DOCUMENT NO.	*SPP-1000*
DOCUMENT NAME	*INFORMATION SECURITY SERVICES POLICY*

REVISION LEVEL	21
REVISION DATE	March 5th, 2018
OWNER	DARREN COOK, DIRECTOR OF INFORMATION SECURITY

REVISION LEVEL	HISTORY	REVISION DATE
1	Initial Release.	November 2005
2 – 5	Versions did not contain revision detail.	Revision details not kept
6		September 2008
7	Additions to TDE section. Application of current template including Detailed Revision History. Added language regarding split knowledge for encryption key recovery. Changed firewall policy to reflect updated rule sets. Updated AV policy to reflect requirements of v1.2. Updated WAF policy regarding use of WAF on a staging server for testing. Updated acceptance letter. Amended numbering to conform to v1.2. Clarified that NBAD is only available in the US.	June 29th, 2009
8	Update to the Vulnerability Assessment Policy Added language to clarify the purposes of the reports, different types of vulnerabilities that may be included, and how they are remediated.	September 11th, 2009
9	Updated to new template. Changed revision levels from letter to numbers. Added "Audit Assistance" section. Updated confirmation letter.	February 2nd, 2010
10	Updated to reflect current branding and terminology. Updated Related Documents Section. Amended Section 2, Web Application Firewall to include subsections 2.4.1-2.4.5 Amended Policy, Section 4.4 of Patch Management. Amended Policy, Section 7.4 of Configuration Assessment. Amended Policy, Section 8.4 of Two-Factor Authentication.	August 19th, 2010
11	Elaborated on Introductions, added Risk Mitigation sections, and updated policy language to the Event Management, Patch Management, and Transparent Database Encryption policies.	April 20th, 2011
12	Updated service delivery policies and references to conform to PCI 2.0 revision.	May 21st, 2012
13	Added new Two Factor solution policy (Datapipe Auth). Added Datapipe's 2012 Trustwave Compliance Letter. Added New hardware WAF policy. Added Anti-malware for Linux Policy. Applied latest template.	November 19th, 2012
14	Added a compliance section with two subsections for available packages (HIPAA and PCI Additions). Removed IPS policy, no longer available as a service. Various policy language changes.	August 12th, 2013
15	Modify Anti-Malware policy to address mobile code Updated Trustwave PCI Compliance letter for 2013	November 12th, 2013
16	Updated Trustwave PCI Compliance letter for 2014	May 11th, 2015
17	Added Cloud WAF & DDoS Network Protection Service Policy Modified System Integrity Monitoring policy to change check frequency from hourly to daily. Network Intrusion Detection System – updated alert escalation threshold Modified Transparent Database Encryption Policy to reflect change over to native TDE Two Factor Section: Removed reference to the certificate based service in the introduction. Two Factor Section: Removed the old cert based service specific sub section. Two Factor Section: Added reference to Secure Cloud Access in the main section title. Two Factor Section: Added the info regarding only setting up the one 'all' group by default in the existing 'defaults' section.	July 28th, 2015
18	Added new section 16 – Datapipe File Encryption Service. Edits to section 2 regarding firewall review services for AWS VPCs. Edit to section 7 malware incident handling. Added data classification watermark. Updated CSO to CTSO.	April 20th, 2016
19	Added Bi-Annual Firewall Review Section	March 31st, 2017
20	Added new "CLOUD PLATFORM SECURITY SCANNING" section as #14, all other section #'s adjusted	August 16th, 2017
21	Changed owner to Director of Information Security Removed CTSO and replaced with Director of Information Security throughout document	March 5th, 2018

	Added note to Purpose and Scope section about security service monitoring Added section 7.5 “Datapipe Internal Change Control Policy”	

INTRODUCTION

PURPOSE AND SCOPE

Defense in Depth is Datapipe's core security strategy, a layered methodology backed by a combination of people, technology and operations. Defense in Depth is a proven security approach that aids in meeting the most rigorous standards of confidentiality, integrity, and availability, thus ensuring the ongoing security of your mission-critical digital assets.

Datapipe has selected the best of breed services to help our customers safeguard data, reduce risk, and satisfy internal security or regulatory compliance needs. This document contains the information security polices for Datapipe's managed security services. These services can be elected individually to mitigate areas of identified risk or as a compliance package to help meet regulatory requirements. Datapipe will and implement, monitor, and maintain each service according to their applicable policies. Unless otherwise noted in the individual service policies, for any reporting console which client has access, reports are retained for at least one year. For reports delivered via email, client must retain these reports based on their retention requirements.

This document can be an audit resource when validating compliance against your internal security requirements or with a 3rd party assessor. Frequently asked questions can be found in this document or in Datapipe's Organizational Security Policy (SPP-1020) which is available upon request.

NOTE 1: The "RISKS MITIGATED" sections do not guarantee immunity against possible exploitation from the listed attacks and vulnerabilities. It is intended to detail the class of risks which the security control is designed to protect. Despite control implementation, there will always be residual risk of a control's susceptibility to being bypassed. Layering many security controls into a single solution and providing for Defense in Depth protection methodology is the most aggressive way to minimize risks associated with multi-faceted attacks and control bypass.

NOTE 2: Datapipe internally monitors the availability of security services noted in this document that are offered and applied to systems, both client and internal. This allows for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of:. Firewalls, IDS/IPS, File Integrity Monitoring, Anti-virus, Physical access controls, Logical access controls, Audit logging mechanisms, Segmentation controls (where applicable)

If a failure is detected, the incident response plan detailed in SPP-1020 takes effect.

RELATED DOCUMENTS

SPP-1002	Firewall and Router Configurations
SPP-1011	Data Classification and Media Control Policy
SPP-1020	Datapipe Organizational Security Policy

TERMS AND DEFINITIONS

NA	NA

RESPONSIBLE PARTIES

INFO SEC MGR	Information Security Manager
SEC ENG	Security Engineer(s)

1 COMPLIANCE

Datapipe certified HIPAA Privacy Security Experts (CHPSE) and Payment Card Industry Internal Security Assessors (PCI ISA) have architected Compliance Packages to help our clients satisfy the requirements for the PCI standard and protect electronic protected health information (ePHI) as required by the HIPAA security rule.

*****The PCI DSS outlines a very prescriptive set of security controls that must be followed in detail to comply to the requirements. Datapipe leverages the PCI requirements as a standard when developing and implementing policies for all managed security services.**

1.1 COMPLIANCE PACKAGE – PCI ADDITION

The Payment Card Industry (PCI) Data Security Standard (DSS) was designed to safeguard cardholder data (CHD) against exposure and compromise. The cardholder data environment is comprised of people, processes and technology that store, process or transmit cardholder data or sensitive authentication data. The PCI DSS security requirements are required on any network component, server, or application that is included in or connected to the cardholder data environment. System components also include any virtualization components such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors.

