Crowe

Smart decisions. Lasting value.™

System and Organization Controls Report SOC 2® Type 2

Independent Service Auditor's Report on Controls at a Service Organization Relevant to Security and Availability

Related to Pantheon Systems, Inc.'s Website Operations Service

Under the AICPA's Statement on Standards for Attestation Engagements No. 18 (SSAE No. 18), Section AT-C 205, *Examination Engagements*

For the Period October 1, 2019 to September 30, 2020

PANTHEON

Table of Contents

SECTION I: Independent Service Auditor’s Report

Crowe

Crowe LLP
Independent Member Crowe Global

INDEPENDENT SERVICE AUDITOR'S REPORT

To Pantheon Systems, Inc.

Scope

We have examined Pantheon Systems, Inc.'s (Pantheon or service organization) accompanying description of its Website Operations service titled "System Description Provided by Pantheon Systems, Inc." throughout the period October 1, 2019 to September 30, 2020 (description), based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (description criteria), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period October 1, 2019 to September 30, 2020, to provide reasonable assurance that Pantheon's service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Pantheon uses subservice organizations to provide various functions as described in Section III of the report. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Pantheon, to achieve Pantheon's service commitments and system requirements based on the applicable trust services criteria. The description presents Pantheon's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Pantheon's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Pantheon, to achieve Pantheon's service commitments and system requirements based on the applicable trust services criteria. The description presents Pantheon's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Pantheon's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

The information included in Section V, "Other Information Provided by Pantheon Systems, Inc. That Is Not Covered by the Service Auditor's Report (Unaudited)," is presented by Pantheon management to provide additional information and is not a part of Pantheon's description. Information about Pantheon's responses to identified exceptions has not been subjected to the procedures applied in the examination of the description and of the suitability of the design and operating effectiveness of controls to achieve Pantheon's service commitments and system requirements based on the applicable trust services criteria, and accordingly, we express no opinion on it.

Service Organization's Responsibilities

Pantheon is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Pantheon's service commitments and system requirements were achieved.

Pantheon has provided the accompanying assertion titled "Assertion of Pantheon Systems, Inc.'s Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Pantheon is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are listed in Section IV.

Opinion

In our opinion, in all material respects:

a. the description presents Pantheon's Website Operations service that was designed and implemented throughout the period October 1, 2019 to September 30, 2020, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period October 1, 2019 to September 30, 2020, to provide reasonable assurance that Pantheon's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organizations and user entities applied the complementary controls assumed in the design of Pantheon's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period October 1, 2019 to September 30, 2020, to provide reasonable assurance that Pantheon's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Pantheon's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of Pantheon, user entities of Pantheon's Website Operations service during some or all of the period October 1, 2019 to September 30, 2020, business partners of Pantheon subject to risks arising from interactions with the Website Operations service, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

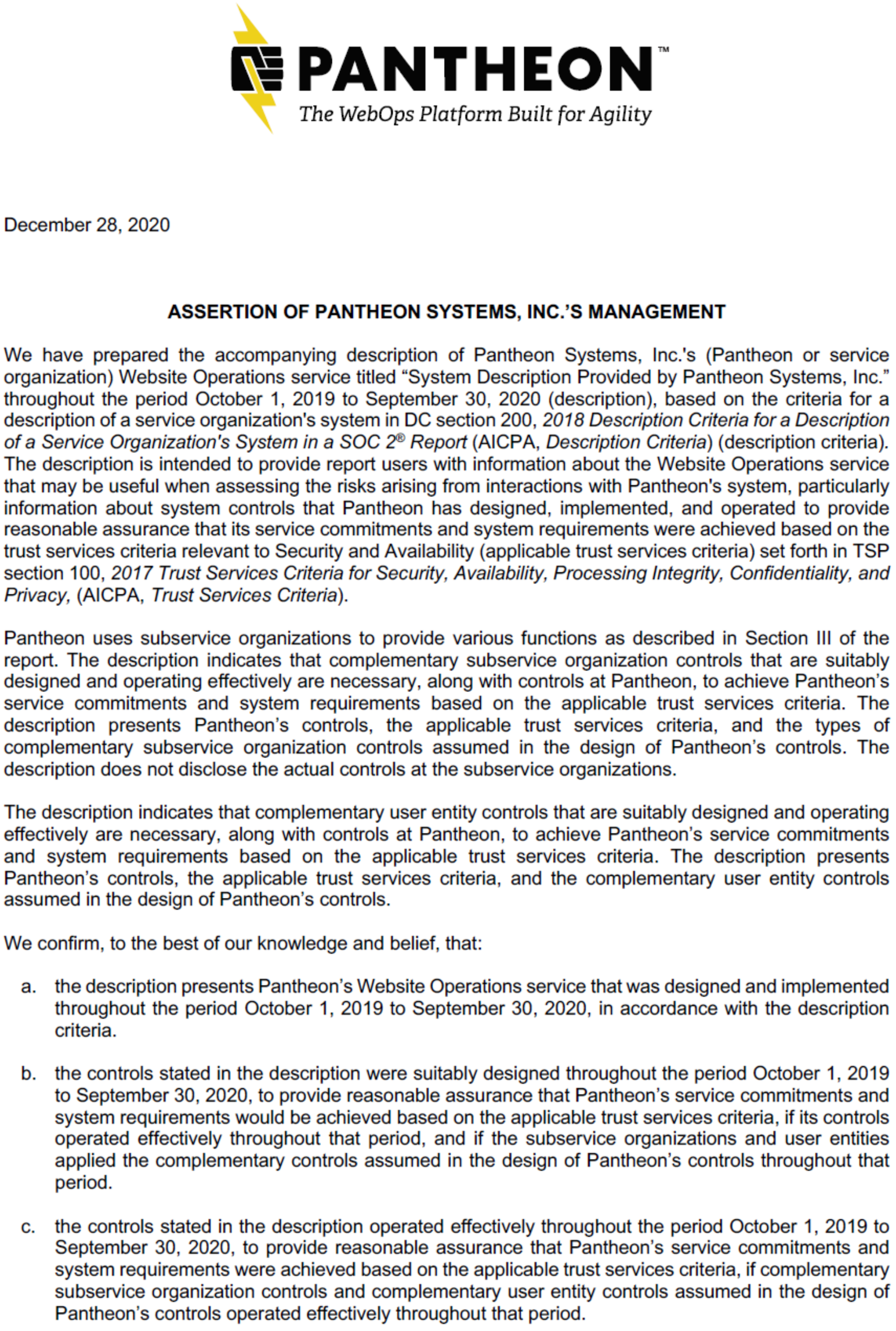
- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

