.3.5.4. Asset Location

1.3.5.5. Asset Owner/Custodian

1.4. **Asset Inventory Audit**

1.4.1. Asset Inventory should be verified against permissions on a monthly basis.

A 8.1.2 Ownership of assets

Policy Statement

"All information assets shall be managed at organization level. Assets maintained in the inventory shall be owned. The ownership of the information assets shall reside with the organization and individuals shall be assigned and made responsible and accountable for the information assets. Specific Individuals shall be assigned with the ownership / custodianship / operational usage and support rights of the information assets. Individuals as well as other entities having approved management responsibility for the asset lifecycle qualify to be assigned as asset owners."

Implementation Guide Lines

1. Legal Owner
The top management shall be legal owner of information asset. No individual can claim IP rights of an Information asset, unless and otherwise specifically agreed andapproved by the management in contractual agreement.

2. Delegated Ownership
The Cogent Managing Director shall have authority to represent the organization for the protection and
security of the information asset as ownership of Information assets is delegated to this organizational role. Cogent Managing Director shall approve the Information Management / Security Policy.

The Cogent Managing Director may delegate full / partial ownership along with the defined responsibilities to any officer / contractor / third party with operational rights and responsibility.

I. Asset Ownership

a. Each Information Asset must have a designated owner. The Asset Owner is the person who has either created the information himself, or is in-charge of the team producing the information.

b. Each Information Asset should also have a nominated Custodian (who may be separate from the Owner of the Information Asset).

II. Assets ownership is described by following 4 (Four) properties of an asset within Cogent :

a) **Location:** This attribute describes the physical location of the assets where the asset situated or preserved. This physical location describes one attribute of logical ownership of the asset.

b) **Department/Division:** Describes department or division name that owns the assets within an organization. This describes logical ownership level of information asset. All employees within that department/division are equally responsible for department's asset.

c) **Owner:** This attribute describes the high-level ownership of the asset. Owner is the ultimate responsible and accountable for an asset.

d) **Custodian:** This attribute describes who is directly managing the asset or who is in charge of that asset. Custodian performs all day-to-day activities to manage the asset or supplies all information related to that assets or the information that the asset produces for organization.

III. Information Asset Owner

a. The responsibilities of the Asset owner are as follows:
- Updating of information asset inventory register;
- Identifying the classification level of information asset;
- Defining and implementing appropriate safeguards to ensure the confidentiality, integrity, and availability of the information asset;
- Assessing and monitoring safeguards to ensure their compliance and report situations of non-compliance;
- Authorizing access to those who have a business need for the information, and
- Ensuring access is removed from those who no longer have a business need for the information.

b. The Information Asset Owner has the responsibility of classifying the asset on the basis of Cogent Asset classification scheme and related guidelines i.e. on the basis of the Asset's Confidentiality, Integrity and Availability. The classification of the assets should be documented. This document should be reviewed and confirmed by Cogent CISO. There should be a strict version control on all documents and each change should be saved as a new version.

c. The Owner of the Information Asset should identify/approve of the controls to be implemented to provide appropriate protection to the asset. The Owner of the Information Asset is accountable for the security of the Information Asset.

d. For all client supplied information and information generated during the projects, will be owned by the Project Manager/Project Leader for the respective project.

IV. Information Asset Custodian

a. The custodian of the Information Asset should be responsible for the protection of the Asset and for implementing the controls (as identified and approved by the Owner of the information asset) and ensuring that protection mechanisms are in place for the classified Information Assets.

V. Declassification/Downgrading

a. The Information Owners for the declassification/ downgrading of the Assets may follow the following guidelines:

i. The designated Information Owner may, at any time, declassify or downgrade information after obtaining approval from the respective Department Head/Project Manager. To achieve this, the Owner should change the classification label appearing on the original document and notify all known recipients/users.

ii. The date from which the confidential information will be declassified or downgraded should be indicated on the sensitive information of the company.

iii. The CISO may, at any time prior to scheduled declassification or downgrading, extend the period that information is to remain at a certain classification level.

iv. The CISO should review the sensitivity classifications assigned to all information, at least once in six months, to determine the need for declassification or downgrading.

VI. Execution Responsibility

a. All the Asset Owners are responsible for ensuring that they classify the Information Assets in their control and purview. The Asset Custodians are responsible for ensuring that they apply the protection mechanisms to the information as per the classification levels as defined by the Asset Owners.

b. The HEAD - IT and CISO must monitor the processes being followed by the various project teams and must conduct periodic reviews (along with the project team) to ensure compliance with the policy.

The HEAD - IT ensures that strategic planning processes are undertaken so that information requirements and supporting systems and infrastructure are aligned to legislative requirements and strategic goals. The CISO ensures that information security policies and governance practices are established to ensure the quality and integrity of the agency's information resources and supporting IT systems. They oversee the development of tools, systems and information technology infrastructure to maximise the access and use of an agency's information resources.

The HEAD - IT is responsible for:

- interpreting the business and information needs and wants of Cogent and translating them into ICT initiatives
- setting the strategic direction for information and communications technology
- and information management for Cogent
- ensuring that ICT and information management investment is aligned to the strategic goals of Cogent
- ensuring that projects and initiatives are aligned and coordinated to deliver the best value
- ensuring ICT planning is integrated into business planning
- identifying opportunities for information sharing and cross collaboration on projects and initiatives.

The Chief Information Security Officer ensures that the information resources of Cogent are managed as a corporate asset and assists in establishing the strategic direction of information management for the organization. He provides support and leadership to Other Information Asset Owners responsible for managing information resources on a day-to-day basis.

The Chief Information Security Officer shall

- provide specialist advice relating to information management practices
- contribute to the strategic direction of information management within the

- organization
- co-ordinate the development and implementation of information management
- practices including policies, standards, guidelines and procedures
- assist business units to define and understand their responsibilities in relation to information management
- assist business units to identify their information needs and requirements
- Work with Other Information Asset Owners to plan and implement systems to
- effectively manage the agency's information assets.

The Information Security Officer
The information security officer is responsible for developing and implementing information systems from any unauthorised access, use, disclosure, corruption or destruction.

The information security officer shall:

- Develop policies, procedures and standards to ensure the security, confidentiality and privacy of information that is consistent with Cogent Information security policy
- Monitor and report on any information intrusion incidents and activate strategies to prevent further incidents.
- Maintenance and upkeep of the asset as defined by the asset owner
- Work with information owners and custodians to ensure that information assets have been assigned appropriate security classifications.
- Identifying the classification level of information asset;
- Implementing any changes as per the change management procedure
- Updating of information asset inventory register;
- Backup of the information
- Defining and implementing appropriate safeguards to ensure the confidentiality, integrity, and availability of the information asset;
- Assessing and monitoring safeguards to ensure their compliance and report situations of non-compliance;
- Authorizing access to those who have a business need for the information, and
- Ensuring access is removed from those who no longer have a business need for the information.

