Cogent E Services Private Limited

Media Handling Policy

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. This document forms part of Cogent's ISMS Policy framework and as such, must be fully complied with; It states the steps Cogent will take to limit the opportunity for information leakage by implementation of best practice, processes and procedures

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	07th Jul'21	CISO	07th Jul'21	ISSC	07th Jul'21	11th Jul'21	
3.2	ISM	07th Apr'22	CISO	07th Apr'22	ISSC	07th Apr'22	11th Apr'22	

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://172.19.197.214/Policies

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

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.

1. Purpose

The purpose of this policy it to define the guidelines for the disposal of technology equipment and components owned by Cogent.

2. Scope

This policy 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.

3. Policy

4.1 Technology Equipment Disposal

4.1.1 When Technology assets have reached the end of their useful life they should be sent to the <Equipment Disposal Team> office for proper disposal.

4.1.2 The <Equipment Disposal Team> will securely erase all storage mediums in accordance with current industry best practices.

4.1.3 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.

4.1.4 No computer or technology equipment may be sold to any individual other than through the processes identified in this policy (Section 4.2 below).

4.1.5 No computer equipment should 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. The <Equipment Disposal Team> will properly remove all data prior to final disposal.

4.1.6 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).

4.1.7 Computer Equipment refers to desktop, laptop, tablet or netbook 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.

4.1.8 The <Equipment Disposal 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.

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

4.2 Employee Purchase of Disposed Equipment

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

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

4.2.3 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.

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

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

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

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

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

1. Objective

The objective of this policy is to prevent the unauthorised disclosure, modification, removal or destruction of assets and interruption to business activities. Media should be controlled and physically protected.

The Cogent E Services Private Limited (hereafter referred to as "Cogent") Media handling policy ensures that appropriate operating procedures are established to protect documents, computer media (tapes, disks), input output data and system documentation from unauthorised disclosure, modification, removal and destruction

2. Scope

a. 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.
b. An automobile is not considered a secure location. Under no circumstances should an automobile be used to store Cogent information, even temporarily.
c. This policy applies to all Cogent workforce members and any other individual with access to Cogent information and / or Cogent systems, devices and networks. For this standard, personally owned devices are out of scope.

3. DEFINITIONS:

"Electronic media" means (1) Electronic storage media including memory devices in computers (hard drives) and any removable / transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or (2) Transmission media used to exchange information already in electronic storage media. Certain transmissions, including of paper via facsimile, and of voice via telephone, are not considered to be transmissions via electronic media because the information being exchanged did not exist in electronic form before the transmission.

"Electronic protected health information" or **"E-PHI"** means protected health information that is transmitted by electronic media or maintained in electronic media.

"Individually identifiable health information" means information, including demographic information collected from an individual, that:

(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

(i) That identifies the individual; **or**
(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

"Physical Media" means electronic storage media and tangible material used to store data, including but not limited to tapes (reel, cassette), cartridges, disks, drums, CDs, DVDs, paper, microfilm, and microfiche.

"Protected health information" or "**PHI**" means individually identifiable health information that is:

(i) Transmitted by electronic media;
(ii) Maintained in electronic media; or
(iii) Transmitted or maintained in any other form or medium.

"Transport" means physical movement of physical media from its current location to any location, including within or between Cogent locations and a Cogent vendor.

"Vendor" means the same as the definition set forth in O.C.G.A. 45-1-6(a)(5), as well as any person seeking or opposing a certificate of need.

4. Information security statement on secure disposal

A 8.3 Media handling

Objective: To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.

Secure data disposal methods

What is this, and why is it important?

Information systems store data on a wide variety of storage media, including: internal and external hard drives; internal solid-state memory, removable flash memory cards and flash drives; floppy, ZIP and other types of removable magnetic disks; tapes, cartridges and other linear magnetic media; optical storage using CDs and DVDs; and paper.

To prevent unauthorized access, it is critical that data be rendered unreadable when it or the device on which it resides are no longer needed. This is required by law (and common sense) for all computers and media containing sensitive information. Insecure disposal is one of the most common causes of sensitive data being compromised. Not coincidentally, it is one of the most common methods by which identity theft occurs.

Organization's Position

Cogent has been using sensitive, private data to accomplish its goals. For the success of Cogent programs, and to meet legislatively-mandated privacy requirements, Cogent must keep that data secure. All data that is collected, maintained, and processed by the Cogent is considered highly sensitive and will be marked, handled, processed, and disposed of based on the requirements of that sensitivity level.

All removable media and documentation for systems owned or operated by Cogent are covered by secure disposal policy. All computer systems, electronic devices and electronic media must be properly cleaned of sensitive data and software before being transferred outside of Cogent premises before being sent for trash.

Computer hard drives must be sanitized by using software that are as detailed below. Non-rewritable media, such as CDs or non-usable hard drives, must be physically destroyed. All paper documents which need to dispose should be shredded in the premises before being sent out.

