DOCUMENT NO.	*SPP-1020*
DOCUMENT NAME	*DATAPIPE ORGANIZATIONAL SECURITY POLICY*

REVISION LEVEL	22
REVISION DATE	MARCH 5th, 2018
OWNER	DARREN COOK, DIRECTOR OF INFORMATION SECURITY

REVISION LEVEL	HISTORY	REVISION DATE
A	Initial Release	May 27th, 2008
B	Added Employee Termination Policy, Adjusted Scope, Added PINs to password policy Added explicit statements about client data	April 23rd, 2009
3	Updated to new template and new revision numbering convention Added Management Commitment section. Minor wording updates	June 1st, 2010
4	Additional details added to the Physical Security Policy. Updated Network Usage Policy to reflect new wireless configuration Minor updates to the Workstation Security Policy	July 21st, 2010
5	Added note at the end of 14.3.6. Added Steps for Compromised Entities, Section 14.4 Amended Policy of Section 15, stating that personal firewalls not required for employee mobile devices	August 25th, 2010
6	Updated badge identification and expiration policies stated in section 4.2	May 26th, 2011
7	Badge audit and expiration updated from a 12 month cycle to a 6 month cycle	January 19th, 2012
8	Detail credential groups and access review Added Section 12.3.3 on SSH Keys Mobile policy updated to refer to modern devices	May 17th, 2012
9	Updated WLAN policy	April 28th, 2013
10	Updated policy language to conform with industry standards and Datapipe policy	August 12th, 2013
11	Added Clean Desk Policy Added clause regarding employee understanding and adherence of regulatory and compliance requirements Added clause defining security's responsible to maintain a level of contact with applicable authorities	October 17th, 2013
12	Standardized definition Confidential Information. Updated Workstation Security Policy, Physical Security Policy, Encryption Policy, Instant Messenger Policy, Remote Access Policy, User Account Management, Mobile Device Protection Policy, and Special Access Agreement Created an Information Handling Policy and Backup Policy	November 12th 2013
13	Updated to reflect ticket requirement for Datapipe visitors and contractors	January 6th, 2014
14	Added in new Security Awareness Training Policy, additions to section 7.3 Unacceptable Activity Use	June 22nd, 2014
15	Added additional responsibilities under section 1.3 concerning department-specific policies and procedures	October 10th, 2014
16	Added third party remote access policy under Section 22, added system owner requirements to "Introduction" of section 20, edited Confidential Information definition in section 1.1	April 1st, 2015
17	Modified Section 9.3 to update encryption policy.	May 1st, 2015
18	Added new section 7 for Distributed Denial of Service Policy, all other sections numbers adjusted for this change. Added PMO responsibilities to section 1.3. Added screen-sharing prohibited activity to Section 8	August 21st, 2015
19	Added Section 24 – Vendor Management Policy, Changed CSO to CTSO, Minor text changes in section 15 and 16, Added data classification watermark to policy, Changes to sections 1 and 2 regarding new security awareness training process and LMS notes, Changes to Instant Messenger Policy – Section 11	March 8th, 2016
20	Section 8.1 C – added clarification regarding applicable laws for computer abuse Section 8.3 C – added examples of prohibited behavior Section 8.3 G – further defined "Internet browsing" Section 9.3.3 – clarified policy for monitoring of internal communication Section 10.3 B – provided guidance on encrypted communication via Datapipe One portal Section 11.3 – added notes regarding usage of ZeroBin Section 16.3 D – clarified mobile device security requirements	February 28th, 2017

21	Section 3.3 C – added policy for software installation on desktops/laptops Section 15.1 B – updated breach policy notification requirements for PCI DSS from v2.0 section 12.9 to v3.2 section 12.10 Section 16.3 F – added policy for mobile phone number retention for terminated users	September 19th, 2017
22	Changed owner to Director of Information Security Removed mentions of CTSO and COO and replaced with Director of Information Security and Operations Team Added Security Audit Team responsibilities to Section 1 Added Wireless Scan policy to section 6	March 5th, 2018

INTRODUCTION

PURPOSE AND SCOPE

This document details the procedures and policies required to maintain organizational security. Adherence to security policies and guidelines applies to ALL employees. This document details the procedures and policies required to maintain organizational and regulatory security compliance objectives. 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 in its possession. While Datapipe does not explicitly classify client data, it treats all client data as confidential.

RELATED DOCUMENTS

SPP-1011	Data Classification and Media Control Policy
SPP-1058	Defender – Self Service Portal Instructions
SC-1004	Token Authorization Form
SPP-1000	PCI Information Security Services Policy
HR-1006	Agreement Concerning Confidentiality, Competition and Certain Restrictions
SC-1005	Acknowledgement of Receipt of Standards of Conduct
HR-1021	Acknowledgement of Security Awareness Training Requirements
SPP-4.2.3	Control of Documents
SPP-1073	Access Control Policy – Logical

TERMS AND DEFINITIONS

RPO	Recovery Point Objective
RTO	Recovery Time Objective
RBAC	Role Based Access Control
LMS	Learning Management System

RESPONSIBLE PARTIES

SEC ENG	Security Engineer
NETWORK	Network Engineering
SUPPORT	Unix and Windows Support Teams
STOR ADMIN	Storage Admin
HR/Training	Human Resources/Training Team

1 SECURITY POLICIES – OVERVIEW

1.1 INTRODUCTION

A. Effective security is a team effort involving the participation and support of every Datapipe employee and affiliate who deals with information and/or information systems. It is the responsibility of every employee to understand and abide by these policies. These policies extend outside of normal working hours and beyond Datapipe owned or controlled premises, and continue in full force and effect subsequent to employment termination. For the purposes of this policy, the term "employee" includes any independent contractor or consultant who through the course of their relationship with Datapipe has access to Datapipe information and/or information systems.

B. The information that is stored by Datapipe is extremely valuable and is a prized target of hackers, criminals, and other miscreants. Datapipe shall make every reasonable effort to safeguard such data from being compromised. This policy document describes the importance and role of the employee in the security framework of Datapipe.

C. As an employee of Datapipe, it is of primary importance to protect the confidentiality and integrity of Confidential Information. This information can include but is not limited to:

1. Sensitive, proprietary company information such as trade secrets and intellectual property
2. Sensitive cardholder data including account numbers, names and addresses
3. Personally identifiable information such as social security numbers
4. Electronic protected health information
5. Government agency information
6. Encryption keys and system passwords

The compromise of such information could cause significant damage to the fiscal viability of Datapipe and permanently damage the reputation of the company and its employees. It is important to understand that if critical information is compromised either intentionally or unintentionally through neglect, it could result in disciplinary action including termination, as well as personal responsibilities for damages caused. It is therefore critical that each employee ensure that they are cognizant of the importance of client data and is diligent in the protection of Datapipe's critical information assets.

D. Any unauthorized copying, modifying, or destruction of client data is strictly prohibited.

E. Employee understanding and adherence to their obligations under regulatory standards ensures compliance to Datapipe policies and procedures. For additional information please reach out to a member of the security department. For your reference, standards / regulatory material for PCI, HIPAA/HITECH, Privacy Shield, U.S-Swiss Safe Harbor, and Datapipe's privacy policy can be found here:

PCI: https://www.pcisecuritystandards.org/security_standards/index.php

HIPAA/HITECH: http://www.hhs.gov/ocr/privacy/

Privacy Shield: https://www.privacyshield.gov/welcome

U.S.-Swiss Safe Harbor: http://2016.export.gov/safeharbor/swiss/

Datapipe's Privacy Policy: https://www.datapipe.com/legal/privacy_policy/

1.2 PURPOSE

To establish fundamental security guidelines, requirements and procedures that reduce risk and provide for the confidentiality, integrity, availability and privacy of Datapipe's information technologies and assets. The protection of information assets is mandatory for business, contractual, regulatory and legal reasons.

1.3 RESPONSIBILITIES

A. The Director of Information Security is responsible for establishing, maintaining, implementing, administering, and interpreting organizational security policies, standards, guidelines, and procedures. The Director of Information Security is also responsible for the proper enforcement of the activities detailed through this Organizational Information Security Policy ("Policy").