End Users

Employees, Third Parties, Contractors authorized by the Owner / custodian to access information and use the safeguards established by the Owner / custodian. Being granted access to information does not imply or confer authority to grant other users access to that information.

The users are bound by the acceptable usage policy of the organization.

A 8.1.3 Acceptable use of assets

Policy Statement

"Cogent explicitly defines the unacceptable behavior and usage of its Information Resources and information Processing resources. Any unacceptable usage identified results in initiation of disciplinary action against the concerned user.

Employees and external party users using or having access to the Cogent assets shall be made aware of the information security requirements of the organization's assets associated with information and information processing facilities and resources. All the users including employees, business partners and third party vendors are briefed about the acceptable usage of the information resources during induction training and before being granted access.

They should be responsible for their use of any information processing resources and of any such use carried out under their responsibility.

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

For security and network maintenance purposes, authorized individual within Cogent *may monitor equipment, systems and network traffic at any time."*

Implementation Guide Lines

Overview

Information Resources are strategic assets of the Cogent and must be treated and managed as valuable resources The purpose of this policy is to establish acceptable and unacceptable use of electronic devices and network resources at Cogent in conjunction with its established culture of ethical and lawful behavior, openness, trust, and integrity.

Cogent provides its employees computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives for the purpose of assisting them in the performance of their job-related duties.
and must manage them responsibly to maintain the confidentiality, integrity, and availability of its information assets. This policy requires the users of information assets to comply with company policies and protects the company against damaging legal issues.

This Acceptable Use Policy in conjunction with the corresponding standards is established to achieve the following:

1. To establish appropriate and acceptable practices regarding the use of information resources.
2. To ensure compliance with applicable laws and other rules and regulations regarding the management of information resources.
3. To educate individuals who may use information resources with respect to their responsibilities associated with computer resource use.

Scope

All employees, contractors, consultants, temporary and other workers at, including all personnel affiliated with third parties must adhere to this policy. This policy applies to information assets owned or leased by Cogent , or to devices that connect to a Cogent network or reside at a Cogent site.

Roles & Responsibilities

Cogent management will establish a periodic reporting requirement to measure the compliance and effectiveness of this policy.

1. Cogent management is responsible for implementing the requirements of this policy, or documenting non-compliance via the method described under exception handling.
2. Cogent Managers, in cooperation with Security Management Team, are required to train employees on policy and document issues with Policy compliance.
3. All Cogent employees are required to read and acknowledge the reading of this policy.

Acceptable Use of Assets

All users who may use sensitive information (non-public) are expected to familiarize themselves with this acceptable use of assets policy and the standards and guidelines supporting it, and to consistently use it.

Cogent shall establish formal Standards and Processes to support the ongoing development and maintenance of the Acceptable Use Policy.

Any security issues discovered will be reported to the CISO or his designee for follow-up investigation

It will commit to the ongoing training and education of Cogent staff responsible for the administration and/or maintenance and/or use of Cogent Information Resources. It shall establish the need for additional education or awareness program in order to facilitate the reduction in the threat and vulnerability profiles of Cogent Assets and Information Resources.

It will establish a formal review cycle for all Acceptable Use initiatives.

Acceptable Use Requirements

i. Users must report any weaknesses in Cogent computer security to the appropriate security staff. Weaknesses in computer security include unexpected software or system behavior, which may result in unintentional disclosure of information or exposure to security threats.
ii. Users must report any incidents of possible misuse or violation of this Acceptable Use Policy through the use of documented Misuse Reporting processes associated with the Internet, Intranet, and Email use standards.
iii. Users must not attempt to access any data, documents, email correspondence, and programs contained on Cogent systems for which they do not have authorization.
iv. Systems administrators and authorized users must not divulge remote connection modem phone numbers or other access points to Cogent computer resources to anyone without proper authorization.
v. Users must not share their account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes.
vi. Users must not make unauthorized copies of copyrighted or Cogent owned software.
vii. Users must not use non-standard shareware or freeware software without the appropriate Cogent Management approval.
viii. Users must not purposely engage in activity that may harass, threaten or abuse others or intentionally access, create, store or transmit material which Cogent may deem to be offensive, indecent or obscene, or that is illegal according to local, state or federal law.

ix. Users must not engage in activity that may degrade the performance of Information Resources; deprive an authorized user access to Cogent resources; obtain extra resources beyond those allocated; or circumvent Cogent computer security measures.

x. Users must not download, install or run security programs or utilities such as password cracking programs, packet sniffers, or port scanners that reveal or exploit weaknesses in the security of a Cogent computer resource unless approved by Cogent CISO..

xi. Cogent Information Resources must not be used for personal benefit, political activity, unsolicited advertising, unauthorized fund raising, or for the solicitation of performance of any activity that is prohibited by any local, state or federal law.

xii. Access to the Internet from Cogent owned, home based, computers must adhere to all the policies. Employees must not allow family members or other non-employees to access nonpublic accessible Cogent computer systems.

xiii. Any security issues discovered will be reported to the CISO or his designee for follow-up investigation. Additional Reporting requirements can be located within the Policy Enforcement, Auditing and Reporting section of this policy.

Exceptions To This Policy

Information Security must approve exceptions to this policy in advance through the CISO. The CISO is delegated authority to grant exceptions to this policy. Division heads must first approve exception requests for consideration by the CISO.

Refer ISMS-L3-A 8.1.3: Guidelines for Acceptable Use of Assets

A 8.1.4 Return of assets

Policy Statement

USE OF COGENT IT ASSETS

"All Cogent employees and external party users should return all of the organizational assets in their possession upon termination of their employment, contract or agreement .

We would like to inform you that during the course of your employment with Cogent , it may provide you with the use of a laptop computer, a PC, or other IT Asset (hereinafter referred to as "IT Assets") for purposes of enabling you to perform your job. The IT Assets will be provided to you under the terms and conditions set forth in this document:

The IT Assets remain the property of Cogent at all times and you will be allowed to use them during your employment with Cogent , subject to the remainder of these provisions.

Any data stored on the IT Assets will be the property of Cogent. This data may be updated or deleted solely by Cogent at any time.

All of Cogent security policies will apply to your use of the IT Assets at all times. You will notify Cogent IT Help Desk immediately in the event any of the IT Assets are lost or stolen.

Cogent has the right to terminate your use of the IT Assets for any reason at any time, in its sole discretion. You will promptly return the IT Assets to Cogent if requested to do so.

Upon termination, for any reason whatsoever, you shall immediately deliver to the Company any IT Assets which may be in your possession or control. If all of the IT Assets are not returned to Cogent on or before the last date of your employment, Cogent may be entitled to withhold some or all of your final paycheck, to the maximum extent allowed by law. Your signature on this document is authorization for such withholding. To the extent Cogent is unable to withhold the full amount of the debt owed, you acknowledge that Cogent may pursue all legal remedies available to recover the amount owed by you."

