DOCUMENT NO.	*SPP-1011*
DOCUMENT NAME	*DATA CLASSIFICATION & MEDIA CONTROL POLICY*

REVISION LEVEL	9
REVISION DATE	DECEMBER 20th, 2017
OWNER	DARREN COOK, DIRECTOR OF INFORMATION SECURITY

REVISION LEVEL	HISTORY	REVISION DATE
A	Initial Release	November, 2005
B	Updated to conform to current organizational structure and new technologies.	March 28th, 2008
3	Updated to latest template and revision numbering convention.	August 6, 2010
4	Added privacy, data classification, and inventory language.	August 12th, 2013
5	Default classification levels New classification scheme	October 17th, 2013
6	Procedures for removable media	November 7th, 2013
7	Added new policy note concerning data classification labels for SPPs, Changed CSO to CTSO, Minor formatting changes	March 8th, 2016
8	Updated team names in 1.3.7 and 1.3.11 to current versions	March 8th, 2017
9	Changed owner to Darren Cook, Removed CTSO from "Responsible Parties", changed CTSO to Director of Information Security in section 1.33	December 20th, 2017

INTRODUCTION

PURPOSE AND SCOPE

This document details the media control methods required to maintain the highest possible level of information security. Additionally, this document defines and classifies critical systems and data, and specifies which departments may access said systems and data as a part of their job function. For the purposes of this policy, the term "employee" includes any independent contractor who through the course of their relationship with Datapipe has access to Datapipe information and/or information systems. Datapipe does not use or disclose client data for any purposes unless written permission in the form of an authorization is provided by the client. Datapipe protects the privacy of all client data. While Datapipe does not classify client data, it treats all client data as confidential.

This document applies to all electronically stored media, hardcopy media, critical systems and confidential data not necessarily attached to a particular medium.

RELATED DOCUMENTS

SPP-1020	Datapipe Organizational Security Policy

TERMS AND DEFINITIONS

NA	NA

RESPONSIBLE PARTIES

SEC ENG	Security Engineer
TEAM LDR	Team Leader
PROJ GR	Project Manager

1 DATAPIPE DATA CONTROL

1.1 SENSITIVITY LEVELS

1.1.1 PUBLIC

Any records or documents that may be shared with clients or prospective clients. Such information might include:

A. Process overviews
B. White papers and marketing publications
C. Audit summary reports

1.1.2 PROTECTED

Any records or documents that may be shared with clients or prospective clients with an NDA in place. Such information might include:

A. Policies governing client services
B. Audit reports

1.1.3 INTERNAL

Records, documents and information made available to all employees. Such information might include:

A. Wiki publications
B. Pipeline
C. Shift reports
D. Training documents
E. Approved process/procedure documents
F. Forms

1.1.4 RESTRICTED

Records, documents and information that only certain privileged employees may view on a need-to-know basis. These include:

A. Training records
B. HR records
C. Contracts

1.1.5 CONFIDENTIAL

This level is reserved for information only available to executive management and their specific designates, when warranted. Such information includes:

A. Financial records
B. Legal information
C. Organizational expansion transaction details
D. Media that includes cardholder data
E. Information Security Management Committee records

1.2 DEFAULT CLASSIFICATION

Documents which are not explicitly labeled shall have a default classification. These default classifications can vary depending on document type or content. The following default classifications have been established:

1.2.1 INTERNAL

Standard Policies and Procedures (SPPs), including Information Security Management System (ISMS) policies and procedures, shall have a default classification level of Internal unless otherwise labeled.

1.2.2 CONFIDENTIAL

Information Security Management System (ISMS) records and other documentation (including Risk Assessment / Risk Treatment Plans) shall have a default classification level of Confidential unless otherwise labeled.

1.2.3 SPP LABELING

Effective March 8th 2016, all reviews and revisions to SPPs must have a data classification label applied to them. This label shall be in the form of a watermark, which states the classification level of the SPP, leveraging the sensitivity levels noted in section 1.1 of this policy.