B. While responsibility for information systems security on a day-to-day basis is every worker's duty, specific guidance, direction, and authority for information systems security is centralized for all of Datapipe within the Security Department. This department will perform information systems risk assessments, prepare information systems security action plans, evaluate information security products, and perform other activities necessary to assure a secure information systems environment.

C. The Security Department with cooperation with other departments will be responsible for conducting investigations into any alleged computer or network security compromises, incidents, or issues. All significant compromises, or those posing the potential to be significant compromises, shall be immediately reported to the Director of Information Security.

D. The Security Audit Team manages all internal reviews, for both logical access (covered under SPP-1073) and quarterly reviews of security policies and operational procedures, which cover but are not limited to:

   a. Daily log reviews

   b. Firewall rule-set reviews

   c. Applying configuration standards to new systems

   d. Responding to security alerts

   e. Change management processes

   The results of reviews are provided to the Information Security Management Committee, and all other internal Information Security Management System policies govern this process.

E. System administrators, specifically the Support Team, Networking Managers, Business operations, and Storage administration managers are responsible for acting as local information systems security coordinators. These individuals are responsible for establishing appropriate user privileges, monitoring access control logs, reviewing and revoking access as necessary based on personnel departure or transfer, and performing similar security actions for the systems they administer. These activities should be performed at least annually or upon a notification from Human Resources/Training team. System administrators are responsible for reporting all suspicious computer and network-security-related activities to the Director of Information Security. System administrators are also responsible for implementing the requirements of this policy and other information systems security policies, standards, guidelines, and procedures.

F. All managers are responsible for ensuring any department policies and procedures conform to this policy and other published security policies and procedures. The Security department will obtain confirmation of this on a yearly basis via the Global Policy Acceptance Training contained in the designated Learning Management System (LMS) training platform.

G. All policies must be reviewed and approved by the ISC in accordance with our document management system. Security is represented on the ISC by Datapipe's Director of Information Security. Any department-specific procedures which could potentially impact the confidentiality, integrity, or availability of an information system must be submitted to Security department for review and approval prior to dissemination to department team members.

H. All employees are responsible for complying with this and all other Datapipe policies defining computer and network security measures. All employees are also responsible for bringing all known information security vulnerabilities and violations that they notice to the attention of the Security Department.

I. The Datapipe Security Department is solely responsible for maintaining contacts with relevant authorities, special interests groups, security forums and professional associations.

J. Datapipe's Service Delivery Managers (SDMs) provide Project Management services for both client environments and internal projects. For client environments, the solution architects (SAs) must gather security requirements from clients during the design and proposal phases. SAs must be trained by Security on the available security controls and operations, deployment options, and risks mitigated. This information must be passed to SDMs during the build phase. For internal projects, key stakeholders are required to engage security during the initial design phase. The deployment phase requires an internal server build workflow be approved by Operations and Security prior to the release of resources. The workflow captures the risk classification and any required security controls. For any projects which may have bypassed an initial security review, the deployment phase will be halted and no security approval will be received until a risk assessment can be performed.

1.4 PROPRIETARY AND CONFIDENTIAL INFORMATION

A. Due to the nature of Datapipe's business operations, there is a large potential for having proprietary information stored on or in Datapipe computers and processing resources. All information stored on or in Datapipe's processing and administrative systems is considered proprietary and confidential and is not to be released to any external entity without permission from appropriate Executive personnel.

B. Upon hiring, all employees shall read and sign, thereby indicating understanding, the Agreement Concerning Confidentiality, Competition and Certain Restrictions. This agreement as issued by the Human Resources Manager (HR MGR) identifies the proper control, ownership and repercussions for misuse of all proprietary and Confidential Information.

1.5 SECURITY INVESTIGATIONS

A. If during the course of regular duties, a Datapipe employee discovers evidence of a violation of this policy, said employee shall notify the Director of Information Security. If the Director of Information Security determines there is probable cause to believe a violation has occurred an additional investigation shall be authorized. The Director of Information Security or other designate of the Director of Information Security will perform any additional investigation.

B. If a member of the Support Team is requested to participate in an investigation of improper use committed by a client, or if Datapipe personnel notices evidence of improper use upon viewing a client's files (after receiving consent) during the normal course of job duties, that member of the Support Team shall be careful not to disclose information about that client or the contents of the client's files to others.

C. Information concerning the client shall only be disclosed to the Director of Information Security, or to a law enforcement agency as necessary. It is extremely important to keep a detailed record of all actions when investigating an allegation of improper use.

1.6 EMPLOYEE BACKGROUND VERIFICATION

A. All potential Datapipe employees undergo a pre-employment background check investigating criminal records, credit history and reference checks, to the extent that local law permits.

B. The Human Resources (HR) team collects relevant personal information from all new and potential employees and enters said information into the Automatic Data Processing Screening and Selection Services' (ADP) hire select system. ADP then conducts background checks based on the aforementioned criteria, generates a report and distributes said report back to the HR Team. HR retains a copy of said reports in each respective employee's personal file.

1.7 SECURITY POLICY REVIEW

Datapipe's security policies shall be reviewed at least annually. Any changes to this Policy will be approved by Datapipe Management in accordance with Datapipe's Control of Documents policy before distribution. If a Datapipe employee wishes to make a policy recommendation, the request must be submitted with the following information:

A. Describe the new or updated policy

B. Provide a reason or justification for new or updated policy and identify the risks of not implementing changes

C. List the major impacts of implementation, compliance, and enforcement (business or technical)

D. Identify the impacted stakeholders

E. Identify the dependencies for implementation of policy changes (i.e. project, regulatory, technology, or organization)

1.8 ENFORCEMENT

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of Datapipe's Information Resources access privileges, civil, and criminal prosecution.

1.9 MANAGEMENT COMMITMENT

Datapipe management is committed to ensuring the policies outlined in this document are followed, enforced, and ultimately embraced. Security is more than just a series of checkboxes and procedures, rather it is a culture. Management strives to cultivate this culture throughout all facets of Datapipe to help reduce risk and ensure the confidentiality, integrity, and availability of corporate assets.

2 SECURITY AWARENESS AND TRAINING

2.1 GENERAL SECURITY AWARENESS

All managers must continually strive to incorporate information security into training courses, internal newsletters, posters, and other tools and visual aids to increase information security awareness among all personnel.

2.2 SECURITY AWARENESS TRAINING PROGRAM

Datapipe administers a security awareness training program using a custom web-based learning management system (LMS). The program consists of courses selected on an annual basis by Datapipe management. Course selection is determined by business requirements and overall relevance of the course subject, as well as relevance to the employee's job function.

2.3 ANNUAL TRAINING REQUIREMENTS

All employees are required to complete any mandatory security awareness training courses selected for the current calendar year. Typically, each course contains a final exam, which requires a passing grade in order for the employee to receive credit for the course. All employees (with the exception of new personnel) will be given a two week grace period to complete their annual training courses and/or curriculum.

2.4 NEW PERSONNEL TRAINING

All new personnel must complete all required corporate training courses and/or curriculum which includes Security Awareness, and Global Policy Acceptance training programs within 7 days of the new hire start date. In addition, personnel will be provided this Policy and are required to sign the SC-1005 & HR-1021forms indicting they read, understood, and agree with the contents therein.

2.5 TRAINING ENFORCEMENT

Working with the HR/training department, the Security department is responsible for content associated with the administration of the Security Awareness training programs and policies. Failure of an employee to complete all mandatory Security Awareness training program requirements will result in escalation to the Senior Vice President of Human Resources and Administration. If an employee has not yet completed the required courses or actions within the allotted time frame, automated reminders from the LMS and/or Human Resources/Training or Security department are communicated via email. Should additional reminders be required, the Senior Vice President of Human Resources and Administration will be made aware of the issue and contact the employee and reporting manager directly.

3 WORKSTATION SECURITY POLICY

3.1 INTRODUCTION

Workstations and thin clients provide employees a desktop working environment for day to day business operations. These systems may have direct or indirect network access to sensitive internal or client Confidential Information.