Implementation Guide Lines

Actions upon Termination of Contract all Cogent equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to Cogent at termination of contract. The termination process should be formalized to include the return of all previously issued physical and electronic assets owned by or entrusted to the organization.

All Cogent data or intellectual property developed or gained during the period of employment remains the property of Cogent and must not be retained beyond termination or reused for any other purpose.

In cases where an employee or external party user purchases the organization's equipment or uses their own personal equipment, procedures should be followed to ensure that all relevant information is transferred to the organization and securely erased from the equipment.

In cases where an employee or external part y user has knowledge that is important to ongoing operations, that information should be documented and transferred to the organization.

During the notice period of termination, the organization should control unauthorized copying of relevant information (e.g. intellectual property) by terminated employees and contractors.

A 8.2 Information classification

A 8.2.1 Classification of information

Policy Statement

"All information and data assets within Cogent must be classified and labeled with appropriate level of Confidentiality, Integrity and Availability. Information asset owners must identify record, maintains and update a register of all its information assets. All information assets must be clearly labeled in order to ensure that all users are aware of the classification of information."

Information handling procedures shall be established in order to provide adequate level of security and control over information and protect from unauthorized disclosure or misuse. These procedures shall be consistent with the information classification system of Cogent. "

The classification system set forth in these Guidelines is intended to be simple and intuitive.

All Cogent information assets, whether generated internally or externally, must be categorized into one of these information classifications:

1. *Public,*
2. *Internal-All,*
3. *Internal- Limited-Circulation,*
4. *Confidential and*
5. *Top Secret.*

When information of various classifications is combined, the resulting collection of information or new information must be classified at the most restrictive level among the sources."

Implementation Guide Lines

The purpose of this Cogent policy guideline is to define the requirement for classifying, labeling and handling document in order to protect sensitive information in Cogent.

The confidentiality and sensitivity of information shall be maintained through an Information Asset classification scheme. All information assets need to be classified so as to provide optimum security for them as per their criticality to the organization. The level of security to be accorded to the information of the company depends directly on the classification level of the asset, which is associated with that information.

Information handling procedures should be established in order to provide adequate level of security and control over information and protect from unauthorized disclosure or misuse. These procedures should be consistent with the information classification system of Cogent.

A classification system will be used to define the information security protection levels required. All information assets must have appropriate classification, which must be in line with the Cogent information classification standards.
Application and information system owners are responsible for defining and periodically reviewing the classification of data held in, or services provided by, their information systems.

Individuals are responsible for ensuring that sensitive information they produce is adequately protected and marked with the appropriate classification.

All sensitive information will be classified according to the standard Cogent definitions.

The classification adopted must be labeled on the asset. Information labeling will help to ensure that user is aware about the sensitivity of the information asset and can handle the information asset in compliance to organization's standards Information classified as CONFIDENTIAL or higher (including outputs from systems handling CONFIDENTIAL or higher data) will be labeled appropriately.

All employees, especially those who may use the sensitive information, are expected to familiarize themselves with this Information Asset classification scheme, and to consistently use it in the business operations.

Policy Details

Defining Information

All organizational IT assets (information, software, physical assets, services, etc) must be accounted for and controlled in the proper manner.

An information classification system must be established to protect organizational information asset based on business needs and their associated impacts. Information must be classified and their need, priorities and degree of protection be indicated.

An owner must be nominated for all information assets. The nominated Data Owners will be responsible for:

1. Establishing the classification of information/data;
2. Maintaining appropriate security controls to safeguard information/data;

The Information Security Council must initiate measures for nominating owners for all major information assets of Cogent. All Cogent critical & confidential application and data must have designated owners.

Files created by individuals must be owned and classified by them.

The Data Owner may delegate their security responsibilities to individual officers or the security team. However, the final accountability over resource integrity and security control resides with the owner.

An Information Asset Register must be maintained for all information assets

Each information asset owner is responsible for recording his asset details in the Information Asset Register.

Asset Classification Criteria

The information can be classified into the following categories:

1. Public
2. Internal-All
3. Internal- Limited
4. Confidential
5. Top Secret

All Information Assets must be classified according to this process. All information shall be handled according to the classification levels to ensure security of the information resource.

Accessibility will enable Cogent to its focus asset protection mechanisms on those assets that are most susceptible to specific risks. Information Assets may be assigned security based on their susceptibility to risk.

Table 1

Accessibility	Descriptive meaning
Public	**Public Information** This class of information does not have any impact on the confidentiality of the Information Asset. This caters to form of information that has either come from a public source or is provided by the company / company's client to the general public. Examples include periodicals, public bulletins, published company financial statements, published press releases, etc.
Internal- All	**Internal Information -All** **(All employees within Cogent)** This class of information is either generated by Cogent or is owned by Cogent. This information shall not be shared externally or with third parties. There can be exception in certain cases, where information has access rights to certain specific person. This form of information must be used within Cogent and not shared externally or with third parties. Examples include staff memos, company newsletters, staff awareness program documentation or bulletins, Service Contracts, Backup Tapes/CDs, etc.
Internal-Limited	**Internal Information – Limited** **(Limited employees within Cogent)** This class of information is either generated by Cogent or is owned by Cogent. This information shall not be shared externally or with third parties. There can be exception in certain cases, where information has access rights to certain specific person. This form of information must be used within Cogent and not shared externally or with third parties. Examples include staff memos, company newsletters, staff awareness program documentation or bulletins, Service Contracts, Backup Tapes/CDs, etc.
Confidential	**Confidential Information** Confidential information is a sensitive form of information. This information is

Accessibility	Descriptive meaning
	distributed on a "Need to Know" basis only. Examples include employee personal information, business plans, unpublished financial statements, Firewall and Router Configurations, etc.
Top Secret	**Top Secret Information** Highly confidential information is the most sensitive form of information. It is so sensitive that disclosure or usage would have a definitive impact on 's business that may lead to significant financial damage or significant loss of good reputation for. Extremely restrictive controls need to be applied (e.g., very limited audience and those who are authorized to have such form of information). Examples include strategic plans, investment decisions etc.