Datapipe's PCI service provider level requires validation of its compliance by undergoing an annual on-site audit from a QSA. The audit encompasses physical security, policies and procedures and our managed security services. Merchant and service providers that require an on-site audit should be able to leverage Datapipe's Report on Compliance (ROC) and may not need to validate the physical security at Datapipe via a 3rd party assessor. However, the entity's acquiring bank may determine that an on-site audit is still required nonetheless. Our ROC is also included in the PCI package welcome packet.

Verification that the following documentation does adhere to the PCI Data Security Standard can be found in Datapipe's PCI Report on Compliance (ROC). If you are interested in obtaining Datapipe's ROC, please contact your Datapipe Sales representative.

Validation of Datapipe's compliance can be found on Visa's list of compliant service providers:

http://www.visa.com/splisting/searchGrsp.do?companyNameCriteria=Datapipe

1.2 COMPLIANCE PACKAGE – HIPAA ADDITION

Health Insurance Portability and Accountability Act (HIPAA), provides federal protections for individually identifiable health information held by Covered Entities (CEs) and their Business Associates (BAs), and gives patients an array of rights with respect to that information. The standards are meant to improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in the U.S. health care system.

The HIPAA Security Rule specifies a series of administrative, physical, technical, and organizational safeguards for CEs and their BAs to use to assure the confidentiality, integrity, and availability of Electronic Protected Healthcare Information (ePHI). HIPAA CEs were required to comply with the Security Rule beginning on April 20, 2005. The Office for Civil Rights (OCR) became responsible for enforcing the Security Rule on July 27, 2009.

http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/index.html

The Health Information Technology for Economic and Clinical Health (HITECH) Act clarified and supplemented HIPAA requirements, particularly by raising the financial penalties in cases of non-compliance, and detailing that BAs are "HIPAA covered" for the full HIPAA Security Rule and the use and disclosure provisions of the HIPAA privacy rule by statute. HITECH became fully enforceable February 18, 2010.

The final Omnibus Rule went into effect on March 26, 2013 and became enforceable on September 23, 2013. This rule states, among other things, that any entity that creates, receives, maintains, or transmits Protected Health Information on behalf of a CE is unequivocally considered a BA.

http://www.hhs.gov/ocr/privacy/hipaa/administrative/omnibus/index.html

As a managed IT service provider doing business with healthcare organizations, Datapipe is a maintainer of the infrastructure of client systems that handles ePHI. While Datapipe employees do not manage or operate healthcare applications directly, and therefore do not have a business need to access or alter such ePHI, its employees do have a need to administratively manage such systems.

Therefore, as a maintainer of ePHI, Datapipe will enter into a Business Associate Agreement (BAA) with a CE provided that the compliance package is elected in its entirety. This package has been specifically designed as a result of Datapipe's internal risk assessment to help safeguard client ePHI, reduce risk of disclosure, and comply with the regulations as mandated by the OCR.

2 FIREWALL SERVICES

2.1 SCOPE

Datapipe supplied hardware firewalls and/or or public cloud security groups (SG).

2.2 INTRODUCTION

Firewalls are security devices that place a layer of security between your solution and the Internet by restricting inbound and outbound flows to hosts employing differing security postures based on specific requirements. Datapipe Firewall Services provide custom tailored policies that permit or deny network traffic based on compliance standards and business needs.

A security group acts as a virtual firewall that controls the traffic allowed to reach one or more instances. When an instance is launched, security groups are configured and assigned. Rules are then added to each security group that control traffic for the instance. The rules for a security group can be modified at any time, with the new rules being automatically applied to all instances to which the security group is assigned. In addition, NACL (Network Access Control Lists act as stateless firewalls for associated subnets, controlling both inbound and outbound traffic at the subnet level.

2.3 RISKS MITIGATED

2.3.1 DATAPIPE HARDWARE FIREWALLS

A. Unrestricted inbound and outbound access to/from the Internet and all systems (firewalls implement stateful inspection)
B. A single logical segment for all systems (firewalls can implement VLANs)
C. Public addressing for internal systems (firewalls perform NAT)
D. Unencrypted transport between remote sites and users (firewalls can implement Virtual Private Networks)

2.3.2 PUBLIC CLOUD SECURITY GROUPS

A. Unrestricted inbound and outbound access to/from the Internet and all systems
B. A single logical segment for all systems
C. Public addressing for internal systems

2.4 DATAPIPE POLICY

Datapipe implements a justified firewall rule set which allows us to actively monitor and provide managed services to your solution. Prior to the deployment of a firewall, a Solutions Architect will interview the client to determine business and technical ports and services required by the client as a business necessity. Datapipe Sales Engineers will subsequently design a network diagram illustrating the interconnections and virtual LANs.

In a typical three tier solution, security zones (VLANs or subnets) will be created segmenting the web and application servers from the internal database networks. Network address translation (NAT) will be used for IP masquerading using a unique dedicated RFC 1918 IP block.

All physical firewall events at level 5 and below will be forwarded via "syslog" to the Datapipe Log Manager solution (included in PCI package) for correlation and review. For AWS VPCs, VPC Flow Logs can be enabled for cases where there is a need to capture information about the IP traffic going to and from network interfaces in the VPC. Flow log data is stored using Amazon CloudWatch Logs. After a flow log is created, log data can be retrieved and viewed in the Amazon CloudWatch UI.

All firewall configuration change requests must follow Change Control procedures before firewall changes will be implemented by Datapipe.

3 BI-ANNUAL FIREWALL REVIEW

3.1 SCOPE

Datapipe supplied hardware firewalls or supported public cloud security groups where service has been elected.

3.2 INTRODUCTION

A firewall is an appliance (a combination of hardware and software) or an application (software) designed to control the flow of Internet Protocol (IP) traffic to or from a network or electronic equipment. Firewalls are used to examine network traffic and enforce policies based on instructions contained within the Firewall's Ruleset. Firewalls represent one component of a strategy to combat malicious activities and assaults on computing resources and network-accessible information. Firewall reviews are a key requirement within a number of industry related standards and regulations, such as the PCI DSS. A firewall security review examines vendor configuration vulnerabilities, misconfigurations, unnecessary open ports, and unused ACLs that could allow an attacker to gain access to your critical resources.