3.2 PURPOSE

The purpose of this policy is to provide guidance for workstation security for Datapipe workstations in order to ensure the security of information on the workstation and information the workstation may have access to. Additionally, the policy provides guidance to ensure the requirements of the HIPAA Security Rule "Workstation Security" Standard 164.310(c) are met.

3.3 POLICY

Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of Confidential Information, and that access to Confidential Information is restricted to authorized users.

A. Employees using workstations shall consider the sensitivity of the information, including Confidential Information that may be accessed and minimize the possibility of unauthorized access.

B. Datapipe will implement physical and technical safeguards for all workstations that access Confidential Information to restrict access to authorized users.

C. Software installation on Citrix instances, laptops, and all other Datapipe-owned devices is restricted to Domain Administrators only. All requests for software installations should be submitted via ticket to the Business Operations Group for review.

D. Appropriate measures include at minimum:

1. Restricting physical access to workstations to only authorized personnel.
2. Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.
3. Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected.
4. Complying with all applicable password policies and procedures.
5. Ensuring workstations are used for authorized business purposes only.
6. Never installing unauthorized software on workstations.
7. Keeping food and drink away from workstations in order to avoid accidental spills.
8. Complying with the anti-malware policy.
9. Restricting access to removable media to limit data loss and malware infection.
10. Limiting administrative access to individuals based on business need and job function.

4 PHYSICAL SECURITY POLICY

4.1 INTRODUCTION

Datapipe will protect its information resources through implementation of sound physical, environmental, and administrative security controls designed to reduce the risk of physical failure of infrastructure components, damage from natural or fabricated environmental hazards, and use by unauthorized personnel.

4.2 POLICY

A. It is Datapipe's policy that individual employee badge access and departmental access roles will be audited semi-annually. Department managers will verify departmental role access via Datapipe's ticketing system. Badges will be valid for up to six months. If the individual has additional access beyond their departmental role access (Special Access), it must be re-authorized by an authorized party as defined in the security procedures. Expired badges with Special Access will have a 2 business day grace period for access to be verified. If access is equal to or less than their departmental role access, badge expiration will be extended for up to six months from date of verification.

B. Client and permanent contractor badges will also be valid for six months. However these badges may be allowed to expire before they are audited. In the event such a badge expires, the individual will need to consult the security officers. At this time the officers will validate that the client still has the appropriate colo_access rights or there is an associated ticket granting access renewal for contractors.

C. All Datapipe operated access control systems shall be monitored by for authentication success, failures, and alarms 24/7/365 by a third party security company. Access logs shall be retained for a period of three years. Additionally, Datapipe operated CCTV systems shall be monitored by the same security company for suspicious activity 24/7/365. The video coverage and retention times may vary between facilities.

D. If a breach is discovered or suspected, the employee shall immediately report the incident through the appropriate chain of management. This includes contacting the onsite security officer, your immediate manager, Data Center Operations manager, and the Director of Information Security. Any and all suspicious activity must be immediately reported. See section on Incident Management.

E. Access to the datacenter is highly restricted. Only employees with a need to access the datacenter are given access. Specifically, all physical access (smartcards and keys) shall be authorized and will only be granted to areas required for job functions. If you see employees or other individuals in a restricted area of the facility without a proper escort or badge, report it immediately.

F. All visitors and contractors must sign-in the appropriate log book. The log will contain at minimum, the visitor's name, their company, and the employee authorizing physical access. Access logs will be reviewed monthly by the Datapipe Security Department.

G. Access requests for visitor, contractor, vendor and personal guests to a Datapipe facility require a Datapipe One ticket. **Note: Ticket exceptions can be made on a case by case basis at the discretion of the local Data Center Operations Manager or by senior management.**

H. Personal guest access outside of the hours of 7:00AM to 7:00PM local facility time must be approved by management through a Datapipe One ticket prior to the visit.

I. Personal guests are only allowed to access employee common areas. Under no circumstances are personal guests allowed to enter any restricted areas such as colocation rooms, MDF rooms, or mechanical rooms.

J. All visitors and personal guests must be escorted by a Datapipe Employee at all times.

K. Datapipe equipment, which has not been expressly issued to you, shall not be taken off-site without prior management approval.

4.2.1 ID BADGES

Individuals must present government issued identification prior to Datapipe badge issuance. If Datapipe provides you with a color-coded ID badge with photo, that badge is to be worn at all times while in a Datapipe facility so you can be easily identified.

4.2.2 KEYS AND KEYCARDS

It is important that security is maintained in all Datapipe facilities at all times. If you are provided with a key, verify that the key is with you at all times and that nobody else has access to it. The key is for your individual only. If you lose your key, report this to your supervisor immediately.

4.2.3 NO PIGGYBACKING

Datapipe's policy states that unauthorized personnel must not be allowed access to Datapipe's facilities. When entering or exiting a secure doorway, verify that the door is closed behind you. Do not hold the door open for other parties.

4.2.4 FIRE DRILLS

Above all material, informational and financial resources, Datapipe considers human life to be the most important asset. As such, we shall conduct yearly fire drills in all locations. Employees must treat any instance of a sounding fire alarm as an actual fire emergency.

5 MEDIA CONTROL POLICY

5.1 INTRODUCTION

This policy details the control methods for media required to maintain the highest possible level of information security.

5.2 PURPOSE

A. This policy shall define and classify critical systems and data, and specify which departments may access said systems and data as a part of their job function.

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

5.3 POLICY

Please refer to SPP-1011, Data Classification Media Control Policy document for media control policies and procedures for the following:

A. Data Control

B. Media Inventory Procedures

C. Media Disposal

D. Backup Media

6 NETWORK USAGE POLICY

6.1 INTRODUCTION

This policy details local access connections to the Datapipe network.

6.2 PURPOSE

The purpose of this policy is to define the restrictions to connecting to Datapipe's wired and wireless networks.

6.3 POLICY

The following network activities are prohibited on Datapipe's LAN or WLAN.

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

B. Port scanning or security scanning is expressly prohibited unless required or requested as part of a Datapipe hosting solution.

C. Executing any form of network monitoring which will intercept data not intended for the employee or client unless this activity is a part of the employee's normal job/duty.

D. It is prohibited to setup rouge access points or to utilize wireless ad-hoc networks.

6.3.1 LAN (WIRED) NETWORK USAGE

It is prohibited to connect any unauthorized network device to any Datapipe Ethernet port including but not limited to the Data Center, Office, and lab environments. Within Datapipe offices, Port Security will restrict unauthorized MAC addresses. In the event an unauthorized MAC address is connected to the LAN the Ethernet port will automatically be disabled. Escalate all occurrences to the Business Operations Group.

6.3.2 WLAN (WIRELESS) NETWORK USAGE

A. Datapipe employees are allowed to use their wireless devices to connect to the Datapipe WLAN. This network is WPA2 encrypted, MAC address restricted, and does not broadcast its SSID. The wireless network provides standard Internet access with no privileges into any trusted network. In order to access internal resources, employees must VPN, requiring 2-factor authentication. This VPN only permits access to Datapipe employee jumphosts, and no direct access to client networks. See section 11.

B. In addition to the employee network, the ‘Datapipe Wireless’ access points are available to approved visitors of the Datapipe facilities. Datapipe wireless requires a username and password to authenticate to these access points. Once authenticated, Internet-only access permitted, and the accounts are revoked after 24 hours. Datapipe wireless is completely segregated from all Datapipe network resources.

C. In both cases, Datapipe wireless networks do not have access to internal resources, client networks, or a part of Datapipe or client Cardholder Data Environment (CDE).

D. Datapipe completes scans for rogue wireless points in its datacenters on a quarterly basis. Datacenter technicians scan the facility using a Wi-Fi scanner application (e.g. inSSIDer) and provide the scan results to the Security department. If an unauthorized wireless access point is discovered, the incident response plan noted in section 15 of this document will take effect.

7 DISTRIBUTED DENIAL OF SERVICE (DDOS) POLICY

7.1 INTRODUCTION

This policy details the implementation and applicability of the Datapipe DDoS mitigation architecture on its network.

7.2 PURPOSE

The purpose of this policy is to define expectations on how DDoS attacks are mitigated and the availability of managed services to help Clients improve their resiliency against attacks.