The primary responsibility for sanitizing computer systems, electronic devices and media rests with the IT Team.

PROCEDURES:

A. Maintaining an Inventory of Data on Physical Media

Where appropriate, Division heads will designate a point of contact responsible for maintaining physical media inventory. The physical media inventory must be updated upon the receipt, transport, or disposal of physical media containing PHI. Additionally, the designated point of contact shall be responsible for periodically verifying the accuracy of the inventory records.

B. Procedures for Securely Sending Physical Media out of Cogent

Prior to routing physical media containing PHI, Cogent employees should: (1) identify the individual responsible for receipt of the physical media, (2) contact the intended recipient to confirm date/time of transport (e-mail is sufficient), and (3) request written (e-mail is sufficient) confirmation of receipt from recipient. Where obtaining this information is not possible, employees should document their efforts and the results in the physical media inventory. See Attachment A. Additionally the inventory should include tracking or other

identification number associated with shipment and indicate whether the data media received are placed into storage or returned, destroyed, or data properly erased.

Cogent employees should use packaging effectively to help enhance security in transporting physical media containing PHI. See Attachment B.

C. Procedures for Securely Receiving Physical Media

Process

Prior to receiving vendor data, the appropriate business unit should work with the vendor to implement secure, electronic methods for transporting data. If the data cannot be sent securely electronically and the data must be shipped using physical media, vendors must encrypt the PHI on the physical media using at least 128-bit encryption prior to transport, in addition to other reasonable measures as defined in the vendor's contract.

Inspection

Packages containing physical media that may contain PHI must be inspected for damage by Cogent prior to accepting delivery. Delivery must be immediately refused for any packages that are discovered to be damaged. The damage must be documented by the inspecting Cogent employee. All instances of damage or missing physical media, regardless of when the damage or loss is discovered, must be immediately reported to the Director of Compliance. If damaged packages are accidentally accepted by a Cogent employee, onward delivery must not be performed.

Tracking

Upon receipt of physical media containing PHI, Cogent employees should promptly confirm receipt with sender. Cogent employees must log receipt into the appropriate physical media inventory. In order to ensure the security of the physical media containing PHI the following shall be required:

- Physical media shall not be transported through a major distribution hub (no mass handling or automated sorting)

- Point to point monitoring shall be required (e.g., signatures designating any change of custody – sender, courier or receiver, bar code scanning, delivery control numbers, logging)
- Materials or items must not be left unattended or in an unsecured vehicle
- Manifests are required and must include shipper, receiver, and driver signatures with delivery time and pick-up
- GPS tracking of physical media with PHI

Access

Designated points of contact within each unit should ensure that:

- Physical media is stored in a locked room or cabinet
- Access to storage areas is limited and restricted to those with a need to carry out their job responsibilities
- Removal of media is recorded, including identification of the handler, purpose, date, time, intended disposition, and expected return date if applicable

D. Dissemination and Training

This policy will be disseminated to employees and the business units via Cogent Intranet.

All vendors who conduct business and transport physical media to and from Cogent shall agree to the terms and conditions of this policy.

The Director of Compliance will provide information to management for training Cogent employees on this policy for transporting physical media containing PHI and compliance with relevant privacy and information security laws, regulations, and requirements.

E. Review, Updates, and Monitoring Compliance

This policy will be reviewed at least annually and updated as appropriate by the Office of General Counsel. The Office of Inspector General shall be responsible for auditing business functions to ensure compliance with this policy.

F. Vendor Relationships

Each contract with vendors shall outline Cogent 's requirements for the safe handling of information as they apply to storage and transport, including access controls, copying, authentication systems, or encryption. Vendors will agree and acknowledge that they have the following:

- Media Storage: Procedures for safe storage of both electronic and print media including requirements for the copying of archived data should that media deteriorate.

- Media Destruction: Procedures for securely erasing data from media or physically destroying media, as well as any requirements for securing transport to facilities for erasure or destruction.

- Media Transport: Information-handling procedures for storage, packaging for internal messenger, packaging for external mail or courier services, shipping tracking, and destruction.

- Audit: Requirements for validating transport and storage controls, data erasure and media destruction methods, and requirements for timing for destruction.

- Incident Management and Escalation: Clear definition around what constitutes "lost media" and the timeline for notifying the Department when an incident has occurred.