3.3 RISKS MITIGATED

Vulnerabilities and unnecessary open ports that can expose your solution to attackers.

3.4 DATAPIPE POLICY

If services elected, bi-annually a Security Engineer shall review client firewall physical and/or security group rule sets and provide client with a detailed report on how to align firewall configurations around the PCI DSS and industry recognized best practices. If remediation is required, the client is responsible for approving the remediation actions as outlined in the report.

The client is responsible for reviewing the rule set to ensure that the rules reflect the current business needs for the client's applications and associated authorized services and ports. The active firewall rule set or VPC security group configuration is always available via your Datapipe One portal (https://datapipeprod.service-now.com) or on the AWS Management Console, respectively.

4 WEB APPLICATION FIREWALL

4.1 SCOPE

All Datapipe supported web servers where service or a compliance package has been elected.

4.2 INTRODUCTION

A Web Application Firewall (WAF) is a hardware appliance, proxy, server plugin, or filter that applies a set of rules to an HTTP/HTTPS conversation. Datapipe's Imperva WAF will combine automated application learning with up-to-date protection policies and signatures to accurately identify and stop attacks. It will inspect web traffic so that attacks can be identified and/or blocked in real-time.

4.3 RISKS MITIGATED

A. Cross-site scripting
B. SQL Injection
C. Cross-Site Request Forgery
D. Information Leakage
E. Content Spoofing
F. Session Hijacking
G. Path Traversal
H. Buffer Overflows
I. Probing
J. Code Injection
K. Remote Command Execution

4.4 DATAPIPE POLICY

The Imperva Web Application Firewall solution provides web security by protecting your websites and web applications from common attacks. The Datapipe Security Team and/or the Imperva SOC will configure the Web Application Firewall to start monitoring client-chosen applications in monitoring mode, which will log, but not block, malicious traffic. Datapipe recommends the WAF to remain in monitoring mode until application traffic is reviewed and tuned. Datapipe security will coordinate with the client to review logged traffic and customize the WAF to prevent the blockage of legitimate traffic. With confirmation from the client, the Datapipe Security Team will set the WAF to active mode, which will start blocking attacks in real time.

Datapipe recommends that a WAF is deployed to the client's production and staging web servers. This allows the WAF to be tuned after code updates without impacting production websites. After the new code and WAF policy have been validated, both can be pushed to the production environment. Each WAF-protected web application will have out-of-the-box protection against the most common threats that potentially put your application at risk. By default, your application will be protected against the threats detailed in the Risks Mitigated section. If an appliance based WAF is elected, client must provide Datapipe with a copy of the SSL certificates used to negotiate the HTTPS connection. Without the certificates, the WAF will not be able to inspect HTTPS traffic.

5 CLOUD DISTRIBUTED DENIAL OF SERVICE & NETWORK PROTECTION

5.1 SCOPE

All Datapipe supported web servers where service or a compliance package has been elected.

5.2 INTRODUCTION

Datapipe's Cloud Distributed Denial of Service (DDOS) & Network Protection service, powered by Imperva's Incapsula, provides enterprise level website security and web DDoS Protection in one solution. It will protect against the most critical web application security risks without the need of additional hardware or software. Your website(s) are protected with a simple DNS change.

5.3 RISKS MITIGATED

A. Cross-site scripting
B. Distributed Denial of Service
C. SQL Injection
D. Cross-Site Request Forgery
E. Information Leakage
F. Content Spoofing
G. Session Hijacking
H. Path Traversal
I. Buffer Overflows
J. Probing
K. Code Injection
L. Remote Command Execution

5.4 DATAPIPE POLICY

Upon election, Datapipe will send out a welcome letter via Datapipe One https://datapipeprod.service-now.com, which will include an introduction to the service as well as several requests for information (RFI). The information being requested is **required** before Datapipe can proceed with the provisioning process. If the information is not returned to Datapipe we will be unable to proceed, and your website(s) will remain unprotected. **Please note** that Datapipe will only protect the website(s) that were provided by the Client during the RFI process.

Upon completion of the provisioning process by Datapipe, the Client will be sent an email from Incapsula Service no_reply@incapsula.com with the **required** DNS changes to be made by the Client. Once the changes are made by the Client, another email will be sent confirming successful completion of the site setup. It can take up to 48 hours for all your traffic to route through Incapsula, depending on your DNS settings. **Please note** that deviating away from the initial DNS settings will result in the loss of protection of the Clients' website(s).

Please note that by default Incapsula will only be monitoring and logging traffic until the Client submits a support request via https://datapipeprod.service-now.com to switch to blocking mode.

Your Incapsula service comes with a shared GlobalSign SSL certificate that is leveraged to analyze your encrypted traffic for security risks. Datapipe will provision your service with the shared certificate by default. Upon written request and approval by Client, Datapipe will work with the vendor to disable early TLS protocol versions.

6 PATCH MANAGEMENT

6.1 SCOPE

All supported operating systems, applications, and hypervisors where service or a compliance package has been elected.

6.2 INTRODUCTION

Security patches are additional pieces of code developed to address problems (commonly called "bugs") in software which address security flaws within a program. Patch management is a security practice designed to proactively prevent the exploitation of IT vulnerabilities that exist within an organization. The expected result is to reduce the time and money spent dealing with vulnerabilities and exploitation of those vulnerabilities. Proactively managing vulnerabilities of systems will reduce or eliminate the potential for exploitation and involve considerably less time and effort than responding after exploitation has occurred. Datapipe's patch management services provide means of identifying and deploying patches to supported applications and operating systems.

6.3 RISKS MITIGATED

Exploitation of known vulnerabilities with associated available patches (complete system compromise, privilege escalation, data loss, etc.)

6.4 DATAPIPE POLICY

Datapipe's Patch Management solution provides notification of newly published security bulletins, patches testing (if an applicable environment is available), scheduled remediation, and verified deployments of supported applications and operating systems in accordance with the PCI specification. When new security vulnerability is publically announced, and its vendor-supplied patch becomes available, Datapipe will take action in accordance with pre-defined criteria including scheduling of installation with Change Control if applicable, configuration changes, and rebooting if necessary. Additionally, Datapipe follows a risk-based approach for prioritizing patch installations as detailed in the PCI Requirement 6.1 of the PCI DSS.

NOTE: **An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.**

As such, all high-risk security operating system and Datapipe supported application binary updates which are released and supported by the vendor shall be installed within 30 days of release. Lower risk updates will either be deployed monthly in conjunction with higher risk updates, or rolled into a quarterly update patch.