Table 2 Information Security Control Matrix

Security		Information Classification			
Service	**Public**	**Internal- All**	**Internal-Limited**	**Confidential**	**Top Secret**
Identification and Authentication	None	User IDs and Passwords	User IDs and Passwords	Strong Authentication (like encrypted username/ password, token, certificate	Strong Authentication (like encrypted username/ password, token, certificate
Authorization and Access Control	Access Control for Modification	Authorization by business department affiliation or function, access control at information category or directory level	Authorization by business department affiliation or function, access control at information category or directory level	Fine-grained access control - by user/role, by document or special purpose directories	Access control and authorization at the field level
Auditing	System-level for modification , events, alarms	System-level for user access, access denials, alarms	System-level for user access, access denials, alarms	System-level for user access, file changes, access denials, alarms	All events, alarms
Physical Control of Media (paper, removable disks, writable CD-ROM, etc.)	None	Labels and Marking, document destruction, secure storage	Labels and Marking, document destruction, secure storage	Encryption (If feasible) Labels and Marking, document destruction, secure storage	Encryption (If feasible) Labels and marking, document destruction, access lists, secure storage, audit program

Security		Information Classification			
Service	**Public**	**Internal- All**	**Internal-Limited**	**Confidential**	**Top Secret**
Security Operations	System configuration-level audit, investigation of security events	System configuration-level audit, compliance audit, investigation of security events	System configuration-level audit, compliance audit, investigation of security events	Frequent system configuration-level audit, compliance audit, investigation of security events	Frequent system configuration-level audit, compliance audit, investigation of security events

Table 3 Information Transmission Control Matrix

Information Medium	Public	Internal-All	Internal-Limited	Confidential	Top Secret
Local area Networks/Wide Area Networks	Use access controls to limit scope across the network	Use access controls to limit scope across the network	Use access controls to limit scope across the network	Don't expose any confidential information in the network. Segregate with in laptops. Encryption (If feasible)	Don't expose any information in the network. Segregate with in laptops. Encryption
Fax	No special requirements	Attend Fax	Attend Fax	Attend Fax Do not use programmed numbers Verify destination number Fax to and from a physically secure location	Use messenger Minimize faxing
Printer	No special requirements	Print to a physically secure printer	Print to a physically secure printer Verify destination printer	Print to a physically secure printer Verify destination printer	Print to an attended and physically secure printer Verify destination printer
Video/Voice Conference Call	No special requirements	Owner approves roster of attendees	Owner approves roster of attendees	Owner approves roster of attendees	Owner approves roster of attendees Ensure that meeting can not be over heard

Information Medium	Public	Internal-All	Internal-Limited	Confidential	Top Secret
					Ensure confidential material not in view of camera
Modem/ISDN	Password	Password Owner defines access requirements	Password Owner defines access requirements	Strong authentication	Stronger authentication
Database	Use Access Controls to limit unauthorized use	Password protection is suggested	Password protection is suggested	Data shall be encrypted when not in use	Data shall be encrypted when not in use
E-mail	No special requirements	Should not be sent to anyone outside Cogent Domain	Should not be sent to anyone outside Cogent Domain	Should not be sent to anyone outside Cogent Domain Encryption (If feasible)	Mark as "Highly Restricted do not copy" Encryption (If feasible)
Paper	No special requirements	External mail Internal mail Mark "Open by Addressee Only"	External mail Internal mail Mark "Open by Addressee Only"	Certified external mail Internal mail Mark "Open by Addressee Only"	Registered external mail Double-envelopes Use messenger service Hand deliver internally Mark "Open by Addressee Only"

Storing and Handling Classified Information

- Appropriate security classification must be clearly mentioned for all information assets of Cogent. Based on the classification, the data owners will define the recipient list and handling procedures for the Information asset.
- All information must be processed and stored strictly according to the classification assigned to that information. Information processing and handling controls must be commensurate with the sensitivity of the information.
- Handling Requirements, as defined in the procedure document, depending on the classified level must be adhered to.

Disclosure of Information

Any information including data or applications held on shared equipment or stored on removable media (e.g., tapes, cartridges, diskettes, CD-ROM's, etc.) must not be disclosed to unauthorized people, business associates or third parties, without obtaining specific approvals from the owner of the data.

Security of media in transit

- Controls should be in place to protect information during physical transport. Reliable courier and delivery channels must be used.
- Confidentiality and Insurance agreements must be signed with all these companies.
- It must be ensured that packaging for information is sufficient to protect contents from physical damage or tampering.

For sensitive information, special controls should be used including, but not limited to:

- Tamper resistant packaging
- Delivery by hand

Isolating Top Secret Information

All information in **Top Secret** category must be isolated and handled in strict compliance to the Information security procedures.

Table 4 Appropriate Protective Measures (Technical and Non-Technical)

These classification "labels" can then be used as the basis for evaluating the appropriate protective measures (technical and non-technical) needed to ensure the risk to these assets is minimized.

Required Processing			**Five level Classification**			
Processing	**Security Measures**	**Restricted**	**Confidential**	**Internal All**	**Internal Limited**	**Public**
Media Storage	Encryption or tangible access controls	Y			Y	
	Encryption (optional)		Y			
	Encryption not recommended			Y		Y
Copying	Obtaining the owner's consent is recommended	Y	Y		Y	
	No restriction			Y		Y
Faxing	Password-protected reception devices or addressee present for reception	Y	Y		Y	
	No restrictions			Y		Y
Transmission over public networks	Encryption	Y				
	Encryption (optional)		Y		Y	
	Encryption not recommended			Y		Y
Destruction	Shredding or disposal in a place secured for this purpose	Y	Y		Y	
	Wastebasket			Y		Y
Disclosure to	Owner's consent and nondisclosure	Y			Y	

Required Processing			Five level Classification			
Processing	**Security Measures**	**Restricted**	**Confidential**	**Internal All**	**Internal Limited**	**Public**
third parties	agreement					
	Nondisclosure agreement		Y	Y		
	No restrictions				Y	Y
Labelling electronic media when necessary	Internal and external labelling	Y	Y	Y		
	Disclosure date and classification	Y	Y			
	No labelling required				Y	
Document labelling when required	On each page (if not bound) and on the front and back covers and title pages of bound documents.	Y	Y	Y	Y	
	Disclosure date and classification	Y	Y	Y		
	No labelling required					Y
Packing internal and external mail	Addressed to a specific recipient and placed inside two envelopes, with the classification label on the inner envelope only.	Y	Y		Y	
	A single envelope without any specific type of labelling			Y		
Granting access rights	Asset owner only	Y	Y		Y	
	Local manager		Y	Y		
	No restrictions					Y
Audit trail	Addressee, number of copies made, location, address, destruction, witnesses.	Y	Y		Y	
	Only required if private			Y		
	Not recommended					Y

A 8.2.2 Labeling of information

Policy Statement

Information labeling

- *Information classified as CONFIDENTIAL or higher (including outputs from systems handling CONFIDENTIAL or higher data) will be labeled appropriately.*
- *Every information asset will be appropriately labeled according to the standard defined above. These labels shall be used as the basis for mandatory access control decisions.*
- *For most classifications a physical label is the most appropriate. However, in some cases, e.g. electronic transmissions, including e-mail, labels will be appended to the transmission.*
- *Output from information systems, such as printing, that contains information classified to CONFIDENTIAL or higher will carry an appropriate classification label in the output. This label will reflect the classification of the most sensitive data in the output. This includes printed reports, screen displays, magnetic media (e.g. tapes, disks, and cassettes), electronic messages and file.*