1.3 ACCESS BY LEAST PRIVILEGE

Access to the above classifications shall be limited to the least privileges required to perform business operations. Least privileges for an individual user shall be detailed and validated by Management with the User Authorization Form. Datapipe defines the following corporate divisions that will receive relevant privileges:

1.3.1 DIRECTORS

These individuals reserve the right to become aware of all sensitivity levels of data as circumstance require, however they do not necessarily require Confidential and Restricted security levels of data as part of their daily job functions.

Directors may also grant Confidential and Restricted data access to those individuals who do not otherwise have such access as part of their normal job function. Directors shall only grant such access on a need-to-know basis.

1.3.2 NETWORKING TEAM

Those individuals most directly responsible for firewall, router and switch administration who possess all associated access rights and privileges, including access to Restricted information relevant to above network components.

1.3.3 SECURITY

Those individuals responsible for maintaining company-wide informational and physical security and who therefore reserve the right to become aware of any required access and administrative rights and privileges of any classification as defined above.

Director of Information Security has full access to all data security levels and must be kept aware of all threats, breaches and/or failures to comply with this policy.

1.3.4 SUPPORT TEAM

1.3.4.1 MANAGEMENT

Those individuals most directly responsible for client web, database and mail server administration who possess all associated access rights and privileges of the Restricted security levels.

1.3.4.2 SUPPORT STAFF

Those individuals most directly responsible for client support who may require access rights to client passwords and other secure client information, but do not generally have access to Restricted information.

1.3.5 DEVELOPMENT TEAM

Those individuals who establish proprietary programs, services and systems. These individuals possess all rights to create a service or system that will contain or transmit secure information, but once such a system is created, these individuals may not access the secure data items contained within.

1.3.6 HR AND ADMINISTRATION

1.3.6.1 HR

Maintains all employee training, payroll, contact and other records. Has access to all levels of sensitivity within the scope of employee information.

1.3.6.2 ADMINISTRATION

Those individuals who administer Datapipe's office operations. As needed, these individuals may be granted access to Restricted data to facilitate their interaction with records, invoices and/or other documents, but are not specifically granted such access by default.

1.3.7 SERVICE DELIVERY MANAGEMENT

Oversees and directs all projects from contract to implementation, and provides clients with assistance in maintaining their Managed Services agreement. May receive access to a variety of Confidential or Restricted data (as each project requires), but do not possess any administrative rights. Service Delivery Management does not have access to financial records which may include cardholder data.

1.3.8 FINANCIAL TEAM

Those individuals responsible for handling all Datapipe finances. These individuals may have access to Confidential information in the form of credit card or other Datapipe client payment information (but not any cardholder information Datapipe clients traffic and/or store). These individuals do not possess administrative access.

1.3.9 MARKETING TEAM

Those individuals responsible for the promotion of the Datapipe name, logo and service commitment. These individuals have access to certain Restricted data, such as the access rights to administer the corporate web page.

1.3.10 SALES TEAM

Those individuals who directly work with prospective and current clients in defining contract specifications. These individuals have access to certain Confidential data, such as contract terms, client contact information and client billing information.

1.3.11 SOLUTION ARCHITECTURE

Architects of client solutions. May access contract terms, setup information and network architecture diagrams.

1.3.12 INVENTORY CONTROL

Those individuals responsible for ensuring that all Datapipe employees possess the equipment and resources required to perform all job functions. These individuals have access to Restricted shipping, receiving and inventory records.

1.3.13 DATA CENTER TECHNICIANS

Rack servers and network components and run cable. These individuals do not have access to Restricted or Confidential information.

1.3.14 STORAGE ADMINISTRATION

Configure backups and help maintain data integrity. These individuals have access to Restricted information needed only to administer and maintain databases.

1.3.15 BUSINESS OPERATIONS GROUP

These individuals maintain and administer Datapipe proprietary equipment and services and do not interact with any client information and services.

1.3.16 LEGAL

Creates and approves all contracts, waivers and agreements and thus has access to many types of Confidential information. Does not have administrative access.

1.3.17 INFORMATION SECURITY MANAGEMENT COMMITTEE

These individuals have access to Confidential Information Security Management Committee records for the purpose of information security management.

2 MEDIA PROCEDURES

2.1 GENERAL

A. A complete inventory of all client systems (which includes associated internal attached media) is maintained in Datapipe's Configuration Management Database (CMDB). However the type and classification of such data housed on client systems is not recorded by Datapipe. If applicable, client must implement their own data classification and labeling schemes for their data.