Datapipe supported firewall IOS upgrades and patches will be deployed under the following conditions:

A. Within 30 days of vendor release, if the release contains relevant security fixes to enable feature sets on the firewall.
B. Business requirement dependent on a bug fix or new feature set.
C. During the 6 month PCI firewall review process to the latest Datapipe tested and supported version.

Datapipe uses the vendor-supplied classification as its default risk rating. A "High" risk vulnerability shall correspond to a "critical" (or highest criticality level available) vendor rated vulnerability. All other vendor-ratings shall constitute a "Lower risk" update. Datapipe may override the vendor rating to a lower or higher classification based on a number of factors, including but not limited to:

A. Network segment of the device (DMZ versus internal)
B. Network exposure (firewalled port)
C. Actively running vulnerability (versus installed but dormant application/library)

D. Common Vulnerability Scoring System (CVSS) rating
E. Exploitation vector (local versus remote)
F. Availability of public exploits
G. Applicable compensating controls

A combination of factors listed above may cause a vulnerability to have a negligible risk rating. In these cases, a patch may not be deployed if there are operational repercussions associated with the installation of the patch; however, vulnerabilities shall be re-evaluated quarterly to determine if the risk rating has changed.

Only reclassified vulnerabilities shall have their risk ratings documented with justification describing the circumstances. Otherwise, the vendor classified rating shall represent Datapipe's risk rating.

Datapipe subscribes to security mailing lists including SANS, CERT, BugTraq, and FullDisclosure. If additional information regarding the specifics of a new security patch is required, the Datapipe Security Team refers to the applicable vendor's website. If a high-risk vulnerability is actively being exploited in the wild, Datapipe may deploy emergency patches outside of the normal patch cycle.

Clients will be notified via email/ticket on a monthly basis, or depending on the adjusted risk-rating, on a quarterly basis, of availability of applicable patches for their operating systems and supported applications. A managed support representative will set a target installation date and time for the patch deployment, and reboot if necessary, in coordination with the client. Clients have the flexibility of rescheduling the patch deployment should the need arise. In some instances, clients may have a predefined patching schedule. Datapipe recommends that all clients leverage a development or QA environment to test patches against client specific applications before being deployed into production. IBM will notify Datapipe if a recently released security patch has been proven to cause any issues. Datapipe will notify clients of any issues found by IBM in the patch notification. If clients wish to OPT out of new patch installations, a ticket with business justification is **required** from the client.

Clusters will always be scheduled and patched one node at a time, usually within a 3 hour window to minimize downtime. Typically the inactive node will be allotted the first 1.5 hours followed by the active node. Load balanced Web/App servers will also typically be allotted a 3 hour patching window. The first half of servers will be scheduled in the first 1.5 hours of deployment followed by the last half of servers in the farm. Datapipe does not include Windows service packs or UNIX kernel upgrades in automated patch deployments. Datapipe recommends clients thoroughly test service packs and UNIX kernel updates in their development or QA environment before being deployed in production. Datapipe will install service packs and UNIX kernel updates for clients manually only after change control management approval.

Custom applications, either created by the client or a third party application service providers, are governed by separate patching policies. Unless specific arrangement have been made for Datapipe to receive / check out code updates, the client is responsible for assessing the risk-rating for any available patches and for deploying the patches in a manner consistent with applicable client policies.

7 ADVANCED CHANGE CONTROL

7.1 SCOPE

All support requests received by Datapipe support where service or a compliance package has been elected.

7.2 INTRODUCTION

Change control is a term used to describe the procedures followed throughout the change lifecycle. This ensures that all change requests are documented, assessed, approved, and tested. Datapipe provides the necessary internal procedures and client communication required to follow change control in a regulated, secure environment.

7.3 RISKS MITIGATED

A. Security features inadvertently or deliberately omitted or rendered inoperable
B. Processing irregularities
C. Stakeholders impacted by changes of which they were unaware

7.4 DATAPIPE POLICY

Support request must use the Datapipe ticket system and must follow the change control procedures outlined by the PCI specification.

Support requests submitted to Datapipe by the client and requests submitted by Datapipe personnel on client's behalf must follow strict change control procedures for all system and software configuration changes.

Detailed change control procedures for Datapipe to follow can be found in the PCI Change Control Procedure document. This document is brought to the managed support representative's attention when reviewing the ticket request via the 'Custom Fields' property indicating the PCI compliance status and linking to said document.

Every support request (ticket) will include the following items:

A. Documentation of impact
B. Documentation of rollback procedures
C. Management sign-off by appropriate parties
D. Test of operational functionality

Management is automatically carbon copied on all ticket requests, and must explicitly approve the change request. Support requests submitted without client management approval will not be honored.

7.5 DATAPIPE INTERNAL CHANGE CONTROL POLICY

Datapipe internal change controls follow the requirements and steps set forth in the "Change Management Process" procedure document (internal distribution only).

Please note that Datapipe will update any relevant internal system documentation as part of a significant change. A significant change is defined as any change that has the potential to impact the critical processes and information security (e.g. moving a system from on-premises to a SaaS).

8 ANTI-MALWARE

8.1 SCOPE

Datapipe servers with Microsoft Windows and Linux based Operating Systems where service or a compliance package has been elected.

8.2 INTRODUCTION

Malware, also known as malicious code and malicious software, refers to a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim. Datapipe's Anti-Malware service offers means of detecting and preventing installation and propagation of many types of malware.

8.3 RISKS MITIGATED

A. Loss of data confidentiality
B. Loss of data integrity
C. System instability leading to loss of service/data availability
D. Trojans, rootkits, viruses, and key loggers

8.4 DATAPIPE POLICY

Datapipe's Anti-Malware solution will be configured and actively running in accordance with PCI specifications. The Anti-Malware software is configured to check for, download and install Malware definitions from the vendor every hour. If malware is detected, the anti-malware software will attempt to clean the file. If the file cannot be cleaned, the file will be deleted and quarantined immediately. The anti-malware agent reports and forwards all events directly to a centrally managed console. Upon client request, the console can be configured to send threat detection notifications and reports based on agent events automatically via email. Note: Datapipe does not explicitly block mobile code; however, if the code is determined to be malicious by Datapipe's anti-malware solution, it will be blocked and logged accordingly.

For Windows servers, threats are detected in real-time when a malicious file is created, opened or executed on a host. Scans are configured to scan local drive and memory once a week or can be manually initiated by the client from the system tray. File and directory exclusions are configured according to Anti-Malware and Operating System vendor recommendations based on applications installed on the host.