- *It is the responsibility of the respective data owners to appropriately classify their data.*
- *The data classification process must be completed for existing data and must be undertaken for any new application development project at the time of designing the new application or generation of data.*

Information labeling standards

- *All information assets must be labeled accordingly; from the time it is created until the time it is destroyed or re-labeled. Such markings must appear on all manifestations of the information (hard copies, floppy disks, Tapes, CD-ROMs, etc).*

Table 5 Information Labeling and Storage Control Matrix

Information Medium	Public	Internal - All	Internal-Limited	Confidential	Top Secret
Servers	No special requirements	Strong Password Locked in physically secure computer room	Strong Password Strong Authentication Restricted user access list Audit trail enabled	Strong Authentication Restricted user access list Audit trail enabled Locked in physically secure computer room	Stronger Authentication Restricted user access list Audit trail enabled Locked in physically secure computer room
Desktops	No special requirements	Strong Password	Strong Password Strong Authentication	Strong Authentication	Stronger Authentication Store on mainframe/servers or removable media
Laptops	No special requirements	Strong Password	Strong Password	Strong Authentication	Stronger Authentication

Information Medium	Public	Internal - All	Internal-Limited	Confidential	Top Secret
		Lock laptops in cabinet when not in use	Strong Authentication	Minimize use Lock laptops in cabinet when not in use	Minimize use Lock laptops in cabinet when not in use
Removable Media (e.g. diskettes)	No special requirements	No special requirements	Lock media in cabinet when not in use	Lock media in cabinet when not in use	Lock media in cabinet when not in use
Hardcopy (Paper, film/videos, etc.)	No special requirements	All pages labeled "Internal Use Only" Printed reports shall be locked in cabinets when not in use	All pages labeled "Internal –for Limited Users Only" Printed reports shall be locked in cabinets when not in use	All pages labeled "Confidential" Confirmation of receipt required Printed reports shall be locked in cabinets when not in use	All pages labeled "Highly Restricted Copy #, Page #" Borrower shall fill out distribution log No Copying Allowed Printed reports shall be locked in cabinets when not in use

- All information must be processed and stored strictly according to the classification assigned to that information. Information processing and handling controls must be commensurate with the sensitivity of the information.
- Handling Requirements, as defined in the procedure document, depending on the classified level must be adhered to.
- Any information including data or applications held on shared equipment or stored on removable media (e.g., tapes, cartridges, diskettes, CD-ROM's, etc.) must not be disclosed to unauthorized people, business associates or third parties, without obtaining specific approvals from the owner of the data.

Implementation Guide Lines

A 8.2.3 Handling of assets

IT assets shall not be confused with nor tracked with other organizational assets such as furniture. One of the main reasons to track IT assets other than for property control and tracking is for computer security reasons. A special IT asset handling and tracking policy will enable the organization to take measures to protect data and networking resources.

This policy will define what must be done when a piece of property is moved from one building to another or one location to another. This policy will provide for an asset tracking database to be updated so the location of all computer equipment is known. This policy will help network administrators protect the network since they will know what user and computer is at what station in the case of a worm infecting the network. This policy also covers the possibility that data on a computer being moved between secure facilities may be sensitive and must be encrypted during the move.

Policy Statement

"All Cogent employees and personnel that have access to organizational computer systems must adhere to the IT asset control policy defined below in order to protect the security of the network, protect data integrity, and protect and control computer systems and organizational assets. The asset control policy will not only enable organizational assets to be tracked concerning their location and who is using them but it will also protect any data being stored on those assets. This asset policy also covers disposal of assets. "

This policy is designed to protect the organizational resources on the network by establishing a policy and procedure for asset control. These policies will help prevent the loss of data or organizational assets and will reduce risk of losing data due to poor planning.

The Chief Information Security Officer is ultimately responsible for the development, implementation and enforcement of this policy.

Implementation Guide Lines

Assets Tracked
This section defines what IT assets shall be tracked and to what extent they shall be tracked.

IT Asset Types
This section categorized the types of assets subject to tracking.

1. Desktop workstations
2. Laptop mobile computers
3. Mobile phones and tablets
4. Printers, Copiers, FAX machines, multifunction machines
5. Handheld devices
6. Scanners
7. Servers
8. Firewalls
9. Routers
10. Switches
11. Memory devices

Assets Tracked
Assets which cost less than Rs100 shall not be tracked specifically including computer

components such as video cards or sound cards. However, assets which store data regardless of cost shall be tracked. These assets include:

1. Hard Drives
2. Temporary storage drives
3. Tapes with data stored on them including system backup data.
4. Although not specifically tracked, other storage devices including CD ROM disks and floppy disks are covered by this policy for disposal and secure storage purposes.

Small Memory Devices

Small memory storage assets will not be tracked by location but by asset owner . These assets include:

1. Floppy disks
2. CD ROM disks
3. Memory sticks

If these types of devices are permitted for some employees, the asset owner of the device must sign for receipt of these devices in their possession. All employees must also agree to handle memory sticks, floppy disks, and CD ROM disks in a responsible manner and follow these guidelines:

1. Never place sensitive data on them without authorization. If sensitive data is placed on them, special permission must be obtained and the memory device must be kept in a secure area.
2. Never use these devices to bring executable programs from outside the network without authorization and without first scanning the program with an approved and updated anti-virus and malware scanner. Any program brought into the network shall be on the IT department list of approved programs.

The Memory Device Asset owner agreement allows employees to sign for receipt of these devices and agree to handle these devices in accordance with the terms of this policy. This form must be submitted by all employees that will work with any organizational data when the employee begins working for the organization. It will also be submitted when employee receives one or more memory sticks, temporary storage drives, or data backup drives.

Asset Tracking Requirements

1. All assets must have an ID number. Either an internal tracking number will be assigned when the asset is acquired or the use of Manufacturer ID numbers must be specified in this policy.
2. An asset tracking database shall be created to track assets. It will include all information on the Asset Transfer Checklist table and the date of the asset change.
3. When an asset is acquired, an ID will be assigned for the asset and its information shall be entered in the asset tracking database.

Transfer Procedure:

1. **Asset Transfer Checklist** - When an asset type listed on the Asset Types list is transferred to a new location or asset owner, the IT Asset Transfer Checklist must be filled out by the asset owner of the item and approved by an authorized representative of the organization. The asset owner is the person whose care the item is in. If the item is a workstation, then the asset owner is the most common user of the workstation. For other equipment, the asset owner is the primary person responsible for maintenance or supervision of the equipment.

   The asset owner must fill out the Asset Transfer Checklist form and indicate whether the asset is a new asset, moving to a new location, being transferred to a new asset owner, or being disposed of.