7.3 POLICY

Datapipe deploys Arbor Networks DDoS detection and mitigation technology to applicable on-premises edge networks to provide active protection against DDoS attacks.

A. The Datapipe Arbor footprint is applicable to internal Datapipe networks only and doesn’t include Client networks.

B. A Client experiencing a DDoS attack can request Arbor protection to mitigate a real time attack or for the prevention of a known potential targeted attack.

C. Arbor protection can be requested no more than three times during the lifecycle of a Client solution at Datapipe.

D. Datapipe reserves the right to disable requested Arbor protection at any time.

E. If an attack is cross impacting other Datapipe Clients, Datapipe reserves the right to black hole Client traffic.

F. Datapipe recommends Clients improve their resiliency against DDoS attacks by electing Datapipe’s Cloud WAF and DDoS network protection service or a 3rd party service that meets Client requirements.

G. Datapipe’s policy on its Cloud WAF and DDoS protection service is available via SPP-1000, PCI Information Security Services Policy.

8 PROHIBITED ACTIVITY POLICY

8.1 INTRODUCTION

A. The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

B. Under no circumstances is an employee of Datapipe authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Datapipe-owned resources.

C. Datapipe IT systems and accounts are to be used only for the purpose for which they are authorized and are not to be used for non-Datapipe related activities. Unauthorized use of a Datapipe account and/or system is a violation of applicable local and international computer abuse and fraud laws. Therefore, unauthorized use of Datapipe IT computing systems and facilities may constitute grounds for dismissal and either civil or criminal prosecution.

8.2 PURPOSE

The purpose of the policies below is by no means exhaustive, but attempts to provide a framework for activities which fall into the category of unacceptable use.

8.3 POLICY

Unacceptable Activity Use includes the following:

A. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Datapipe.

B. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Datapipe or the end user does not have an active license is strictly prohibited.

C. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. This would include but is not limited to: software licenses, proprietary encryption keys/algorithms, source code, or system builds/network diagrams. The appropriate management should be consulted prior to export of any material that is in question.

D. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.).

E. Revealing your account password to others or allowing use of your account by others.

F. Using a Datapipe computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

G. Internet browsing (perusal of websites for research or on a casual basis) from any other computer except for those assigned for employee use (e.g. AppBoxes, Citrix, MacMini, LTSP, or employee assigned laptops and desktops). Datacenter laptops and any other Datapipe management systems/servers must not be used for internet browsing.

H. Making fraudulent offers of products, items, or services originating from any Datapipe account.

I. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

J. Circumventing user authentication or security of any host, network or account.

K. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

L. Providing any information about Datapipe employees to parties outside of the Datapipe Community.

M. Users shall not make copies of system configuration files for their own, unauthorized personal use or to provide to others.

N. Users shall not download, install or run security programs or utilities that reveal weaknesses in the security of any system. For example, Users shall not run password-cracking programs, “network sniffer” utilities or other sleuthing or tracing programs on Datapipe IT computing systems.

O. Creating “reverse tunnels” in order to allow remote connections to Datapipe’s internal networks which bypass perimeter security protections. This includes technologies and protocols such as SSH, TeamViewer, and GotoMyPC

P. While use of screen-sharing sessions is permitted, Confidential Information must not be disclosed to clients or any other parties. Applications with Confidential Information that could be visible during screen sharing (i.e. full desktop sharing) should be closed or minimized.

Q. Storing personal content on company-provided file storage and collaboration platforms or on the company intranet is strictly prohibited.

9 EMAIL USE POLICY

9.1 INTRODUCTION

The Datapipe email systems are used to allow effective communication between employees, clients, and business associates. Email transmission over the internet is inherently insecure and subject to security breaches that include message interception, message alteration, and spoofing. Users of the Datapipe email systems should not assume the confidentiality or integrity of any message that is sent or received via the Internet.

9.2 PURPOSE

The purpose of this policy is to define appropriate and inappropriate use of the Datapipe email system.

9.3 POLICY

9.3.1 PROHIBITED USE

The Datapipe email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin, as well as Confidential Information. Employees who receive any emails with this content from any Datapipe employee should report the matter to their supervisor immediately.

9.3.2 PERSONAL USE

Using a reasonable amount of Datapipe resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work-related email. Sending chain letters or joke emails from a Datapipe email account is prohibited.

9.3.3 MONITORING

Datapipe reserves the right to retrieve the contents of messages for the purposes of monitoring; whether the use of the email system is legitimate, to retrieve lost messages due to computer failure, to assist in the investigation of wrongful acts or to comply with any legal obligation.

9.3.4 DISCLAIMERS

Datapipe mail servers have been configured to automatically append disclaimer language to all outgoing emails. Using any other disclaimer language except the approved legal language is strictly prohibited.

10 ENCRYPTION POLICY

10.1 INTRODUCTION

Encryption is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

10.2 PURPOSE

The purpose of this policy is to enforce a standard that limits the use of encryption techniques to only Datapipe approved algorithms and utilities which will securely transmit sensitive data to ensure confidentiality and integrity of confidential information over the internet.

10.3 POLICY

A. Datapipe deploys strong cryptography based on industry-tested and accepted algorithms, along with strong key lengths and proper key-management practices. Cryptography includes both encryption (which is reversible) and hashing (which is not reversible, or "one way"). SHA-256 is an example of an industry-tested and accepted hashing algorithm. Examples of industry-tested and accepted standards and algorithms for encryption include AES (128 bits and higher), TDES (Triple-length keys), RSA (2048 bits and higher), ECC (256 bits and higher), and ElGamal (2048 bits and higher).

B. Sensitive customer data must not be sent unencrypted over the Internet. When sending such data via Datapipe One, the Datapipe Encryption Page must be utilized, as described further in the Datapipe One training material. Confidential data includes but is not limited to the following:

1. IP Addresses (Which includes both Public and Private IP Addresses)
2. System Credentials (Username and Passwords)
3. Customer Account Information
4. Network Diagrams
5. Encryption and Decryption keys
6. Cardholder Information

C. Datapipe systems transmitting Confidential Information over the Internet shall use strong cryptography.

- Datapipe shall perform a risk assessment on a case-by-case basis to determine if transmission of Confidential Information over internal networks requires protection via strong cryptography.

D. Datapipe shall adhere to legal, contractual, and compliance requirements for encryption, including but not limited to:

1. Encryption of Datapipe Confidential Information at rest.
   - Datapipe shall perform a risk assessment on a case-by-case basis to determine if other Datapipe Confidential Information, not otherwise governed by legal, contractual, or compliance requirements, shall be encrypted at rest.
2. Restrictions on usage and import/export of hardware and software for performing cryptographic functions.

E. Specific policies detailing the requirement for encryption of certain data, or under certain conditions shall prevail.

11 INSTANT MESSAGING POLICY

11.1 INTRODUCTION

The use of Instant Messaging and IRC systems, also known as Chat is a form of real-time communication between two or more people based on typed text. Instant messaging and IRC are a critical part of Datapipe internal communication system. It is important to understand the acceptable use of this technology in the Datapipe environment.

11.2 PURPOSE

Instant Messaging and IRC is limited to the capabilities provided by Datapipe on internal network systems. All employees must use the Instant Messaging and IRC service provided in a manner that protects company assets and confidential Information.

11.3 POLICY

Datapipe leverages Slack and IRC as internal communication mediums. Employees should be logged into Slack throughout their workday and optionally IRC. This will allow other employees to know you are in the office and they can communicate with you instantly. You are encouraged to use these conferences to communicate with employees in your department.

Please note that sending unencrypted confidential information via instant messaging is strictly prohibited. Users must utilize ZeroBin in order to encrypt the data before transmitting it via instant messaging. Any users who require assistance with using ZeroBin must contact the Security department. Further information regarding ZeroBin and its use can be found here: https://datapipe.box.com/ZeroBin-FAQ

12 REMOTE ACCESS POLICY

12.1 INTRODUCTION

Remote access allows employees to connect to Datapipe application servers so they may continue to work when outside the Datapipe facilities.