For Linux servers, NOD32 will be configured to update signatures daily and scan for malware weekly. If malware is detected during a scan, the Anti-Malware software will attempt to clean the file. Real time protection will not be enabled on Linux. If the file cannot be cleaned, the file will be deleted and quarantined immediately.

Datapipe will retain anti-malware scan logs, update logs, and malware detection related logs for at least one year. Requirement 5.1 of the PCI DSS indicates that anti-virus software should be deployed on all systems commonly affected by malicious software (particularly personal computers and servers). This may include Linux servers depending on the server's role and current threats in the wild. The client is required to perform a risk assessment at least annually to determine if their Linux based servers are at risk for infection by malware. Datapipe recommends anti-virus for all supported platforms; however, a risk assessment is a cost effective approach for determining necessity. Some Unix-based antimalware products do not support scanning on file execution or central logging, in these cases, scans will be configured to run on a set schedule and store results locally. Ultimately, only a QSA can determine if anti-virus is required on your solution.

9 CONFIGURATION ASSESSMENT

9.1 SCOPE

All Microsoft Windows, Red Hat Linux, and Solaris server platforms where service or a compliance package has been elected.

9.2 INTRODUCTION

Computer systems are typically hardened upon initial deployment; however, over time, configuration settings may change due to software installation, troubleshooting, or deliberate user modification. Datapipe's Configuration Assessment service provides regular monitoring and alerting on any deviation of a known and trusted system state. Your solution will be evaluated and hardened against industry recognized secure configurations, based on the PCI DSS and the CIS benchmark. You will be alerted of any deviation of the security policy so compliance can be maintained.

9.3 RISKS MITIGATED

A. Reconfiguration resulting in non-compliant / insecure configurations
B. Lack of visibility to the system hardening state

9.4 DATAPIPE POLICY

Datapipe's Configuration Assessment solution will monitor, alert, and report on any non-compliant deviation of the Datapipe implemented secure configuration standard.

The host based agent leveraged in Datapipe's Configuration Assessment service will take a baseline of a system after the secure configuration has been applied. After a system is baselined, the agent will perform weekly compliance checks to determine if the system is still in compliance with the Datapipe hardening standard. If a deviation is detected, the client and the Datapipe security team will receive a PCI DSS Policy Deviation Alert email detailing how the system is non-compliant with respect to Datapipe's hardening standard. It is the responsibility of the client to review the deviation reports and create support tickets for any remediation as necessary. Please note any changes performed by Datapipe will always be accompanied by an associated change control ticket with approval from the client.

In the event the client's solution cannot be brought into a compliant state for technical or business reasons, Datapipe can issue a waiver on the failing policy test(s). Clients will also receive a Weekly PCI DSS Policy Results report via email. These reports indicate the degree to which monitored systems comply with the established policies.

10 TWO-FACTOR AUTHENTICATION

10.1 SCOPE

All authorized clients and Datapipe support personnel remotely accessing servers in the Solution where service or a compliance package has been elected.

10.2 INTRODUCTION

Two-factor authentication is an extra layer of security identification that uses two different authenticating factors (any two of the following: something you have, something you are, or something you know) to verify or authenticate a user's identity to a system. Datapipe's Two-factor Authentication service utilizes One Time Passwords. The One Time Passwords are a combination of a token value (something you have) and a PIN number (something you know). Requiring a second factor of authentication significantly increases your system security by removing the risk of unauthorized access by a password that has been compromised. System access is granted only upon successful authentication of both factors.

10.3 RISKS MITIGATED

A. Brute force password attacks
B. Account and system compromise

10.4 DATAPIPE POLICY

Datapipe's Two-factor Authentication solutions will leverage two-factor authentication for all remote access.

10.4.1 CLIENTS UTILIZING DATAPIPE AUTH TWO-FACTOR

NOTE: This includes the Secure Cloud Access service

Clients connecting remotely to their solution will use two-factor authentication utilizing an IPSEC or SSL VPN with one time passwords for authentication. The two factors of identity being used in the authentication process are:

A. Something you have - A device with the Datapipe Auth token manager application installed
B. Something you know - Your Datapipe Auth PIN

Once a client is configured to use Datapipe Auth, all aspects of managing client users and tokens can be handled by the designated customer administrators. This empowers the client to control access to their solution in real time, without the need to wait for Datapipe personnel to intervene. Datapipe security personnel also have the ability to manage these items and are available for support as needed by opening a support ticket on the Datapipe One portal.

The Datapipe Auth web portal will be used by customer administrators to manage remote access to the environments within their hosted solution. Within the portal, customer administrators will:

A. Create/delete Datapipe Auth user accounts for their users
B. Provision and/or de-provision their user's tokens, including extending token lifetimes when necessary
C. Approve/deny their user's additional device registration requests
D. Lock/unlock their user's devices as necessary

By default, users are allowed to register one device with the system without requiring approval. After that, any device they attempt to use will generate an additional device registration request which will be sent to the customer administrators. A customer administrator must login to the web portal to approve this request before the user will be able to retrieve their tokens using the device.

The following are Datapipe Auth default settings; they can be changed upon client request:

A. "Authentication Level" for resources is set to "Username and Token". Username being the Datapipe Auth username and token being the combination of PIN + token value.
B. "Bad PIN threshold" is set to 5. After 5 invalid authentication requests to a resource the token is disabled and must be manually re-enabled by a customer administrator or a Datapipe security team member.
C. "Token Lifetime" is set to 365 days. This is essentially an expiration, after which the token will not work.
D. "Token Registration Validity Timeframe" is set to 14 days. This is a timeframe, starting from the day an administrator provisions a token, within which the user must retrieve the new token or it becomes invalidated. The user retrieves the token using a token manager application.
E. One 'all' group is setup which allows access to all subnets configured on the firewall, or all subnets within the VPC in the case of AWS and Secure Cloud Access. Additional access control groups can be configured upon customer request by opening a support request in Datapipe One.

10.4.2 DATAPIPE SUPPORT PERSONNEL

To manage client solutions remotely, Datapipe personnel must first connect to the Datapipe corporate network via IPSEC VPN with two-factor authentication using either a physical or soft token used in combination with a PIN to create a one-time password (OTP). Once on the Datapipe corporate network, support personnel must use the token based two-factor authentication method again to log on to a Datapipe application server, from which they can connect to the client solutions.

11 VULNERABILITY ASSESSMENT

11.1 SCOPE

All Microsoft Windows, Linux, and Solaris server platforms where service or a compliance package has been elected.