The following is provided for guidance to enable adherence to the security and protection of data and the handling of related media:

- Data, information and media must only be accessed, processed and transmitted as and when required by authorised persons for Cogent business purposes and must not be accessed, viewed or processed in any way for casual or personal use

- Formal Information Sharing/Exchange policies and procedures must exist across all Cogent departments where information sharing and exchange is required or occurs between Cogent and any external partner or organisation

- Cogent provides a process by which requests may be made to the IT Service Desk for data which needs to be encrypted on portable media such as laptops, memory sticks and DVDs/CDs. This will ensure that the security and integrity of data being delivered/transported to other Cogent locations, external organisations and partner agencies is maintained and cannot be intercepted/amended. Encryption levels of data on such media must be a minimum of 128bit AES - in line with the Cogent 's Encryption Policy. Sensitive and personal data must not be faxed to an unsecured

location under any circumstances. All requests for encrypted media must be requested via the IT Service Desk

- Formal Information Sharing/Exchange agreements must detail the responsibilities, technical and procedural control standards, liabilities and any special controls that may be required in order to ensure the secure information exchange through all communication methods

- All information assets must be classified and appropriately marked to determine the level of security protection (including backup, storage, encryption, maintenance, records and audit requirements) they are afforded based on risk assessments. More information on data backups is available in the Cogent 's Information Backup and Restore Procedures
- Paper files, removable media and other records or documents containing personal or sensitive information and data must be kept in secure environments in line with the Cogent 's Clear and Secure Desk Policy and not removed, transmitted, transferred or copied in any form (including physical transfer or electronic communications method) that, if loss or interception occurs, introduces an unacceptable risk of disclosure, theft, or damage of data and information.

- If media contains sensitive or person identifiable information and data and you cannot physically secure your workspace or area, you must store any such media securely within a locked cupboard, drawer, office or other securely 'locked' environment

- The use of courier contractors to transfer information/media is restricted to organisations and agencies with which Cogent has formal contractual agreements

- Personal or sensitive information and data held on, or transmitted between, electronic systems and the systems themselves, are protected by the implementation of procedural and technical controls that reduce risks of interception, unauthorised disclosure, loss or unauthorised alteration to acceptable levels as defined by the Cogent 's Risk Management Strategy

- Person identifiable or sensitive information and data is not transmitted via electronic messaging services including email and EDI systems unless appropriately protected and with the approval of IT management and the Information Security Manager. The transmission of person identifiable or sensitive information by SMS text and Instant Messaging services is not permitted under any circumstances

- The retention of information must be defined by retention policies which meet the requirements of the Cogent , contract or UK legislation and appropriate procedures must be implemented to ensure that information is held securely and is safely retrievable on request

- Sensitive or personal information and data held on any media must be physically destroyed when due for disposal or no longer required. Procedures for identifying media that requires secure disposal must be implemented and an audit trail of any media passed to external organisations must be maintained. Where specialised disposal techniques are required, media must only be passed to reputable organisations dealing with secure disposal of information with whom Cogent has formal contractual agreements. Backup data/media no longer required must be disposed of securely and with due environmental consideration

- All sensitive and person identifiable information and data stored on portable media must be Cogent supplied media and encrypted in line with the Cogent 's Encryption Policy:

a. Management of removable media

i. Procedures should be in place for the management of removable media which ensures that

ii. All media should be stored in a safe, secure environment in accordance with the manufactures specifications.

iii. Removable media drives should only be enabled if there is a business reason for doing so. The head of the department or SVP Project should authorize the request for enabling media.

iv. If no longer required, the content of any re-usable media should be made unrecoverable.

Media Handling

1. 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: • Legitimate business need • Management approval • Meet Cogent controls.
1. 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.	

b. Disposal of Media

c. Formal procedures for secure disposal of removable media (tapes, disks, flash disks, removable hard drives, CDs, DVDs and printed media) should minimize the risk of sensitive information leakage to unauthorised persons. The following procedures should be followed

i. Media containing sensitive information should be stored and disposed of securely and safely.

ii. Devices containing sensitive information should be physically destroyed or the information should be destroyed, deleted or overwritten using techniques to make the original information non-retrievable.

iii. Damaged devices containing sensitive data should be assessed to determine whether the items should be physically destroyed rather than repair.

iv. All unusable magnetic tapes and hard drivers should be erased securely using a degaussed.

v. When disposing of paper documents, always shred documents in the cross shredders; and do not throw them in the garbage. If one is not able to shred the document, use receptacles (i.e. locked recycle bins) designed for secure paper disposal.

vi. A record of all media disposed and the relevant authorization forms for such disposal should be maintained.

• Portable devices and electronic media will be disposed of according to *Media and Device Sanitation and Disposal Standard* 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., eCogent data, 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 Enterprise Security in accordance with System Policy PROV-ICP-717 *Early Reporting of Significant Compliance, Risk and Regulatory Issues*.	**Workforce Members** • Report information security incidents to your manager and then contact the Technology Operations Center.

Further information and observations

- The procedures for secure disposal of media contain sensitive information should be commensurate with the sensitivity of that information.
- Disposal of sensitive items should be logged where possible in order to maintain an audit trail.