12.2 PURPOSE

The purpose of this policy is to define standards for connecting to Datapipe's network from any host outside the Datapipe network (e.g. mobile or employee owned computers). These standards are designed to minimize the potential exposure to Datapipe from damages which may result from unauthorized use of Datapipe's resources. Damages include the loss of sensitive or company Confidential Information, damage to public image, damage to critical Datapipe internal systems, etc.

12.3 POLICY

A. All employees possessing a security token will be allowed to remotely connect to Datapipe application servers to work from outside the Datapipe facilities. No external computers (e.g. mobile devices or employee owned computers) can connect directly to client solutions.

B. Employees may utilize VPN, or Citrix virtual desktops to work remotely.

C. Once an employee is authenticated via VPN, employees will be restricted to their application servers to which they normally have access.

D. Utilizing a security token ensures two-factor authentication when VPN'ing into Datapipe's network, connecting to a virtual desktop, or logging in to Datapipe's Single Sign On for ticket access. A Personal Identification Number (PIN) combined with the One Time Password (OTP) generated by the token, serves as the employees password when authenticating to these systems.

13 PASSWORD POLICY

13.1 INTRODUCTION

A. In computing, a password is a word or string of characters, entered, often along with a user name, into a computer system to log in or to gain access to some resource. Passwords are a popular form of authentication. Full security requires that the password be kept.

B. The length, complexity, and secrecy of a password are vital to prevent compromise.

13.2 PURPOSE

The purpose of this policy is to identify the characteristics of strong passwords and use them accordingly.

13.3 POLICY

A. It is the policy of Datapipe that everyone be aware of how to select strong passwords. Poor, weak passwords have the following characteristics:

  1. The password contains less than eight characters
  2. The password is a word found in a dictionary (English or foreign)
  3. The password is a common usage word such as:
     - a. Names of family, pets, friends, co-workers, fantasy characters, etc.
     - b. Computer terms and names, commands, hardware, software.
     - c. The company name (Datapipe), city, street or any other unique company indicator.
     - d. Birthdays and other personal information such as addresses and phone numbers.
     - e. Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
     - f. Any of the above spelled backwards.
     - g. Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

B. Strong passwords have the following characteristics:

  1. Contain both upper and lower case characters (e.g., a-z, A-Z)
  2. Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
  3. Are at least eight alphanumeric characters in length.
  4. Are not words in any language, slang, dialect, jargon, etc.
  5. Are not based on personal information, names of family, etc.

C. Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation. NOTE: Do not use either of these examples as passwords!

13.3.1 PASSWORD PROTECTION STANDARDS

A. Do not use the same password for Datapipe accounts as for other non-Datapipe access (e.g., personal ISP account, option trading, benefits, etc.).

B. Where possible, don't use the same password for various Datapipe access needs. For example, select one password for the special access (administrative) and a separate password for screensaver.

C. Do not share Datapipe passwords with anyone. All passwords are to be treated as Sensitive Datapipe information.

D. Additional Password "Don'ts:"

   1. Don't reveal a password over the phone to ANYONE
   2. Don't reveal a password in an email message
   3. Don't reveal a password to your team manager
   4. Don't talk about a password in front of others
   5. Don't hint at the format of a password (e.g., "my family name")
   6. Don't reveal a password on questionnaires or security forms
   7. Don't share a password with family members
   8. Don't reveal a password to co-workers while on vacation

E. If someone demands a password, refer them to this document or have them call someone in the Security Department.

F. Do not use the "Remember Password" feature of applications (e.g., Internet Explorer and Firefox)

G. Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

H. If an account or password is suspected to have been compromised, report the incident the Director of Information Security and change all passwords.

I. Password cracking or guessing may be performed on a periodic or random basis by the Director of Information Security or his/her delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

J. Recommended password encryption storage programs are KeePass and Password Agent.

13.3.2 PIN SELECTION STANDARDS

A. Numbers should always be used when available.

B. Avoid ascending and descending number sequences

C. Avoid common dates such as birthdays and other personal information.

13.3.3 SSH KEYS

SSH Keys from your home machines are not permitted.

14 USER ACCOUNT MANAGEMENT

14.1 INTRODUCTION

Computer accounts are the means used to grant access to Datapipe's Information Resources. These accounts provide a means of providing accountability, a key to any computer security program, for Information Resources usage. This means that creating, controlling, and monitoring all computer accounts is extremely important to an overall security program.

14.2 PURPOSE

The purpose of this policy is to establish the rules for the creation, monitoring, control and removal of user accounts.

14.3 POLICY

A. Users shall sign the Agreement Concerning Confidentiality, Competition and Certain Restrictions (HR-1006) and Acknowledgement of Organizational Security Policy (SC-1005) prior to being issued a user ID permitting access to Datapipe systems.

B. All accounts created must have an associated request and approval that is appropriate for the Datapipe system or service.

C. First time account passwords must be a random password with "reset password on next logon" checked.

D. All internal accounts must be uniquely identifiable using the assigned user name or individuals using a shared account must be identifiable via other means ensuring user accountability.

E. All default passwords for accounts must be constructed in accordance with the Datapipe Password Policy.

F. All non-role accounts must require passwords to be changed every 90 days.

G. Accounts of individuals on extended leave (more than 30 days) will be disabled.

H. All new user accounts that have not been accessed within 30 days of creation will be disabled.

I. All role accounts / service accounts which are set to not expire must meet the password complexity requirements and have a minimum length of 16 characters.

J. Business Operations Group or other designated staff:

1. Are responsible for removing the accounts of individuals who change roles within Datapipe, or are separated from their relationship with Datapipe.
2. Must have a documented process to modify a user account to accommodate situations such as name changes, accounting changes and permission changes.
3. Must have a documented process for periodically reviewing existing accounts for validity.
4. Are subject to independent audit review.
5. Must provide a list of accounts for the systems they administer when requested by authorized Datapipe management.
6. must cooperate with authorized Datapipe management investigating security incidents

14.3.1 ACCESS BY LEAST PRIVILEGE

Access privileges are granted to Datapipe employees based on departmental role. Roles have been granted the least privilege necessary to perform their job function. See Access Control Policy - Logical for additional information.

15 INCIDENT RESPONSE PLAN

15.1 INTRODUCTION

A. Computer security incident handling can be divided into six phases: preparation, identification, containment, eradication, recovery, and follow-up. Understanding these stages, and what can go wrong in each, facilitates responding more methodically and avoids duplication of effort.

B. In the event of a suspected or confirmed breach of client data is detected by Datapipe, the client will be notified without unreasonable delay in accordance with the procedures outlined in their Server Escalation Action Plan (SEAP) and Datapipe's Incident Response Plan. Note that Datapipe will not perform a risk assessment to determine if notification should be made to client. Rather, Datapipe will in all circumstances notify the client of an actual or suspected breach. Client may then need to perform a risk assessment, taking into account the type and quantity of data which was breached to determine if they need to notify any individuals whose information was breached in accordance with client's internal policies and/or local or federal regulations. Additionally, Datapipe will not inspect client data (such as records within a database) nor perform a forensic investigation, but will work with its clients and 3rd party auditors/investigators to aid them in any way reasonably necessary. This breach notification policy conforms with notification requirements of PCI DSS v3.2 section 12.10, and HIPAA §164.410

C. The six phases:

1. Phase 1: Preparation
2. Phase 2: Identification
3. Phase 3: Containment
4. Phase 4: Eradication
5. Phase 5: Recovery
6. Phase 6: Follow-up

15.2 EMERGENCY ACTION CARD

A. One part that is especially useful for companies that are unprepared, but face an incident, is called the Emergency Action Card. It offers at simple prescription for what to do if you find yourself in that unpleasant situation.

B. When a computer security incident occurs, and you are not prepared, follow these ten steps.

15.2.1 EMERGENCY STEP 1 - REMAIN CALM

Even a fairly mild incident tends to raise everyone's stress level. Communication and coordination become difficult. Your calm can help others avoid making critical errors.

15.2.2 EMERGENCY STEP 2 - TAKE GOOD NOTES

Use the forms in the back of this (Incident Handling: Step-by-Step) guide. Start with the one titled "Incident Identification." Then work your way through the others that are relevant. As you complete the forms, keep in mind that your notes may become evidence in court. Make sure you answer the four Ws - Who, What, When, and Where- and, for extra credit, How and Why. You may find a small hand-held tape recorder to be a valuable tool.