11.2 INTRODUCTION

Vulnerabilities are flaws that can be exploited by a malicious entity to gain greater access or privileges than it is authorized to have on a computer system. Not all vulnerabilities have related patches; thus, system administrators must not only be aware of applicable vulnerabilities and available patches, but also other methods of remediation (e.g., device or network configuration changes, employee training) that limit the exposure of systems to vulnerabilities. Vulnerability management is a security practice designed to proactively prevent the exploitation of IT vulnerabilities that exist within an organization. The expected result is to reduce the time and money spent dealing with vulnerabilities and exploitation of those vulnerabilities. Proactively managing vulnerabilities of systems will reduce or eliminate the potential for exploitation and involve considerably less time and effort than responding after an exploitation has occurred. Datapipe's Vulnerability Assessment service identifies known security vulnerabilities and assists in prioritizing threats for remediation. Utilizing a non-intrusive scanning engine, Datapipe can facilitate in securing client assets against even the most recent of discovered vulnerabilities.

11.3 RISKS MITIGATED

Exploitation of known vulnerabilities associated with patches, configuration settings, and policies

11.4 DATAPIPE POLICY

Datapipe's vulnerability assessment service uses an industry standard network vulnerability scanner. The Datapipe security department will configure automated internal scans of all hosts at least monthly. Datapipe scans well-known TCP ports (0-1023) as well as common application TCP and UDP ports by default. Additional ports can be scanned upon request.

Clients have access to initiate on demand scans through Datapipe's central console. Reports are available in the central console for risk assessment purposes only. The report may contain vulnerabilities related to missing system patches and configuration weaknesses. To ensure your system is fully up to date with necessary security patches, you can contact the Datapipe support team. Resolution of the remaining system configuration vulnerabilities included in the report will not be initiated by Datapipe unless a formal remediation request is submitted to Datapipe using the Datapipe ticketing system. Please note, the Datapipe security team performs vulnerability scans independently, and all remediation approved by the client will be performed by the Datapipe support staff. In some cases, the Datapipe security team may be consulted for vulnerability remediation.

Because of the diversity of client applications, resolution of such vulnerabilities may impact your solution. Therefore, Datapipe highly recommends that any alteration of your system configuration settings to address vulnerabilities should first be tested in a development/staging environment. Once the change has been confirmed to have no negative impact to your solution, you may contact Datapipe support to deploy the recommended fix in your production environment. Vulnerability signatures are received automatically from the vendor and updated as they are available.

The Datapipe security department will create the necessary local or domain dedicated scanner user on all hosts so that the scanner may authenticate to perform necessary local vulnerability checks. The scanner will only run non-intrusive checks to avoid possible service interruptions. The credentials used by the scanner will always follow the PCI password policies guidelines. The scanner will always authenticate to hosts via protocols which support password encryption.

Note: This service only satisfies the internal vulnerability scan requirement. Requirement 11.2.1 of the PCI specification still requires external vulnerability scanning to completely satisfy this requirement. Please see Networking Intrusion Detection System for more details on external scanning. The scanner only scans for operating system and various off the shelf application vulnerabilities and does not scan for custom web application related weaknesses.

12 NETWORK INTRUSION DETECTION SYSTEM

12.1 SCOPE

All servers in PCI environment will be monitored for intrusions where service or a compliance package has been elected.

12.2 INTRODUCTION

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. Intrusion detection systems (IDS) are primarily focused on identifying possible incidents, logging information about them, optionally attempting to stop them, and reporting them to security administrators. In addition, organizations use IDSs for other purposes, such as identifying problems with security policies, documenting existing threats, and deterring individuals from violating security policies. IDSs have become a necessary addition to the security infrastructure of nearly every organization. Datapipe's Network Intrusion Detection System offering monitors and detects malicious network activity that can compromise the security of a computer system. The service provides attack detection and alerting by a dedicated team of trained IDS experts.

12.3 RISKS MITIGATED

A. Suspicious activity is not investigated
B. Successful attacks go undetected

12.4 DATAPIPE POLICY

Datapipe's Network Intrusion Detection System will monitor all network traffic and alert personnel in accordance with PCI specification.

The signature based IDS sensor receives a copy of all client internal VLAN traffic. All traffic is then analyzed by the IDS 24 hours a day 365 days a year for potential attacks. All events are logged and correlated based on threat trends, severity, attack signatures, and repeat offenders. Encrypted web traffic using SSL can be terminated and analyzed by the IDS seamlessly decrypting this traffic using the private keys of the website(s) SSL certificates. This is an additional feature and is not implemented by default. NOTE: Since the IDS does not terminate traffic it cannot inspect traffic encrypted with Perfect Forward Secrecy. For deployments that include a physical firewall, the IDS has the ability to 'shun' or block an attackers IP address for a predetermined amount of time. This feature is not enabled by default, but can be enabled upon request. A client provided whitelist of IP addresses is required before Datapipe will enable the 'shun' feature. A client firewall configuration change is also required before 'shunning' can be enabled.

AlertLogic analysts will review incidents no longer than 30 minutes after detection and will escalate as soon as the incident has been reviewed. A detailed incident summary will then be created and sent to the Datapipe security team and Client via email. In the event an incident severity level is categorized as high or above, the Alert Logic Security Operations Center (SOC) will escalate to Datapipe via phone call. The Datapipe security team will immediately start investigating the threat and will notify clients via phone, ticket or email depending on Client SEAP. If the incident severity level is categorized at a lower threshold, it will be considered non-actionable; therefore no mitigating or investigative actions will be taken by Datapipe. If Client requires additional information, or specific actions to be taken against a specific lower severity incident, the Client must submit a support request via https://datapipeprod.service-now.com

IDS incidents and related events are retained for one year and are available for client review in AlertLogic's Threat Manager web-based interface. Included with the IDS is access to a PCI ASV (Approved Scanning Vendors) Scanner. This scanner allows customers to define their assets by IP or CIDR notation and scan their assets quarterly as per PCI 11.2.2 requirements. As each customer requirements differ, Datapipe requests clients to create a ticket for Datapipe personnel to remediate the items that they require.

13 SYSTEM INTEGRITY MONITORING

13.1 SCOPE

All Microsoft Windows, Red Hat Linux, and Solaris server platforms where service or a compliance has been elected.

13.2 INTRODUCTION

System Integrity Manager detects changes to servers, applications, devices and other IT assets in real-time across physical and virtual IT infrastructures so all change can be tracked and validated. Datapipe's System Integrity Monitoring service provides hourly reporting of all critical changes which could have a potential impact to the overall security or integrity of the system, including: files, security settings, registry settings, configuration parameters and permissions. This ensures that all changes are planned and verified, and all unauthorized changes are investigated.