5. Roles and Responsibility

Chief Information Security Officer (CISO) shall ensure procedures are in place for the following:

- Approve, as needed, reproduction of sensitive data files.
- Sign for, or designate an alternate to sign for, receipt of registered, certified, or express mail which can contain sensitive data.
- Review the transmittal logs on a monthly basis to ensure all tapes and hard copies are accounted for and to resolve any discrepancies.
- Identify in the security plan the disposition procedures for media no longer used to process or store sensitive information.

Supervisors shall:

- Ensure that employees are aware of the Cogent security requirements.
- Monitor employee activities to ensure compliance with all security requirements and legal requirements.
- Ensure that only Cogent authorized software runs on Cogent automated information systems.
- Approve, as needed, reproduction of sensitive data files.
- Sign for, or designate an alternate to sign for, receipt of registered, certified, or express mail which can contain sensitive data.
- Review the transmittal logs on a monthly basis to ensure all tapes and hard copies are accounted for and to resolve any discrepancies.
- Identify in the security plan the disposition procedures for media no longer used to process or store sensitive information.

System/Application Administrators shall:

- Designate the user profiles.
- Establish and communicate the safeguards required for protecting their systems, data, and databases.
- Ensure that sensitive data are not stored on personal computer's hard disks.
- Track data sets from creation through destruction.

Users shall:

- Adhere to the security safeguards required to protect sensitive data, databases, and application systems.
- In accordance with the data rules listed below, appropriately identify, date, and mark sensitive information originated, produced, or processed by Cogent .
- Ensure that media containing sensitive data are labeled: "This contains SENSITIVE INFORMATION" and are stored in key-locked or combination-locked filing cabinets when not in use.
- Do not store both sensitive and non-sensitive data on the same media.
- Ensure that sensitive information is not printed on printing devices that use printer ribbons.
- Do not leave computers unattended when processing sensitive data or when sensitive data or a critical application system is resident in memory.
- Sign for all data sent, received, or transported.
- Shred sensitive printed products and appropriately dispose of other data storage media when no longer needed.

6. Framework

A 8.3.1 Management of removable media

Control
Procedures should be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.

Chain of Custody for Information Assets

1. 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.
Portable devices and media that process or store	

confidential or internal-use information must be registered with the local information services group (Regional or System Office) and will be reconciled on a quarterly basis by the local information services group.	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.
2. 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 should include: a. Name of workforce member assigned b. Asset tag number and/or serial number c. Date assigned d. Date returned e. Encryption status	
1. Portable devices and media that are not entered via the inventory procedure and registered with the local information services group (Regional or System Office) will be prohibited from connecting to Cogent information systems.	

Media Labeling

1. Data Owners, and or Business Unit Managers should identify and appropriately label all electronic storage media that contains Cogent information. If business requirements do not require the 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 should be for business purposes only. CD ROMs, floppy disks, and all media should be labeled as noted below: The information is to be 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.
2. Label information may vary depending on media purpose. Backup media labels or backup library information should 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)	

Device and Media Storage

1. Business Unit Managers shall develop procedures for the secure handling and storage of media and devices for which they are responsible. 2. Media and devices that store confidential or internal use Cogent information must be secured from unauthorized access and use at all times. 3. Appropriate redundant copies of Cogent information stored on devices and portable electronic media should be maintained to ensure information availability should the device or media be lost, stolen or damaged. 4. Media and devices must be stored in a location providing physical security appropriate to the media classification level. 5. Access to electronic media storage must be restricted to enable viewing, handling or use only by authorized individuals. 6. Information classified as public should be protected to maintain integrity and availability (for details regarding information classification)	**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 should 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 should be protected to ensure that the information does not get changed or damaged.

Media Storage Off-site

1. 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. 2. Media containing confidential or internal-use information that is stored off-site shall be encrypted and password protected. 3. 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) should be retained. A comprehensive migration strategy should account for vendor stability, system obsolescence and media longevity. 4. An inventory shall be maintained for all Cogent media stored at the off-site storage facility. 5. Appropriate privacy / security agreements must be in place with the media storage vendor before the devices or media are transferred to the	**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. 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

custody of the vendor. All contracts for off-site media storage will be submitted to OCIO Legal for review and inclusion of appropriate agreements.	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.

Media Transport

1. Cogent employed couriers or contracted third-party carriers should be used to transport media or devices with a classification of confidential or internal use, and must protect the 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** <u>Media Transport Responsibilities:</u> 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 log is kept of the transfer (chain of custody) • The device or media is encrypted • The device or media has been packaged correctly • An authorized method is used to transport the device or media
2. 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.
3. Medical devices being retired or returned to vendor/manufacturer and contain Cogent information should 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

A 8.3.2 Disposal of media

Control
Media should be disposed of securely when no longer required, using formal procedures.

What is really secure?

As with the secure retention of information, there is no bright line that separates "secure" from "insecure" forms of disposal. For each storage medium there are more and less secure methods. What is appropriate in a particular situation depends on the sensitivity of the information at issue, and the perceived threats to it. The more secure methods generally cost more to implement, both in time and explicit expense, and/or require more expertise to do correctly. In the end, only total physical destruction affords total security. For its most secret information, the US government requires that one "[d]isintegrate, incinerate, pulverize, shred, or smelt."