The following information must be filled in:

1. Asset Type
2. ID number
3. Asset Name
4. Current Location
5. Designated Asset owner
6. New Location
7. New Asset owner
8. Locations of Sensitive Data

Once the asset owner fills out and signs the Asset Transfer Checklist form an authorized representative must sign it.

2. **Data entry** - After the Asset Transfer Checklist is completed, it will be given to the asset tracking database manager. The asset tracking database manager will ensure that the information from the forms is entered into the asset tracking database within one week.

3. **Checking the database** - Managers who manage projects that affected equipment location shall check periodically to see if the assets that recently were moved were added to the database. The database shall provide a recent move list which can be easily checked. Managers shall check the database weekly to be sure assets moved within the last 2 or 3 weeks are included in the database.

Asset Transfers

This policy applies to any asset transfers including the following:

1. Asset purchase
2. Asset relocation
3. Change of asset asset owner including when an employee leaves or is replaced.
4. Asset disposal, including:
   - Asset returned to manufacturer or reseller due to warranty return
   - Leased asset returned to Lessor

In all these cases the asset transfer checklist must be completed.

Media Sanitization

When transferring assets to another asset owner , any confidential information on the device must be protected and/or destroyed. The method of data destruction is dependent on the sensitivity of the data on the device and the next user of the device (within the organization and its controls or outside the organization).

Asset Disposal

Asset disposal is a special case since the asset must have any sensitive data removed during or prior to disposal. The manager of the user of the asset must determine what the level of maximum sensitivity of data stored on the device is. Below is listed the action for the device based on data sensitivity according to the data assessment process.

1. None (Unclassified) - No requirement to erase data but in the interest of prudence normally erase the data using any means such as sanitization, physical destruction or degaussing.
2. Low (Sensitive) - Erase the data using any means such as electronic sanitization, physical destruction or degaussing.
3. Medium (Confidential) - The data must be erased using an approved technology to make sure it is not readable using special hi technology techniques.
4. High (Secret) - The data must be erased using an approved technology to make sure it is not readable using special hi technology techniques. Approved

technologies are to specified in a Media Data Removal Procedure document by asset type including:

1. Floppy disk
2. Memory stick
3. CD ROM disk
4. Storage tape
5. Hard drive.
6. RAM memory
7. ROM memory or ROM memory devices.

Media Use

This policy defines the types of data that may be stored on removable media and whether that media may be removed from a physically secure facility and under what conditions it would be permitted. Removable media includes:

1. Floppy disk
2. Memory stick
3. CD ROM disk
4. Storage tape

Below is listed the policy for the device based on the rated data sensitivity of data stored on the device according to the data assessment process.

1. Unclassified - Data may be removed with approval of the first level manager and the permission is perpetual for the employee duration of employment unless revoked. The device may be sent to other offices using any public or private mail carrier.
2. Sensitive - Data may only be removed from secure areas with the permission of a director level or higher level of management and approvals are good for one time only.
3. Confidential - The data may only be removed from secure areas with permission of a Vice -president or higher level of management. There must be some security precautions documented for both the transport method and at the destination.
4. Secret - - The data may only be removed from secure areas with the permission of the President or higher level of management. There must be some security precautions documented for both the transport method and at the destination.
5. Top secret - The data may never be removed from secure areas.

Enforcement

Since data security and integrity along with resource protection is critical to the operation of the organization, employees that do not adhere to this policy may be subject to disciplinary action up to and including dismissal. Any employee aware of any violation of this policy is required to report it to their supervisor or other authorized representative.

Employee Training and Acknowledgment of policy

Each employee in the organization is expected to be aware of current policies and procedures related to IT Security and shall be trained on these policies and procedures on at least an annual basis. Employees are required to sign an acknowledgment that they are aware of the policy and will meet its requirements.

A 8.3 Media Handling

A 8.3.1 Management of removable media

Policy Statement

Removable Media Policy

The purpose of this policy is to minimise the loss, unauthorised disclosure, modification or removal of sensitive information maintained by Cogent. This policy refers to all types of computer storage which are not physically fixed inside a computer and includes the following:

- Memory cards (like those used in cameras), USB pen drives etc;
- Removable or external hard disk drives;
- Newer Solid State (SSD) drives
- Mobile devices (iPod, iPhone, iPad, MP3 player);
- Optical disks i.e. DVD and CD;
- Floppy disks;
- Backup Tapes.

Classification of Data

For the purposes of this policy, data is to be classified into different categories :

Non-sensitive Data: Data whose inappropriate use would not adversely affect an individual, for example:

- Class lists (course and learner names only)
- Management information reports which do not identify individuals
- Any data which has been made a matter of public record

Sensitive Data: Sensitive data includes:

- Any data identified by the Data Protection Act (1988) as personal sensitive data, specifically data relating to radical or ethnic origin, political opinions, religious beliefs, membership of trade union organisations, physical or mental health, sexual list, offences or alleged offences.
- Data that if lost or stolen would be likely to cause damage or distress to one or more individuals. This includes, but is not limited to, human resources data and exam or assessment results, which are not a matter of public record.
- Any data, which may reasonably be expected to be considered sensitive, personal confidential or commercially confidential. For example, data or materials pertaining to existing or planned courses, which may be of interest to a competing organisation.

Highly Sensitive Data:

- Data, which if used inappropriately may have a significant impact upon Cogent or an individual. In particular employee or student banking details or any other data that it is believed could be used for illegal purposes.

Implementation Guide Lines

- The use of removable media is not prohibited within Cogent ; it is infact an essential part of everyday business.

- The use of removable media to transport non-sensitive data can be done on standard devices (see above list for details).

- Regularly updated Anti Virus software shall be present on all machines from which the data is taken from and machines on which the data is to be loaded.

- When removable media is used to transport sensitive data, the data on the device must be encrypted to a recommended encryption standard (AES-256).

- Mobile devices and/or removable storage containing sensitive or highly sensitive data shall not be sent off site without prior agreement. IT Services shall be consulted to ensure the level of security is appropriate for the type of data being transferred. For example, database 'dumps'.

- If highly sensitive data is required to be transported via removable media please seek advice from IT Services.

- Removable media used to store sensitive and highly sensitive data shall only be used by staff who have an identified and business need for
- them.

- Any sensitive or highly sensitive data transferred to a removable media device must remain encrypted and must not be transferred to any external system in an unencrypted form.

- Data stored on removable media is the responsibility of the individual who operates the devices.

- The user must note and accept that shall their encryption password be forgotten, the removable device allows for a new password to
- be created, but this will involve a reformatting of the device and thus a total loss of the data. The removable device must therefore not be used to keep data that is not backed-up security in a central location.

- Removable media shall be physically protected against loss, damage, abuse or misuse when in use, storage and transit.