13.3 RISKS MITIGATED

A. Authorized and unauthorized changes not being reviewed
B. Not having accountability for changes
C. Changes to critical files going undetected

13.4 DATAPIPE POLICY

Datapipe's System Integrity Monitoring solution will check for all critical system changes daily (exceeding the PCI specification).

The host based system integrity agent will check, alert, and report on any changes to critical computing resources daily. Change detection rules can be added, removed, or customized per solution if requested. Default change detection rules will applied based on operating system to detect critical system changes. A report detailing these monitored locations will be included with your setup letter. Additionally, with the assistance of the client, the Datapipe security team will determine what file system locations contain application code and/or cardholder data so that client specific change detection monitoring can be configured. Please note that there is a 100k file limit per node on daily custom content checks. However, Datapipe can monitor custom content with more than 100k on a weekly schedule which is still in accordance with the PCI specification.

Upon detecting a change, the Datapipe security team and the client will receive a Critical File System Change Alert via email, containing detailed information such content, permission, and attribute changes. The change data may also be correlated to the local username which initiated the change depending on the Operating System and Tripwire agent version.

NOTE: Change reports will include the public IP address of all hosts that changed. Upon request, Datapipe can rename your nodes in Tripwire to DNS or Host names if you consider public IP addresses as sensitive information.

Datapipe is responsible for providing the infrastructure to report on changes that are detected on client systems. It is the responsibility of the client to review the change notifications to determine if they were authorized. Upon discovery of unauthorized change, the client should escalate to Datapipe for investigation. Please note any changes performed by Datapipe will always be accompanied by an associated change control ticket with approval from the client.

14 CLOUD PLATFORM SECURITY SCANNING

14.1 SCOPE

Supported cloud platforms that require security scanning for compliance with vendor, security-specific best practices. This applies to all accounts deployed after August 2017, please consult Datapipe Security for confirmation regarding your account.

Currently supported cloud platforms:

- Amazon Web Services

14.2 INTRODUCTION

The platform security scanning service checks for vulnerabilities in the form of misconfigurations or deviations from the recommended security best practices. These misconfigurations/policy deviations could be exploited by a malicious entity in order to gain unauthorized access/privileges or otherwise compromise the integrity of a cloud environment. Proactively detecting and remediating vulnerabilities will reduce or eliminate the likelihood for exploitation, as well as requiring considerably less time and effort than responding after an exploitation has occurred. Utilizing a non-intrusive scanning platform, Datapipe can facilitate in securing client assets in supported cloud platforms.

14.3 RISKS MITIGATED

Noncompliance in regulated infrastructures and exploitation of known vulnerabilities associated with misconfigurations and other deviations from established security best practices.

14.4 DATAPIPE POLICY

Datapipe's cloud platform security scanning service uses a best of breed SaaS scanning platform. The Datapipe security department will configure customer environments to be scanned as requested by the Service Delivery Management team. The scanning service checks customer cloud accounts against security best practices that are established by the vendor and tuned by Datapipe for common deployment scenarios. The scans are run at regular intervals and make API calls to the cloud platform. Customers have access to the scanning service's web console to view current alerts and reports. To remediate any findings included in the reports/console, the customer will need to open a support ticket on the Datapipe One portal.

Because of the diversity of client applications, remediation of these security findings may impact a customer's solution. Datapipe highly recommends that any remediation changes be tested in a development/staging environment before applying them to a production environment. Once the changes have been confirmed to have no negative impact to your solution, the customer may open a support ticket on the Datapipe One portal, requesting the deployment of the recommended changes in the production environment.

The Datapipe security department will create the necessary cross-account trust to enable the security scanning service to perform its checks. A 'DatapipeOpsAccess' role will be created in the customer's account which is required for the scanning service to function. The scanner requires read-only access to query the cloud platform API, no host level access is required.

15 LOG MANAGEMENT

15.1 SCOPE

All Microsoft Windows, Red Hat Linux, and Solaris server platforms and supported hardware firewalls where service or a compliance package has been elected.

15.2 INTRODUCTION

A log is a record of the events occurring within an organization's systems and networks. Logs are composed of log entries; each entry contains information related to a specific event that has occurred within a system or network. Many logs within an organization contain records related to computer security. The number, volume, and variety of computer security logs have increased greatly, which has created the need for computer security log management—the process for generating, transmitting, storing, analyzing, and disposing of computer security log data. Datapipe's Log Manager/Event Management service provides agent or agentless collection, log storage, reporting and alerting, correlation, monitoring, and workflow management for security logs into a single solution.

15.3 RISKS MITIGATED

A. Attackers can modify audit logs obscuring their actions
B. Audits trails not being reviewed
C. Suspicious behavior and intrusion attempts go undetected
D. System and application anomalies go unnoticed

15.4 DATAPIPE POLICY

Event Management solution will collect, correlate, alert on incidents, hash, and retain events according to the PCI specification.

Datapipe will configure all applicable log sources to generate system and security related event logs which will be collected and forwarded to AlertLogic's Security Operations Center where they are stored for a full year. The logs will either be reviewed daily or in real-time depending on the service elected by the client. If the result of the log review triggers an incident, a detailed notification will be created and sent to the client via email. Upon receipt of notification, if additional assistance is required, the client can submit a support request via https://www.one.datapipe.com.

Log events and incidents are aggregated and correlated into Alertlogic's secure event console web based interface for quick access and easy reporting. Unique logins will be issued to only those who are authorized to view event data for their specific solution. Audit trails and integrity checks provide assurance to business owners and auditors that all review and escalation activities are be performed as required.

Event attributes on applicable components will include no less than the user identification, type of event, date and time, success or failure indication, origination of event, and the identity or name of affected data, system component, or resource.

16 TRANSPARENT DATABASE ENCRYPTION

16.1 SCOPE

Supported on servers running Oracle Enterprise with advanced security license, or servers running Microsoft SQL enterprise.

16.2 INTRODUCTION

Transparent data encryption (TDE) performs real-time I/O encryption and decryption of data to protect sensitive data at rest. Generally applications do not have to be modified and will continue to work seamlessly. Data is automatically encrypted when it is written to the database and automatically decrypted when accessed by the application. Granular access policies govern which users and groups can perform specific actions as well as logging details.