Disposal Guidelines for Paper-Based Media

1. The proper media disposal technique for any paper based documentation must match the highest classification of data that is contained in that document. Therefore, a document containing both Cogent classified sensitive and restricted data must be disposed of in the manner required for the disposal of restricted data.
2. Existing Departmental Managers are responsible for overseeing paper-based document disposal in his or her area.
3. Destruction methods for paper-based documentation includes use of the Purdue Cogent Confidential Material Recycling Program, and other methods such as shredding (cross-cut shredding is best), disintegration, incineration, and pulverization.

Disposal Guidelines for Electronic-Based Media

4. The proper media disposal technique for electronic storage devices depends whether or not the electronic storage media is being repurposed for Cogent use.
5. Electronic Storage Devices Repurposed for Cogent Use: If the physical media is going to be repurposed for Cogent use, then the electronic storage device must be wiped with a multiple pass/DoD secure overwrite prior to being repurposed to another unit or area.
6. Electronic Storage Devices NOT Repurposed for Cogent Use: If the physical media is not going to be repurposed for Cogent use, then the electronic storage device must be physically destroyed.
7. Existing Departmental Managers are responsible for overseeing electronic storage device disposal in his or her area. This responsibility includes ensuring that

appropriate multiple pass/DoD secure overwrites are properly completed and documented in the event that storage devices are repurposed for Cogent use.

8. Multiple pass/DoD overwrite means to overwrite all addressable locations with a character, its complement, then a random character, and verify.

9. Physical destruction methods for electronic storage devices include use of the Purdue Recycling for the Future program. Other methods of physical destruction may be acceptable so long as the electronic storage device is destroyed and the data contained on that device may not be recovered by any means.

Paper media

Paper containing sensitive information should be shredded. Dumpster-diving" for data is common.
Cogent office should have access to a shredder or a secure shredding service.
Strip cut shredders (also called straight cut or spaghetti cut) render paper into thin, long strips. Cross-cut shredders (also called confetti cut) provide both length-wise and width-wise dismemberment. Cross-cut units make re-assembly much more difficult, but are, unfortunately, slower than strip-cutters, more expensive, and tend to require more maintenance.

Alternatively, paper records can be pulverized (rendered into a powder by grinding), macerated (rendered into pulp by chemicals) or incinerated (burned). This is appropriate for extremely sensitive information.

Electronic media

The appropriate "cleaning" method for electronic media depends on the type. The main division is between "magnetic media" and "optical media." Though both contain information in electronic form, the methods for secure disposal are very different.

Many people are under the impression that all they need to do is "delete" a file from a computer's hard drive or other storage media. Unfortunately, that's almost never sufficient. In most cases,"delete" simply changes indexing information about a file, sort of like marking through the entry in a book's table of contents but leaving the pages behind.

Emptying the "recycle bin" or the "trash" folder of deleted files is usually also ineffective. These methods remove the pointers (indexes) to the deleted files, but the data itself still remains on the storage media as unallocated space.

Even if the unallocated space is subsequently used by new files, there are sophisticated scanning methods that could be used to recover data previously stored in those locations.

Some un-rewritable media, like CD-Rs and DVD-Rs, can't have their contents deleted in any case. Inoperable media, like a crashed hard drive, may be so corrupted that you cannot access it using normal computer operations; but it still may have data on it that can be recovered by others.

Demagnetizing magnetic media

Removable magnetic "disks" (floppies, ZIP disks, and the like) and linear magnetic media (tape reels, cartridges) can be "degaussed" -- that is, demagnetized. An appropriately-sized and -powered "degausser" is required.

For each particular type of magnetic storage and size of degausser there is a minimum erasing time. "High coercivity" magnetic media require more powerful degaussers and/or more time to achieve sufficient cleansing effects.

As with disposal of paper information, there are trade-offs rather than absolute standards for "erasing" magnetic media. The more powerful and lengthy the degaussing process applied to any given type of storage media, the less likely it is to be subsequent recovered by others.

Secure degaussing cannot be achieved with household or over-the-counter magnets, no matter how powerful they may seem to be. (Such magnets can do some damage to data you want to keep, however. Keep them away from your computing devices and storage media.)

Note that degaussing can make the media inoperable, so this method is not recommended if the media needs to be reused and/or has resale value. Use over-writing instead.

Over-writing magnetic media

"Fixed" internal magnetic storage, such as computer hard drives, as well as external "mini" and "micro" hard drive storage, can be cleaned by software that uses an over-writing or "wiping" processes. USB "flash drive" devices and plug-in memories like CompactFlash, Memory Stick, Secure Digital, and SmartMedia can also be cleaned in this way.