B. Offline storage media utilized for archival or back-up purposes will at all times be handled and retained in a secured environment such that only Datapipe personnel and contracted storage facility personnel have access to the archival media. Positive log-out and log-in of archive media will take place during all archive media transfers.

C. All media movement from one location to another shall be logged and authorized in a ticket as being transferred, by whom and to where and was it properly received.

D. All media, including removable media, that is no longer needed must either be destroyed or rendered unrecoverable. See Media Disposal for additional information.

E. Quarterly inventories of all stored media shall take place.

F. Precautions must be taken when utilizing removable media:

1. Staff may only use Datapipe supplied removable media in Datapipe systems.
2. Never connect personal removable media, or removable media of unknown origin, to any Datapipe system.
3. Information classified with a sensitivity level of Internal may be stored on removable media only when required in performance of your assigned duties.
4. Information classified with a sensitivity level of Restricted or Confidential shall not be stored on removable media without explicit permission by management.
5. When the business purpose has been satisfied, removable media containing non-Public information must be removed through secure deletion.
6. Any lost removable media must be immediately reported to the Security Team.

2.2 IDENTIFICATION AND DISTRIBUTION OF PAPER MEDIA

A. Access to secure electronic media is limited to access by least privileges required to perform job functions.

B. Datapipe does not routinely transport media of any sensitivity level offsite. However if necessary to do so, hardcopy media shall be sent via courier or secure other carrier service.

C. Confidential should not be sent electronically.

D. When sending Restricted information off the corporate network, employees must use proper precautions which include encryption utilizing utilities such as WinZip or PGP.

2.3 MANAGEMENT APPROVAL

A. Applicable TEAM LDR and Director-level management must remain aware of all secure media transported off site.

B. No secure media may be transported or otherwise distributed unless approved by management.

C. Shipping logs contain media transport details and are signed off upon by applicable managers.

2.4 STORAGE MECHANISMS

A. All electronic media files are accessible to permitted employees from any work station within the local area through the use of RDP.

B. All active electronic media files are kept current to Datapipe's current business operations. Datapipe maintains a public email folder accessible to all employees for non-sensitive electronic media that pertain, or could potentially pertain, to all departments.

C. All outdated electronic media are archived in said public folders for the client defined archival period, if applicable. All electronic media without archival period is stored indefinitely as "space" permits.

D. Hardcopy media are stored and labeled accordingly by those individuals responsible for their use. Hardcopy media are stored in file cabinets located in applicable employee's workspace. Lockable filing cabinets are available for secure hardcopy media storage. All media that contains cardholder data shall be stored in locked filing cabinets.

E. Periodically, applicable employees conduct inventory reviews for both electronic and hardcopy media storage locations. Such inventories involve ensuring that all required media are present and all antiquated, obsolete or otherwise irrelevant media are removed from active inventory.

F. When required, archival locations are established to store hardcopy media for the required period.

G. Periodic archive inventory reviews involve the removal of media that have reached their archival limit. Once removed, archived media are destroyed appropriately.

H. In the event of electronic or hardcopy media transfer, management and/or applicable on both ends of transfer shall sign off on transmission logs indicating shipment and receipt.

3 MEDIA DISPOSAL

3.1 SHREDDING

A. All hardcopy media that have been removed from the active inventory and have fulfilled relevant archival period are sent to the cross-cut shredder.

B. Media are placed into the shredder immediately unless the shredder is full or otherwise inoperable.

C. In the event of shredder inoperability, a locked storage container labeled, “To be Shredded” exists.

3.2 KILLDISK

For the deletion of obsolete information, Datapipe employs KillDisk technology. All hard drives are to be stored for two weeks after server decommissioning, and then securely wiped. If evidence of destruction is required, a support request must be made by the client before any server(s) are decommissioned by Datapipe.

According to the manufacturer:

"Active@KillDisk - Hard Drive Eraser is powerful and compact software that allows you to destroy all data on hard and floppy drives completely, excluding any possibility of future recovery of deleted files and folders... KillDisk conforms to US Department of Defense clearing and Sanitizing standard DoD5220.22-M..." (KillDisk.com)