16.3 RISKS MITIGATED

A. Data is unencrypted in the database
B. Attackers can retrieve valuable information
C. Non-compliance

16.4 DATAPIPE POLICY

Datapipe shall protect TDE encryption keys against both disclosure and misuse by limiting access to authorized Datapipe database administrator personnel. Such Datapipe personnel are required to sign key custodian forms (SC-1018) stating they understand and accept their key-custodian responsibilities. A password protected backup of these keys are securely distributed to Clients for business continuity propose. If Client becomes in receipt of their keys via a Datapipe provided backup or has privileged logical access to the database, they will also share key custodian responsibilities.

Both the database encryption key (DEK) and key encrypting key (KEK) will leverage the advanced encryption standard (AES) with 256-bits. The TDE keys do not have a cryptoperiod, therefore key rotation based on expiration is not applicable.

However, there will be scenarios when encryption keys need to be changed. This most often happens when a key custodian changes roles, leaves the organization (and had persistent off-line access to encryption keys), or the Client has a specific key rotation policy. If key rotation is required by the Client, a formal change control must be submitted via Datapipe One https://datapipeprod.service-now.com.

17 AUDIT ASSISTANCE

17.1 PURPOSE

Datapipe's audit assistance service provides the relevant policies and evidence clients require to satisfy PCI DSS requirements designated as Datapipe responsibility. The evidence collected also serves as an opportunity for clients to evaluate their configuration for potential changes.

NOTE: **Datapipe cannot provide policies or evidence for controls designated as client responsibility.**

17.2 SCOPE

All managed system components within the cardholder data environment where PCI package has been elected.

17.3 INTRODUCTION

PCI DSS requires an annual validation process, which in part is satisfied with a Report on Compliance (RoC) or Self-Assessment Questionnaire (SAQ). The determination is made based on annual transaction volume and acquiring bank requirements. If the hosted solution requires an SAQ, Datapipe can provide the information necessary to help complete the questionnaire, **however the document must be filled out by the client.**

17.4 RISKS MITIGATED

A. Not being able to provide proper evidence to a QSA
B. Not meeting validation deadlines

17.5 DATAPIPE POLICY

Datapipe will provide various reports and sample data upon request which may include the following information if applicable:

A. General Evidence
    1. Secure System Configuration
    2. System Groups and Users
    3. Report of Issued Remote Access Certificates
    4. Current Patch status
    5. Network Time Protocol configuration
    6. Rouge access point scanning
B. Evidence of Services (As Applicable)
    1. Active Anti-virus protection
    2. Event Log Collection & Archiving
    3. Change Control
    4. Intrusion Detection
    5. Intrusion Prevention
    6. Vulnerability Assessment
    7. Web Application Firewall
    8. Transparent Database Encryption

Datapipe will not be able to determine if the provided list of client user accounts for system components is still warranted. It's the client's responsibility to review the evidence and alert Datapipe with any necessary changes.

NOTE: Datapipe requires at least two weeks lead time and an agenda, if applicable, before an on-site audit to collect the necessary evidence.

18 DATAPIPE FILE ENCRYPTION SERVICE

18.1 SCOPE

All Datapipe supported servers where service has been elected.

18.2 INTRODUCTION

Datapipe's File Encryption Service protects **data-at-rest** by means of access control and encryption technology which is managed outside of the host operating systems. It features a software agent that receives policy from a central Data Security Manager. The agent runs in the file system to provide high-performance encryption and least-privileged access controls for files and directories.

18.3 RISKS MITIGATED

Unauthorized access to sensitive clear text data, and encrypted data

A. Including access by privileged operating system accounts

B. Examples of sensitive data: ePHI, PII, PANs and other protected PCI related data

18.4 DATAPIPE POLICY

Upon service election and completion of initial deployment, Datapipe will send out a welcome letter via Datapipe One which will include an introduction to the service as well as several requests for information (RFI). The information being requested is **required** before Datapipe can proceed with activating the service. If the information is not returned to Datapipe we will be unable to proceed, and your sensitive data will remain unprotected. **Please note** that Datapipe will only protect the data locations that were provided by the Customer during the RFI process.

Upon completion of the configuration process, Datapipe will notify the customer via Datapipe one.

18.4.1 MANAGEMENT MODELS

18.4.1.1 DATAPIPE FULLY MANAGED

Datapipe will do the initial setup/configuration and maintain full administrative management of the entire Vormetric platform. **This is recommended unless you are under the purview of a particular policy or directive explicitly prohibiting it.**

18.4.1.2 DATAPIPE PARTIALLY MANAGED

Datapipe will do the initial setup/configuration, and ongoing management capabilities of the Vormetric platform will be controlled by the customer via the administrator permissions they explicitly grant Datapipe. In this case the customer will own the initial 'System Administrator' account which is the only account type which can be used to create/edit other administrator accounts and set their types/permissions. This allows the customer to control Datapipe's access level, as well as remove Datapipe's access at any time. Datapipe's key management responsibilities are based on the level of access granted to Datapipe by the Client.

18.4.1.3 CUSTOMER MANAGED

Break Glass Support: Datapipe will do the initial setup/configuration of the Vormetric platform and then hand over all administrator credentials to the customer. At this point the customer can reset those passwords leaving Datapipe without any access to the system or access to use keys. In the case of an issue or a support request requiring Datapipe's action the customer will need to 'break glass' and provide Datapipe with appropriate credentials to log in to the system. This may affect how quickly Datapipe can respond to an incident as we will have to wait for credentials to be supplied. It is the customer's responsibility to maintain the required credentials in this model. If the credentials are lost, there is nothing Datapipe can do.

18.4.2 KEY ROTATION

The system does not allow user access to the actual key material, keys are only known by an arbitrary name given to them. Because of this, most often key rotation can be avoided. By default Datapipe will not perform any key rotation. If the customer requires key rotation the customer must inform Datapipe of this via the RFI process and open a support request each time a key rotation is required. Depending on the scenario, downtime may be required for key rotation.

18.4.3 DATA OWNERSHIP

The customer remains the owner, and therefore the ultimate responsible party of their data. Datapipe may be assuming a role of a data custodian to the degree in which the customer prefers or requires. This can be controlled by the 'Management Model' chosen by the customer (defined above, and also provided in the service welcome letter).

18.4.4 DSM BACKUPS

If the customer chooses to maintain (store) the DSM configuration backup files themselves, it will be the customers responsibility to make those files, along with all the required key parts, available to Datapipe should the Client require Datapipe to perform a restore on their behalf.

If the management level requested by the Client warrants Datapipe to backup Clients DSM configuration files. Datapipe will securely transmit and securely store the backup files leveraging strong cryptography as defined in the PCI Glossary.