Special software is used to over-write all the usable storage locations. The simplest method is a single over-write; additional security is provided by multiple over-writes with variations of all 0s, all 1s, complements (opposite of recorded characters) and/or random characters so that recovery even by the most sophisticated methods becomes almost impossible.

Most "secure file deletion" software offers a choice of more and less secure over-writing. More secure methods take more time, given the multiple over-write operations, so again there is a tradeoff. (Note also that the quality of the over-write algorithms offered by alternative products varies.)

There are a few free public domain programs like DBAN that perform secure over-writes. There are also many commercial offerings (see the list of links on the DBAN web page). ***Use caution with these products. They perform deletes from which you cannot recover.***

If you have a Macintosh computer running Mac OS X, you have several built-in options for securely removing data:

For files you've deleted by dragging them to the Trash, use Secure Empty Trash from the Finder menu. It will overwrite and delete files in your Trash folder.

For whole file systems, use the Disk Utility, which can be found in the /Applications/Utilities/ folder. Select the file system on which you want to securely remove data, then select the Erase tab. On the Erase pane, the Erase Free Space button lets you overwrite free space on the file system--that is, space that may contain data for files that have been deleted insecurely. The Security Options button lets you

delete or overwrite files that still exist. Each of these buttons gives you the option of overwriting files once, 7 times, or 35 times.

For individual files, use rm -P from the command line. It overwrites files three times before deleting them.

Mangling magnetic media

You can take a hammer or a high-speed drill to your hard drive, USB drive or other device. Chances are excellent that you'll render it inoperable in short order.

But be warned that recovery of data from physically mangled magnetic devices is still possible. Physical destruction is generally something that must be done by a trained person to be completely effective, particularly for hard drives.

Floppy disks can be broken open and the internal magnetic disk cut up. As with optical media (see next discussion), caution is required to avoid personal injury from flying plastic parts, etc., and it is still theoretically possible to recover data even from a mangled disk.

Optical media

"Write-many" optical media (such as CD-RWs and DVD-RWs) can be processed via an over-write method similar to that for magnetic media. However, the vast majority of optical media in use are of the "write once" type -- notably the ubiquitous CD-Rs and DVD-Rs. They cannot be over-written. Because such media are optical rather than magnetic, neither can they be degaussed.

So, as with paper, only physical destruction will do. Many higher-capacity paper shredders are rated for CD/DVD destruction for exactly this reason. It's a good investment to upgrade to a shredder that is CD/DVD capable if you regularly rely on optical media for your data storage.

As with magnetic media, you can perform a physical attack. Cutting a CD or DVD with scissors is an alternative if you have only a few to do. But note that cut-up discs have been successfully reassembled and read, so cut them into multiple pieces and, ideally, dispose of the pieces in different trash receptacles.

Breaking discs in half with your hands can send dangerous shards of plastic flying. Burning discs (or microwaving them) can release toxic fumes. Don't ever do this!

Computer recycling programs

For a whole system, some manufacturers (like Dell and Apple), and many retailers of computer equipment, offer recycling programs that meet both security and environmental concerns. These programs will process the entire old system for disposal, including cleaning the hard drive and any other storage media, when you trade it in as part of a new purchase.

Use a search engine to find out what is available for your home system. For your work system, make sure you follow the surplus equipment procedure.

Disposal of equipment:

Computer hardware disposal can only be authorized by the IT security officer who should ensure that data storage devices are purged of sensitive data before disposal or securely destroyed. The procedures for disposal must be documented. Unusable computer media should be destroyed (eg floppy disks, magnetic tapes, CD ROMS).

Media disposal:

All removable media should be reformatted before disposal, however if this is not possible, the media should be destroyed.

Disposal process

Overview The scope of this process covers all current known media types. Some of the forms of media are not used by Cogent so there is no method of disposal; where this is the case the process in this section is marked as "Not Applicable. Medium not used by Cogent ". To keep the processes as clear as possible and to make adherence easier, wherever possible common methods of disposal will be applied to the various forms of data and information in use. In these cases cross-reference will be made to the first instance of that method.

The processes

1.Paper documents : Secure media must be shredded, using one of the shredders situated on the Xxxxxx xxxxx floor of Xxxxxx xxxxx. The shredded material is then sent for recycling with

Shredded and general waste are all disposed of by Waste Services.

Recycled non-confidential waste is collected by Xxxxxx xxxxx

Non-Secure items can be disposed of either by recycling or through the general waste disposal procedure. It should be noted that the recycling process does NOT entail shredding before recycling, thus it should not be used for Secure disposal.

Disposal of Media

The companies used for paper waste disposal are given in Appendix 1 to this document.

2. Voice or other recordings

Secure items:

Tapes from tape-based telephone answering machines and dictation machines should be erased before disposal.

Digital telephone answering machines should have message stores cleared by removing the back-up batteries and unplugging the machine from the mains. The manufacturer's instructions should be consulted on how to do this. Once this is done the machine can be passed on to another user or disposed of in the general waste – taking care to follow the environmental policy at the same time.