- Mobile devices and/or removable media that have become damaged shall be handed back to local IT Support or IT Services to ensure it is disposed of securely to avoid data leakage.

- If a member of staff who used a mobile device and removable media was to leave, they shall return the devices to local IT Support or IT Services for secure destruction and/or redistribution.

- The use of removable media by sub-contractors and temporary worker on Cogent owned machines shall be risk assessed and authorised.

- When the business purpose has been satisfied the contents of the removable media shall be removed from the media through a destruction method that

makes recovery of the data impossible. Alternatively the removable media and its data shall be destroyed and disposed of beyond its potential reuse.

A 8.3.2 Disposal of media

Overview

Technology equipment often contains parts which cannot simply be thrown away. Proper disposal of equipment is both environmentally responsible and often required by law. In addition, hard drives, USB drives, CD-ROMs and other storage media contain various kinds of Cogent data, some of which is considered sensitive. In order to protect our constituent's data, all storage mediums must be properly erased before being disposed of. However, simply deleting or even formatting data is not considered sufficient. When deleting files or formatting a device, data is marked for deletion, but is still accessible until being overwritten by a new file. Therefore, special tools must be used to securely erase data prior to equipment disposal.

Policy Statement

Technology Equipment Disposal

"When Technology assets have reached the end of their useful life they shall be sent to Cogent Information Security office for proper disposal.

Cogent systems Information Security will securely erase all storage mediums in accordance with current industry best practices.

All data including, all files and licensed software shall be removed from equipment using disk sanitizing software that cleans the media overwriting each and every disk sector of the machine with zero-filled blocks, meeting Department of Defense standards.

No computer or technology equipment may be sold to any individual other than through the processes identified in this policy

No computer equipment shall be disposed of via skips, dumps, landfill etc. Electronic recycling bins may be periodically placed in locations around Cogent. These can be used to dispose of equipment. Cogent systemsInformation Security will properly remove all data prior to final disposal.

All electronic drives must be degaussed or overwritten with a commercially available disk cleaning program. Hard drives may also be removed and rendered unreadable (drilling, crushing or other demolition methods)."

Cogent defines the guidelines for the disposal of technology equipment and components owned by Cogent systems in of this policy which applies to any computer/technology equipment or peripheral devices that are no longer needed within Cogent including, but not limited to the following: personal computers, servers, hard drives, laptops, mainframes, smart phones, or handheld computers (i.e., Windows Mobile, iOS or Android-based devices), peripherals (i.e., keyboards, mice, speakers), printers, scanners, typewriters, compact and floppy discs, portable storage devices (i.e., USB drives), backup tapes, printed materials.

All Cogent employees and affiliates must comply with this policy.

Implementation Guide Lines

Procedure

- Hard disks must be cleared of all software and all Cogent confidential and restricted information prior to disposal or re-use.
- The Information Security Manager is responsible for the secure disposal of storage media and the disposal of all information processing equipment is routed through his office. A log is retained showing what media were destroyed, disposed of, and when. The asset inventory is adjusted once the asset has been disposed of.
- Hard disks are cleaned using Wipe Disk software and Cogent approved agency dispatch services.
- Devices containing confidential information are (dependent on a risk assessment) destroyed prior to disposal and are never re-used.
- Devices containing confidential information that are damaged are subject to a risk assessment prior to sending for repair, to establish whether they shall be repaired or replaced.
- Portable or removable storage media of any description are destroyed prior to disposal.
- Documents containing confidential and restricted information which are to be destroyed are shredded by their owners, using a shredder with an appropriate security classification. These shredders are located in the access controlled area.
- Soft copies of documents shredded shall also be destroyed taking into consideration the relevant document retention requirements. The log of the same to be maintained.

Item	Disposal Method
Paper / Documents	Shredding
Hard Disks	Destroy
CD / DVD/ Flash Drives / USB Drives	Physical destruction
Floppies	Physical destruction
Tape Cartridges	Physical destruction

Computer Equipment refers to desktop, laptop, tablet or net book computers, printers, copiers, monitors, servers, handheld devices, telephones, cell phones, disc drives or any storage device, network switches, routers, wireless access points, batteries, backup tapes, etc.

Cogent Information Security team will place a sticker on the equipment case indicating the disk wipe has been performed. The sticker will include the date and the initials of the technician who performed the disk wipe.

Technology equipment with non-functioning memory or storage technology will have the memory or storage device removed and it will be physically destroyed.

Employee Purchase of Disposed Equipment

Equipment which is working, but reached the end of its useful life to Cogent , will be made available for purchase by employees.

A lottery system will be used to determine who has the opportunity to purchase available equipment.

All equipment purchases must go through the lottery process. Employees cannot purchase their office computer directly or "reserve" a system. This ensures that all employees have an equal chance of obtaining equipment.

Finance and Information Technology will determine an appropriate cost for each item.

All purchases are final. No warranty or support will be provided with any equipment sold.

Any equipment not in working order or remaining from the lottery process will be donated or disposed of according to current environmental guidelines. Information

Technology has contracted with several organizations to donate or properly dispose of outdated technology assets.

Prior to leaving Cogent premises, all equipment must be removed from the Information Technology inventory system.

Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

A 8.3.3 Physical media transfer

Policy Statement

Device and Media Handling, Storage, and Transport

"Cogent Media containing information should be protected against unauthorized access, misuse or corruption during transportation. It shall establish minimum standards for the secure handling, transport and storage of Assimilate Media containing information in order to maintain the confidentiality and integrity of the information being handled, transported or stored and to prevent unauthorized use or disclosure of the information.

This policy applies to all Cogent workforce members and any other individual with access to Cogent information and / or Cogent systems, devices and networks.

Implementation Guide Lines

Portable devices and electronic media containing Cogent information shall only be removed from Cogent facilities to meet business requirements. Portable devices and removable media include, but are not limited to laptop computers, personal digital assistants (PDAs), enhanced cell phones/smart phones, backup media, tapes, disks, compact disks (CDs), digital video disks (DVDs), flash drives, hard drives and medical devices with memory storage.

An automobile is not considered a secure location. Under no circumstances shall an automobile be used to store Cogent information, even temporarily.

Media Handling

The use and handling of portable devices and media will be restricted to those individuals who are authorized to access the device or media.	**Workforce Members** Access and use of portable devices and media is restricted and requires management approval. The use of devices and media requires authorization by the regional Information Services (IS) department. If a staff member wishes to use a device he/she owns, the following is required: 1. Legitimate business need 2. Management approval 3. Meet Cogent controls.
Personally owned electronic storage media storing Cogent confidential or internal-use information are only allowed for Cogent business reasons and only when authorized by Cogent management. All such uses of personally owned electronic storage media must follow Cogent policies and standards relating to media controls.	