15.2.3 EMERGENCY STEP 3 - NOTIFY THE RIGHT PEOPLE AND GET HELP

Begin by notifying your security coordinator and your manager and asking that a coworker be assigned to help coordinate the incident handling process. Get a copy of the corporate phonebook and keep it with you. Ask your helper to keep careful notes on each person with whom he or she speaks and what was said. Make sure you do the same.

15.2.4 EMERGENCY STEP 4 - ENFORCE A "NEED TO KNOW" POLICY

Tell the details of the incident to the minimum number of people possible. Remind those individuals, where appropriate, that they are trusted individuals and that your organization is counting in their discretion. Avoid speculation except when it is required to decide what to do. Too often the initial information in an incident is misinterpreted and the "working theory" has to be scrapped.

15.2.5 EMERGENCY STEP 5 - USE OUT-OF-BAND COMMUNICATIONS

If the computers may have been compromised, avoid using them for incident handling discussions. Use telephones and faxes instead. Do not send information about the incident by electronic mail, talk, chat, or news; the information may be intercepted by the attacker and used to worsen the situation. When computers are being used, encrypt all incident-handling email.

15.2.6 EMERGENCY STEP 6 - CONTAIN THE PROBLEM

Take the necessary steps to keep the problem from getting worse. Usually that means removing the system from the network, though management may decide to keep the connections open in an effort to catch an intruder.

15.2.7 EMERGENCY STEP 7 - MAKE A BACKUP OF THE AFFECTED SYSTEM(S) ASAP

Use new, unused media. If possible make a binary or bit-by-bit backup.

15.2.8 EMERGENCY STEP 8 - GET RID OF THE PROBLEM

Identify what went wrong if you can. Take steps to correct the deficiencies that allowed the problem to occur.

15.2.9 EMERGENCY STEP 9 - GET BACK IN BUSINESS

After checking your backups to ensure they are not compromised, restore your system from backups and monitor the system closely to determine whether it can resume its tasks.

15.2.10EMERGENCY STEP 10 - LEARN FROM THIS EXPERIENCE

Mitigate the possibility of getting caught unprepared the next time an incident occurs. This incident response plan is designed to help you by proving a systematic approach to incident handling.

15.3 PLAN

15.3.1 PHASE 1 - PREPARATION

In the heat of the moment, when an incident has been discovered, decision-making may be haphazard. The following steps should be taken in the preparation phase:

A. Monitor and analyze the network traffic, assess vulnerabilities and permissions, look at server history in MyDatapipe for previous compromises.

B. Review client SEAP

C. Notify managed representative (if applicable) and security team when an incident occurs.

15.3.2 PHASE 2 - IDENTIFICATION

Identification involves determining whether or not an incident has occurred, and if one has occurred, determining the nature of the incident. The following steps should be taken in the identification phase:

A. Assign a person to be responsible for the incident.

B. Determine whether or not an event is actually an incident. Check for simple mistakes such as errors in system configuration or an application program, hardware failures, and most commonly, user or system administrator errors.

C. Identify and assess the evidence in detail and maintain a chain of custody. Control access to the evidence.

D. Notify appropriate officials such as immediate supervisors or the security department.

15.3.3 PHASE 3 - CONTAINMENT

During this phase the goal is to limit the scope and magnitude of an incident in order to keep the incident from getting worse. The following steps should be taken in the containment phase:

A. Check client SEAP for client specific containment plan.

B. Keep a low profile. Avoid looking for the attacker with obvious methods.

C. Avoid potentially compromised code. Intruders may install malware and similar malicious code in system binaries.

D. If appropriate, back up the system. It is important to obtain a full back up of the system in order to acquire evidence of illegal activity. Determine the risk of continuing operations.

E. Change passwords on compromised systems and on all systems that regularly interact with the compromised systems.

F. If appropriate, restrict network activity.

15.3.3.1 LOGICAL SECURITY INCIDENT

If a system is suspected of being compromised, please follow customer SEAP and Compromised Server Training Guide.

15.3.3.2 PHYSICAL SECURITY INCIDENT

If a physical security incident is detected, please escalate immediately to security officers or the Datapipe Security Department.

15.3.4 PHASE 4 - ERADICATION

This phase ensures that the problem is eliminated and vulnerabilities that allow re-entry to the system are eliminated. The following steps should be taken in the eradication phase:

A. Isolate the attack and determine how it was executed.

B. Implement protection techniques as those documented in the Datapipe Security Services Policy Document as appropriate.

C. If appropriate, perform vulnerability analysis.

D. Remove the cause of the incident.

E. If available, locate the most recent clean back up (to prepare for system recovery).

15.3.5 PHASE 5 - RECOVERY

This phase ensures that the system is returned to a fully operational status. The following steps should be taken in the recovery phase:

A. If appropriate, restore the system if backups exist.

B. Validate the system. Once the system has been restored, verify that the operation was successful and the system is back to its normal condition.

C. Decide when to restore operations. Management and/or client may decide to leave the system offline while operating system upgrades and patches are installed.

D. Monitor the systems. Once the system is back on line, continue to monitor for back doors that escaped detection.

15.3.6 PHASE 6: FOLLOW-UP

A. This phase is important in identifying lessons learned that will prevent future incidents.

1. Develop a detailed incident report and provide copies to managed representative (if applicable), client, and enter it into MyDatapipe for tracking.
2. Send recommended changes to client.
3. Implement approved actions.

B. In the event that an incident investigation require s law enforcement agencies, the Datapipe security team should be contacted immediately to ensure the process is handled as required by the agency

C. Solutions that contain card holder data that are suspected of being compromised must take action immediately to help prevent additional exposure. The customer of Datapipe that is processing, storing, or transmitting card holder data must contact the card brands for a forensic investigation. Failure to notify the card brands can result in fines.

15.4 STEPS FOR COMPROMISED ENTITIES

A. Immediately contain and limit the exposure. Prevent further loss of data by conducting a thorough investigation of the suspected or confirmed compromise of information. To preserve evidence and facilitate the investigation:

1. Do not access or alter compromised systems (i.e., don't log on at all to the machine and change passwords, do not log in as ROOT).
2. Do not turn the compromised machine off. Instead, isolate compromised systems from the network (i.e., unplug cable).
3. Preserve logs and electronic evidence.
4. Log all actions taken.
5. If using a wireless network, change SSID on the AP and other machines that may be using this connection with the exception of any systems believed to be compromised.
6. Be on "high" alert and monitor all systems with cardholder data.

B. Alert all necessary parties immediately. Be sure to contact:

1. Your internal information security group and incident response team.
2. Your merchant bank.
3. If you do not know the exact name and/or contact information for your merchant bank, notify Visa Fraud Investigations and Incident Management group immediately at (650) 432-2978.
4. Your local office of the United States Secret Service.

C. Provide all compromised Visa, Interlink, and Plus accounts to your merchant bank within 10 business days. All potentially compromised accounts must be provided and transmitted as instructed by your merchant bank and Visa Fraud Investigations and Incident Management group. Visa will distribute the compromised Visa account numbers to Issuers and ensure the confidentiality of entity and non-public information.

D. Within 3 business days of the reported compromise, provide an Incident Report document to your merchant bank. **NOTE**: Visa, in consultation with your merchant bank, will determine whether or not an independent forensic investigation will be initiated on the compromised entity.

16 MOBILE DEVICE PROTECTION POLICY

16.1 INTRODUCTION

Implementing mobile device protection greatly reduces the risk of sensitive data being exposed if an unauthorized person had the mobile device in their possession.

16.2 PURPOSE

The purpose of this policy is to describe the Information Security requirements for protecting data at rest on Datapipe mobile devices.

16.3 POLICY

A. All mobile devices containing Datapipe Confidential Information must use an approved method of encryption to protect data at rest. Mobile devices are defined to include laptops, smartphones, and tablets.

B. Users are expressly forbidden from storing Datapipe data on devices that are not issued by Datapipe, such as storing Datapipe email on a personal smartphones or laptops.