Non-Secure an be disposed of either by recycling or through the general waste disposal procedure.

3. Carbon paper

Medium not used by Cogent .

4. Output reports.

These should be disposed of by the appropriate procedure in "Paper documents" in section 1 above.

5.One time-use printer ribbons

Not Applicable. Medium not used by Cogent .

6. Magnetic tapes

Secure items : all tapes used on IT systems are included in this procedure. All tapes are to be sent to IT Operations for erasure of data and disposal. Each tape is to have data removed in accordance with the manufacturer's instructions.

Once the data has been erased tapes be disposed of as in the general waste disposal procedure.

Non-Secure items: be disposed of through the general waste disposal procedure.

7. Removable disks or cassettes

Cassettes: Not Applicable. Medium not used by Cogent .

Secure items:

(Hard disks should be returned to the IT Operations department at Xxxxxxx where the data will be removed either by low level reformatting or by use of a proprietary package.

Floppy disks and zip disks: these should be either reformatted by the user before

disposal or re-use on another system or returned to the IT Operations department at Xxxxxxx for reformatting for re-use or disposal in the same way as for hard disks in above para.
Non-Secure items can be disposed of either by recycling or through the general waste disposal procedure.

8 Optical storage media

Cogent uses compact disks (cd) and digital video disks (dvd). Both can contain proprietary software etc. from suppliers and cds can be written to hold Cogent data and information.
Secure items : Re-writeable cds & dvds must be re-formatted prior to disposal or re-use. Read-only cds & dvds must be rendered unreadable either by shredding, scratching, heating or similar means which is "bad" for the item.
If sufficient numbers of such disks are to be destroyed the Facilities Manager is able to organise an external company to shred the disks either on or off-site.
Once the data has been removed or rendered unreadable as above the disk material can be disposed of via the general waste disposal procedure.
Non-Secure items can be disposed of through the general waste disposal procedure.

10. Test data

Secure items: should be dealt with as per the particular type of media's "Secure items" procedure above.
Non-Secure an be disposed of through the general waste disposal procedure.

11. System documentation

Secure items: should be dealt with as per the particular type of media's "Secure items" procedure above.
Non-Secure an be disposed of through the general waste disposal procedure.

Other data and information

The Human Resources department shreds all Secure items as in "Paper documents" above. Other records, which must be kept, are archived.
For information, the Purchasing Executives receive tender information from potential suppliers in printed from and quite often on floppy disk. This information is archived in secure off-site storage. Disposal of these items should be through the processes described above.
Users with data or information holding media whose disposal is not covered by one of the above processes should be referred to the IT Security Officer for guidance.
All staff in Cogent have a duty to protect all official information .Handling of such information and data is covered in the "Compliance" procedures prepared by Cogent 's IS department. Of particular relevance to this report (Disposal of Media) is the "Destruction" section under the heading "Safeguarding official material outside government" as is the "Fifth principle" of the Data Protection Act (as given in the section headed "Data protection and privacy of information".
7.4 Recording of Disposal
All disposals of media are recorded in the "Media Disposals" record log. This records the date received, the owner, the media type, the number of items, the labelling of items, the date disposed of by IT Operations and who did it. A sample form can be found in Appendix 4

Methods of erasure/destruction
5.1 Software disk wiping utilities
5.1.1 Software disk wiping utilities aim to completely remove data from the disk. Various standards exist for the number of passes a disk wiping utility may use – generally 1, 3 or 7 overwrites called as passes. The software wiping utilities approved by Cogent are
Recuva
Shred

DBAN
Geeks nerds Drive Wiper
5.2 Degaussing
5.2.1 Degaussing is the process of decreasing or eliminating an unwanted magnetic field. It is an acceptable method of destroying data from magnetic media.
5.3 Physical destruction
5.3.1 Physical destruction is the last option for secure disposal of media which gives the absolute guarantee. Physical destruction is an option for defective disks which cannot be wiping using the software.

A 8.3.3 Physical media transfer

Control
Media containing information should be protected against unauthorized access, misuse or corruption during transport ation.

Backup Tapes Movement

- **Cogent Backup Outgoing Tape Movement Process**
    - System administrator will be sending an email to the Admin and Finance point of contact to collect the backup tapes from respective locations
    - System administrator will label the tapes, securely pack the tapes with the labeling, seal them and Head – IT needs to sign on the package.
    - IT will be initiating the request to move the backup tapes – Backup Outgoing Tape Authorization Form has to be filled by the IT engineer who is packing the tapes


Outgoing tapes form

    - IT rep will take the Head IT's approval for sending the backup media out of the office
        - Admin representative will collect the tapes, and give a confirmation on the form before taking the tapes out from the office
    - Admin will deposit the copy of that form on reception as gate pass to take the tapes to the offsite location.
    - Admin and Finance representative will be accessing the bank locker and will deposit the backup tapes. They are responsible for bringing the weekly tapes, additional tapes for restoration and any adhoc request back from the bank locker too
    - Then the process of Incoming Tape Movement will follow.
- **Cogent Backup Incoming Tape Movement Process**
    - Admin and Finance reps are also responsible for brining the weekly and any other adhoc tapes back from the offsite location.