Portable devices and electronic media will be disposed of according to NIST Special Publication 800-88 Revision 1 when the device or media is removed from service.	IT Staff Devices must be destroyed safely by qualified IS personnel. Any mobile device and any electronic media that contains Cogent information must be encrypted. This includes devices synchronizing with Cogent e-mail.
Any portable electronic media or device containing Cogent information classified as confidential (e.g., ePHI, PII) or internal use (Cogent Information) must be encrypted and password protected.	
Loss, theft or destruction of electronic media or devices must be reported to Information Security .	Workforce Members Report information security incidents to your manager and then contact the Technology Operations Center.

Chain of Custody for Information Assets

Laptops assigned to the business unit and any other portable devices or electronic media such as flash drives, PDAs, enhanced cell phones or other memory storage devices are the responsibility of the business unit manager where the device is being used.	Department Managers All portable devices or electronic media used within the business unit are the responsibility of the business manager. These devices must be registered with the local information services. To track devices and the information they hold, keep a log of all portable devices and electronic media that exists in the department. This includes laptops, PDAs, USB drives, etc. If devices or media are moved outside of the department to another location the log needs to indicate that the information has been moved. Lines A. through E. describe the information to be included in the log. Periodically the inventory list registered with the local information services will be reconciled with the department inventory list. Portable devices not registered with the local information services group cannot be connected to the Providence network.
Portable devices and media that process or store confidential or internal-use information must be registered with the local information services group (Head or Local Site Office) and will be reconciled on a quarterly basis by the local information services group.	
Portable devices and media that process or store confidential or internal-use information must be inventoried and inventory logs maintained by the Business Unit Manager. Logs shall include: • Name of workforce member assigned • Asset tag number and/or serial number • Date assigned • Date returned • Encryption status	
Portable devices and media that are not entered via the inventory procedure and registered with the local information services group (Head or Local Site Office) will be prohibited from connecting to Cogent information systems.	

Media Labeling

Data Owners, and or Business Unit Managers shall identify and appropriately label all electronic storage media that contains Cogent information. If business requirements do not require Cogent information be present on the portable media or device, such information shall be removed. For media where labeling is infeasible or unwarranted (e.g., due to form-factor or typical use of media) reasonable means must be used to provide some physical identifying characteristic to the media indicating ownership and content (e.g., owner's name, contact information).	Department Managers and Data Owners The information on a device shall be for business purposes only. CD ROMs, floppy disks, and all media shall be labeled as noted below: The information is to be

Label information may vary depending on media purpose. Backup media labels or backup library information shall generally include: a) classification of the information present on the media b) format of the data c) software and version used to generate the information d) operating system and version e) date the media was last read and checked (for backup media)	classified as confidential, internal use, or public. If the media cannot be labeled the owner's name and contact information needs to be supplied. Lines A through E describe the information to be included when labeling media.

Device and Media Storage

Business Unit Managers shall develop procedures for the secure handling and storage of media and devices for which they are responsible.	**Department Managers and Data Owners** Store devices and media containing confidential or internal use Cogent information in a secure storage area such as a locked cupboard, drawer or a locked office with restricted access. Storage locations shall be in areas where the risk of damage to the devices or media is minimized. Those devices that store confidential information require a more secure location than those storing public information. Public information does not have the same security requirements, but shall be protected to ensure that the information does not get changed or damaged.
Media and devices that store confidential or internal use Cogent information must be secured from unauthorized access and use at all times.	
Appropriate redundant copies of Cogent information stored on devices and portable electronic media shall be maintained to ensure information availability shall the device or media be lost, stolen or damaged.	
Media and devices must be stored in a location providing physical security appropriate to the media classification level.	
Access to electronic media storage must be restricted to enable viewing, handling or use only by authorized individuals.	
Information classified as public shall be protected to maintain integrity and availability (for details regarding information classification see 801.100 Information Security Glossary)	

Media Storage Off-site

Cogent information which must be kept long-term may be stored off-site in an environment providing physical security appropriate to the information classification level.	**Department Managers and Data Owners** When information must be kept for long periods it may be moved to a long term storage facility. It is important to recognize that data may outlive the media that it is stored on. Data and media stored off-site must be encrypted and password protected.
Media containing confidential or internal-use information that is stored off-site shall be encrypted and password protected.	
In the event Cogent electronic information must be retained for an extended period of time, the data owner shall ensure that both the storage media and access technologies (e.g., applications) shall be retained. A comprehensive migration strategy shall account for vendor stability, system obsolescence and media longevity.	

An inventory shall be maintained for all Cogent media stored at the off-site storage facility.	A plan needs to be in place to ensure stability, media longevity, etc. (Consult with local IS for procedures.) Records are to be kept identifying the type and classification of the information. Before anything is moved off-site individuals responsible for establishing contracts with 3rd parties must ensure that all of the correct agreements are in place.
Appropriate privacy / security agreements must be in place with the media storage vendor before the devices or media are transferred to the custody of the vendor. All contracts for off-site media storage will be submitted to OCIO Legal for review and inclusion of appropriate agreements.	

Media Transport

Cogent employed couriers or contracted third-party carriers shall be used to transport media or devices with a classification of confidential or internal use, and must protect Cogent information assets from unauthorized disclosure. A formal record of transfer must be kept of the media or device given to the courier or third-party carrier and its receipt at the destination.	**Department Managers and Data Owners** Media Transport Responsibilities: Cogent information that is shipped to another location must be transported by either a Cogent courier or a 3rd party contracted courier. Managers must ensure that: a) A log is kept of the transfer (chain of custody) b) The device or media is encrypted c) The device or media has been packaged correctly d) An authorized method is used to transport the device or media
Individuals transporting portable devices or media off-site must be proficient in the use of appropriate security controls for those devices/media.	**Workforce Members** Individuals who take devices or media offsite for business purposes must be familiar with the security protections such as encryption and secure storage.
Medical devices being retired or returned to vendor/manufacturer and contain Cogent information shall have the data irretrievably removed prior to transfer from Cogent custody.	Department Managers and Data Owners Retired medical devices must have the memory wiped if they contain confidential information

9. Roles and Responsibilities

- The Chief Information Security Officer and is responsible for the content, communication and enforcement of this Cogent Policy . This Cogent Policy establishes minimum Cogent security specifications. Regional or local procedures or processes may exceed these minimum specifications. Violations of this Cogent Policy are subject to Cogent Disciplinary policy.
- The Information Security Manager is responsible for managing the secure disposal of all storage media in line with this procedure when they are no longer required, and is the Owner of the relationship with who is the approved contractor for removing shredded documents.
- All Owners of removable storage media are responsible for ensuring that these media are disposed of in line with this procedure. When we list out the assets; owners are identified , and they are responsible to adhere to the process/ procedures.

10. Related Documents

11.1. ISMS L3-A8.1.3: Guidelines to Asset Management