C. Users are expressly forbidden from storing any client data on any Datapipe mobile device. It also prohibited to utilize any software which relays Datapipe credentials to a third party. For example, instant messengers on smartphones with proxy connections.

D. Datapipe issued mobile devices shall maintain active and up to date operating system and application patches. Laptops shall also maintain active and up to date antivirus and personal firewalls. **NOTE**: Exceptions for antivirus deployment, based on Operating System, must be approved by the Director of Information Security.

E. Mobile devices and media taken offsite shall not be left unattended in public places.

F. Regarding users who were issued Datapipe smartphones: please be aware upon employment/contract termination, Datapipe is under no obligation to release the mobile phone number that was associated with the smartphone back to the user. This includes personal numbers that were ported over into the Datapipe mobile device program. Exceptions may be made to this policy as per management's discretion, and the user may be authorized to retain the mobile number they were issued. Please take this under consideration before porting over your personal mobile phone number.

16.3.1 SMARTPHONES AND TABLETS

Any smartphone or tablet that contains Datapipe information must have a security policy to auto lock after inactivity and wipe the device after 10 unsuccessfully password attempts. The password or PIN used to lock the mobile device must also adhere to Datapipe's password policy.

16.3.2 LOSS AND THEFT

The loss or theft of any mobile device containing Datapipe data must be reported immediately.

17 CLIENT VERIFICATION POLICY

17.1 INTRODUCTION

Datapipe customer verification page provides several different ways to verify an unknown caller's identity before continuing.

17.2 PURPOSE

The purpose of this policy is to define a standard on how employees verify an individual's identity before disclosing any information.

17.3 POLICY

A. Datapipe policy states that Confidential Information about clients cannot be disclosed to unauthorized parties. It is required to verify the identity of the caller before providing support or disclosing Confidential Information. Datapipe has a customer validation tool.

B. This tool allows for employees to validate customer information before disclosing any information or taking any actions on a customer's devices. It is prohibited provide information to an unrecognized caller without validating them first.

17.3.1 PIN ON CUSTOMER ACCOUNT

For added security, some customers require that a PIN be provided when someone calls in for support or questions about that account. When that customer's record is pulled, you will receive a message to ask the caller to verify their PIN. Only provide information to a customer if they confirm the correct PIN.

17.3.2 SOCIAL ENGINEERING

Many unscrupulous individuals may try to use a tactic called 'social engineering' in an attempt to convince you to inadvertently provide sensitive information such as employee data, business operating models, passwords and other data. Many times, the information they will pursue appears innocuous and irrelevant. When compiled however, this information provides significant information for criminals to access the systems and infrastructure of Datapipe. For this reason, no information shall be shared with anyone who is not identified as working with the company or authorized via the methods above. Any questions related to the verification of such individuals shall be directed to immediate supervisor. Do not freely offer information related to the operations, personnel, or business of Datapipe.

18 EMPLOYEE TERMINATION

18.1 INTRODUCTION

It is necessary for prompt and complete revocation of a terminated employee's access and company owned assets to address the associated risk of interacting with company resources post termination.

18.2 PURPOSE

To ensure proper termination procedures are performed in a timely manner.

18.3 POLICY

In the event of a terminated employee, department managers must be notified, access to any Datapipe resource must be immediately revoked, and all company-owned property must be dispossessed. The Datapipe Human resources department is responsible for collecting all company-owned property such as mobile devices, tokens, keys, access cards, and notifying department managers before the terminated employee is escorted out of the Datapipe facility. Immediately after receiving a terminated employee notification, responsible parties shall revoke all facility, computer, network, and data access from said employee.

19 CLEAN DESK POLICY

19.1 INTRODUCTION

An effective clean desk effort involving the participation and support of all Datapipe employees can greatly protect paper documents that contain sensitive information about our clients, customers and vendors.

19.2 PURPOSE

To reduce the threat of a security incident as Confidential Information will be locked away when unattended and to provide a positive image for visitors.

19.3 POLICY

A. Allocate time in your calendar to clear away your paperwork.

B. Always clear your workspace before leaving for longer periods of time.

C. If in doubt - throw it out. If you are unsure of whether a duplicate piece of sensitive documentation should be kept - it will probably be better to securely destroy it.

D. Consider scanning paper items and filing them electronically in your workstation.

E. Use the Code Shred bins or shredders for sensitive documents when they are no longer needed.

F. Lock your desk and filing cabinets at the end of the day

G. Lock away portable computing devices such as laptops or tablets

H. Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer

20 SPECIAL ACCESS AGREEMENT

20.1 OVERVIEW

A. As a Datapipe employee, your current or future role may call for you to administer internal Datapipe or client resources. These resources may require 'root', 'administrator', or 'enable' level access in order for you to perform your job ("Special Access"). Special Access levels grant the operator unrestricted access to view, modify, or delete system settings and data which may contain Confidential Information. You are responsible for all actions performed on any Datapipe or client resource.

B. All employees must adhere to Datapipe's acceptable use policies, non-disclosure agreements, and other internal polices as prerequisites for Special Access as well as undergo security training and background checking, as applicable by local law.

C. In addition to the aforementioned requirements, the following Special Access Guidelines have been developed to help employees use Special Access rights in a responsible and secure manner.

20.2 GENERAL GUIDELINES

20.2.1 BE AWARE OF THE DATAPIPE ENVIRONMENT

Each Datapipe facility is highly specialized and contains numerous computing systems and equipment of differing configurations and functions. The proper use of these resources is documented in this Policy. It is the responsibility of all employees to READ, UNDERSTAND and ADHERE to the procedures and policies detailed within.

20.2.2 DOCUMENT ALL MAJOR ACTIONS AND/OR INFORM APPROPRIATE PERSONNEL

A. For all changes to Datapipe resources and client systems, Datapipe employees must adhere to Datapipe's change control policy and procedures documented in SPP-1055, as well as any applicable client specific change control procedures documented within Datapipe's configuration management systems.

B. Datapipe employees are responsible for documenting the approved change control ticket number and/or reason when requesting credentials to Datapipe or client resources. Before actions are taken in response to an incident on client systems, employees are responsible for checking for additional client supplied documentation provided by the client in their Solution Escalation Action Plan (SEAP). (GRC-1000)

20.2.3 HAVE A BACKUP PLAN IN THE EVENT SOMETHING GOES WRONG

Special Access, especially root, has a tremendous potential for causing damage with only a few keystrokes. Develop and document a detailed rollback plan in accordance with Datapipe's change control policy. A clear rollback plan ensures that in the event a change causes unexpected impact, the changes can be reverted to a functioning state. You must be able to restore the system to its prior approved state, or ensure the client acknowledges that a rollback plan is not possible when appropriate.

20.2.4 KNOW WHOM TO TURN TO IF PROBLEMS ARISE

Through the use of Special Access, new and unique problems and/or situations may arise. Although Datapipe has many written procedures, they do not cover every possible scenario. If any doubt exists as to how you should trouble-shoot a problem, ask for assistance. Know whom to ask.

20.3 SPECIFIC RESTRICTIONS

A. Do not share Special Access passwords with anyone.

B. Do not write down Special Access passwords.

C. Do not routinely log onto a system, for which you have an account, as "root" or any other Special Access account unless it is absolutely necessary.

D. Do not browse other users' files, directories or email using a Special Access account unless the proper permission has been granted.

E. Do not make a change on any system that is not directly related to your job duties.

F. Do not use Special Access to for any personal activities (storing files, sending mail, playing games, browsing websites, etc.).

G. Do not disclose, copy, modify, delete, or otherwise access Confidential Information unless explicitly authorized.

H. Do not create additional Special Access accounts unless explicitly authorized and documented.

21 INFORMATION HANDLING POLICY

21.1 INTRODUCTION

Information assets include, but are not limited to, data in databases and data files, system documentation, user manuals, training materials, operational and support procedures, continuity plans and archived information. They are classified according to sensitivity of the data, and they should be handled properly to reduce risks associated with improper information handling practices. All information and associated systems with a sensitivity level of RESTRICTED or CONFIDENTIAL must be assigned an owner who shall be responsible for adhering to all relevant policies.