- At the time of keeping the weekly backup tapes, they will take back last week's backup tapes to the onsite location.
- If the request for brining the weekly or monthly is fresh, the entire process for tape movement initiation needs to be followed.
- On returning, they will fill up the **"Incoming Backup Tapes Register"** kept at the reception and after getting that register signed from IT rep they will hand over those tapes to that IT rep. That entry also needs to be countersigned by security personnel and after that tapes would be allowed to enter in the company premises.

- **Tape Labeling Nomenclature**


Tape Labeling Nomenclature.doc

Recommendations for specific types of media

Different type of media would require different procedures for disposal.

4.1. Magnetic Media

4.1.1 Magnetic disk contains lots of data which is not scrambled completely by formatting the media. Data can be easily recovered from the formatted hard disk. Disk wiping utilities should be used for permanent erasure of data.

4.1.2 Cogent recommends use of tools like Geeks nerds Drive Wiper, Symantec's Norton GDisk, Shred or DBAN for disk wiping. DBAN which is a free ware is the DOD 5220-22M compliant tool which makes three (1, 2 and 7) of the seven passes recommended under DOD 5220-22.M standard.

4.1.3 Media which cannot be erased using the software must be either

4.1.3.1 Degaussed or

4.1.3.2 Physically destroyed

4. Policy Compliance

5.1 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.

5.2 Exceptions

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

5.3 Non-Compliance

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

Appendix

A – List of Methods Approved for Secure Data Destruction

The following are general classes of Electronic Media:

- **Magnetic Media** – include, but not limited to, internal or external computer or printer hard drives (IDE, SCSI, SATA USB, or other type of connector), Zip or Jaz drives, floppy disks, magnetic tapes, VHS tapes, cassette tapes, etc.
- **Optical Media** – include, but not limited to, laser disks, CDs and DVDs, etc.
- **Solid State Drives** – include, but not limited to, USB storage devices (such as thumb drives), digital storage cards (such as camera cards), cell phones, PDAs, etc.

1. **Overwriting** - Using NIST 800-88 compliant multi-pass software or hardware to overwrite Electronic Media with zero's or generic patterns. This is typically Magnetic Media and rewritable optical media.
2. **Degaussing** – Using NIST 800-88 compliant degaussing (or demagnetizing equipment) to erase Magnetic Media.
3. **Physical Destruction** – Using NIST 800-88 compliant methods for physically destroying media. Optical media may be shredded or be passed through a grinder; Magnetic media may be melted or pulverized after being degaussed or overwritten. Solid State Drives present a particular challenge as their nature of storage lends itself to data remanence. As such, may be melted or pulverized after an attempt at degaussing or overwriting.

B - Physical Media Inventory

Each record listed in the physical media inventory must include:

- Origin of data
  - -designated Cogent owner of the physical media
  - -technical contact of data creation
- Destination (location to which the physical media will be transported or received)
- Frequency of transport (e.g., daily, weekly, monthly, periodic)
- Physical media type
- Approximate number of records contained in the physical media
- Data type (e.g. "public information"; "Cogent data")
- Encryption, if not public information (e.g., give password or specify other means)
- Number of items typically included in the shipment
- Size of data on media (e.g., 100 MB, 3 GB)
- Data protections in place to help protect the physical media from loss, theft, or unauthorized disclosure
- Description of shipping method and level of service
- Risk (e.g., no impact, minor, significant, tangible, serious, grave)

The physical media inventory must be updated upon the receipt, transport, or disposal of physical media.

C- Packaging Physical Media

Cogent employees and vendors should enhance the security in transporting physical media, especially when the media contains SENSITIVE DATA.

Envelopes shall not be utilized to ship physical media containing Cogent data. Metal containers with a locking mechanism should be used. If metal containers are not available or are not practical for shipments, Cogent employees and vendors may use hard cardboard boxes that comply with the following parameters:

- Prior to packaging, duplicate the media and securely store the duplicate so that it may be promptly identified, located and used as needed, in the event of a loss
- Secure the data on the media through encryption, such as a strong password, or other technological means
- Double box the package, i.e., place the inner container in a new, outer corrugated cardboard box
- Tape with 2” pressure sensitive shipping tape
- Reinforce the box at four corner points and place tape across box
- Lock or seal containers before leaving secure premises
- Enclose the physical media in tamper-resistant / tamper-evident wrap
- Do not mark the outside of the box with information pertaining to its contents or classification
- Shipments should be addressed clearly to a specific recipient by name, using business address.