21.2 PURPOSE

The purpose of this policy is to define the procedure on information handling so as to reduce the risk of a security breach attributable to improper information handling.

21.3 POLICY

The policy defines the best practices on information handling for individuals as follows:

A. Encryption policies must be followed, where applicable. Refer to the Encryption Policy Section for additional information.

B. All information asset(s) shall be properly handled and protected according to the information classification level of the asset(s).

C. Information assets shall be accessed by least privilege. Refer to SPP-1073, Access Control Policy – Logical, and SPP-1011, Datapipe Classification and Media Control Policy for additional information.

D. Information assets shall be properly protected during transmission, processing, storage and disposal throughout the information asset lifecycle.

E. For systems storing or processing Restricted or Confidential data, associated asset inventories shall be maintained documenting pertinent classification details including:

1. Sensitivity level in accordance with SPP-1011, Data Classification and Media Control Policy

2. The value of the information, legal requirements, and criticality to the organization shall be noted as appropriate.

21.4 DATASET HANDLING

A dataset is a set of information in varying formats (e.g. database, xml, statistics, reports, records, etc…) collected and organized for a specific purpose. The below policies shall be followed when accessing datasets within internal Datapipe production systems, or similar such datasets in associated disaster recovery systems.

A. Datasets with Confidential Information must not be stored on non-production systems unless expressly authorized by system owner and management. In such cases:

1. Where possible, datasets shall be selected to only include the minimum amount of data necessary to fulfill the business function.

2. Systems containing Confidential Information must be protected using materially equivalent security controls to the production systems. A risk assessment may be performed to determine exceptions to this policy.

B. Datasets must be accessed only by authorized person based on RBAC (please refer to Access Control Policy - Logical). Depending on the sensitivity level of the data, restrictions can be made such that only specific individuals in a department may have access to the dataset. Exceptions should be granted only if it is authorized by the system owners and expressly approved by Director of Information Security.

21.5 KEY MANAGEMENT

A. Encryption keys must be protected from unauthorized disclosure, modification, loss, and destruction. Protection of the encryption keys at rest is typically implemented by leveraging the access controls enforced on file systems containing such keys, at the operating system level. Additionally, the following guidelines shall be observed for the protection of encryption keys:

   1. Protection of keys in transit must be secured in accordance with the Encryption Policy.

   2. Encryption keys protected with a password must be secured in accordance with the Password Policy

   3. Logical access restricting authorized persons shall be based on RABC. Please refer to the Access Control Policy – Logical for additional information.

B. Examples of encryption keys requiring protection:

   1. SSL certificates

      a. Internal and client systems

      b. Keys imported for use in WAF and IDS. Please refer to PCI Information Security Services Policy for additional information.

   2. SSH keys

   3. Datapipe One client encryption feature

   4. Transparent Database Encryption keys

C. Certain Datapipe internal or Client applications may utilize a Hardware Security Module (HSM) for the generation, protection, and secure access of encryption keys. HSMs shall be secured with appropriate physical and logical security controls. The following guidelines shall be observed when HSMs are in use. All encryption keys:

   1. Must be generated in accordance with the Encryption Policy.

   2. Must be generated in a manner to prevent exportation in cleartext keys.

   3. Which are synchronized between multiple HSMs, must leverage a secure and encrypted mechanism for synchronization.

22 BACKUP POLICY

22.1 INTRODUCTION

The intent of this policy is to maintain the integrity and availability of critical Datapipe systems in the event of accidental loss or damage.

22.2 PURPOSE

Electronic backups enable the recovery of data, systems, and applications in the case of events such as natural disasters, system disk drive failures, compromises, data entry errors, or system operations errors. Backups facilitate the availability, restoration, and performance of essential functions during any emergency or situation that may disrupt normal operations.

22.3 POLICY

This policy defines the best practices on backups for information systems as follows:

A. All critical systems shall require backups.

B. A combination of backup methodologies (full, incremental, and differential) can be used depending on the system configuration and RPO and RTO requirements as determined by the system owner.

C. The frequency and retention of backups must be in accordance with the importance of the information, acceptable risk, and any legal, contractual, or regulatory compliance requirements the system is mandated by.

D. Based on data criticality, storage of backup media may include multiple storage strategies such as both onsite and offsite backups.

E. Backup media stored should have appropriate labeling to manage ownership, sensitivity and rotation where applicable.

F. Testing should be done routinely. When testing backups, extra caution should be used not to impact your operations. When, where, and how are important decisions before attempting to validate your backups.

23 THIRD PARTY REMOTE ACCESS POLICY

23.1 INTRODUCTION

The intent of this policy is to govern the process by which vendors and all other third parties can access Datapipe systems.

23.2 PURPOSE

Vendors and other third parties may require remote access to Datapipe systems for the purposes of system engineering, monitoring, break/fix solutions, patching, or other such reasons. Datapipe must implement proper security controls in order to mitigate any security risks while also minimizing any possible impacts resulting from these remote access activities.

23.3 POLICY

This policy defines the requirements for granting vendors and third parties remote access to Datapipe systems:

A. Approval is required from the Datapipe Security department before vendors and third parties can access Datapipe systems. The requestor must open a ticket via the Datapipe One portal to request access, then complete and attach a SC - 1016 Third Party Remote Access Request Form to the ticket. The Security Team will then review and approval/deny the request.

B. A review of the third party's security practices and contract language must be completed as part of the approval process.

C. A firewall appliance must be deployed to protect Datapipe systems.

D. Secure protocols (e.g. https, ssh) must be adopted for remote access where applicable.

E. VPN requirements:

  1. If persistent access is required by the vendor, a site-to-site VPN must be established.

  2. If periodic or one-time access is required, the vendor must utilize a remote access VPN while using two-factor authentication via the DPAuth system.

  3. Any exceptions to the above VPN requirements must be detailed in SC-1016 as part of the approval process.

F. Access restrictions by source IP must be enforced where applicable.

G. Third party user access rights must be reviewed semi-annually.

H. Third party user registration and de-registration process must be enforced.

I. The system account(s) used for vendor access must conform to Datapipe's Password Policy, with auditing/logging of account activities enabled as well.

J. Datapipe User Account Management Policy must be followed where applicable.

24 VENDOR MANAGEMENT POLICY

24.1 INTRODUCTION

There are various risks associated with the use of third party vendors when outsourcing specific functions of business to perform various actions on Datapipe's behalf. To effectively use a vendor in any capacity is for Datapipe management to appropriately assess, measure, monitor, and control the risks associated with the relationship.

24.2 POLICY

It is Datapipe's policy that a formal vendor risk assessment is completed to ensure the vendor is complying with Datapipe's policies and that underlying risk is accepted by management. All vendors with potential access to Datapipe and/or customer data must execute a Datapipe's Data protection agreement, or have an agreement in place which has been reviewed by Legal and Security that contains contractual provisions that ensure Datapipe and/or client is adequately protected.

24.3 RISK MANAGEMENT PROCESS

24.3.1 RISK ASSESSMENT

Prior to engaging in any activity with a vendor, Datapipe will perform a risk assessment to determine whether the relationship meets overall Datapipe goals. The risk assessment process should include (but is not limited to) answers to the following questions:

1. Will the proposed vendor have access to Datapipe and/or client data?

Can Datapipe business operations be negatively impacted by service interruptions caused by this vendor?

B. The business owner, appointed by management will determine whether the proposed activities, related costs, product and services standards, and third-party involvement, are consistent with the Datapipe's policies, business strategy and risk tolerances.

24.3.2 DUE DILIGENCE

A. The business owner will perform due diligence review(s) prior to entering into any arrangement with a third party vendors.

B. Oversight reviews will require technical expertise, financial condition, organizational policies, and applicable laws and regulations.

C. All potential vendor agreements must be reviewed and approved by both Security and Legal before they can be executed.

24.3.3 CONTRACT REVIEW:

A. The business owner will review the contract to determine if there are any outstanding issues.

a. Upon approval by the business owner, the contract will be executed by the Datapipe legal counsel based on a mutual agreement between Datapipe legal and the vendor.