Crowe LLP
Crowe LLP

South Bend, Indiana
December 28, 2020

SECTION II: Assertion of Pantheon Systems, Inc.’s Management



PANTHEON™

The WebOps Platform Built for Agility

December 28, 2020

ASSERTION OF PANTHEON SYSTEMS, INC.’S MANAGEMENT

We have prepared the accompanying description of Pantheon Systems, Inc.'s (Pantheon or service organization) Website Operations service titled “System Description Provided by Pantheon Systems, Inc.” throughout the period October 1, 2019 to September 30, 2020 (description), based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (description criteria). The description is intended to provide report users with information about the Website Operations service that may be useful when assessing the risks arising from interactions with Pantheon's system, particularly information about system controls that Pantheon has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy,* (AICPA, *Trust Services Criteria*).

Pantheon uses subservice organizations to provide various functions as described in Section III of the report. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Pantheon, to achieve Pantheon’s service commitments and system requirements based on the applicable trust services criteria. The description presents Pantheon’s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Pantheon’s controls. The description does not disclose the actual controls at the subservice organizations.

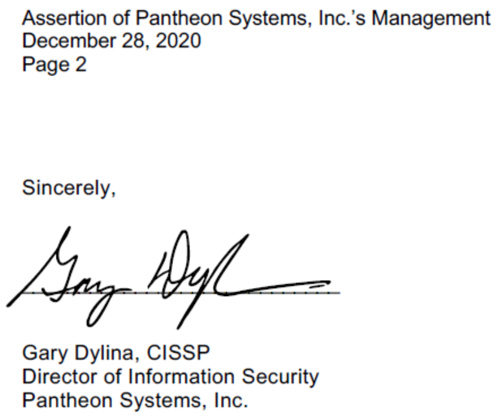
The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Pantheon, to achieve Pantheon’s service commitments and system requirements based on the applicable trust services criteria. The description presents Pantheon’s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Pantheon’s controls.

We confirm, to the best of our knowledge and belief, that:

a. the description presents Pantheon’s Website Operations service that was designed and implemented throughout the period October 1, 2019 to September 30, 2020, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period October 1, 2019 to September 30, 2020, to provide reasonable assurance that Pantheon’s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of Pantheon’s controls throughout that period.

c. the controls stated in the description operated effectively throughout the period October 1, 2019 to September 30, 2020, to provide reasonable assurance that Pantheon’s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Pantheon’s controls operated effectively throughout that period.



Assertion of Pantheon Systems, Inc.'s Management
December 28, 2020
Page 2

Sincerely,

Gary Dylina, CISSP
Director of Information Security
Pantheon Systems, Inc.

SECTION III: System Description Provided by Pantheon Systems, Inc.

Company Overview

Pantheon Systems, Inc. (Pantheon or Company) is a professional WebOps (Website Operations) platform serving customers with Drupal and WordPress websites. Pantheon enables web teams to embrace an agile build-test-learn approach that helps them innovate faster and drive business results. Empowering web teams with agile tools enables them to more effectively differentiate and compete based on digital experience. Using Pantheon, companies can speed their marketing iteration and take their best ideas to market faster while increasing their website's performance, reliability, security, and ability to scale to dramatic increases in volume.

Scope of the Report

Website Operations

Pantheon services covered under this system description can be divided into two logical groups. Website Development Services support customer website development activity and Website Operations Services support running websites developed and managed on the Pantheon Website Operations Platform.

Website Development Services

Pantheon Dashboard

The Pantheon Dashboard exposes administrative interfaces that facilitate the creation and management of website resources. It supports a delegated administration model that allows customers to assign roles appropriate to their team members.

SAML Authentication

Authentication to the Pantheon Dashboard can be configured to use Security Assertion Markup Language (SAML). Using SAML gives customers direct control over session parameters and simplifies user management.

Terminus

Terminus is an extensible command-line interface that supports interactive and scripted access to Pantheon Dashboard functions.

Upstream Distributions

Content Management Systems (CMS) upstream distributions based on the most recent CMS releases are maintained by Pantheon to facilitate customer initiated core updates to Drupal and WordPress.

Custom Upstream Distributions

Custom upstreams may be created and deployed by customers to facilitate managing a customized distribution of Drupal or WordPress across groups of websites.

Source Code Version Control

Source code version control based on open-source Git source code management supports coordinating development and deployment among a team of developers. Artifact based deployments to Test and Live environments ensure reliable and repeatable processes.

Multidev

Pantheon's Multidev feature configures a full stack of website resources to run a branched version of a website under development. This allows a team of website developers to perform nonlinear development then merge the code changes back into the master branch for deployment.

Site Traffic Metrics

Daily, weekly and monthly counts of unique website visitors and page views are collected and reported through the Pantheon Dashboard Site Metrics.

Quicksilver Platform Hooks

Several development and deployment operations can be triggered using operations primitives that can be combined to automate recurring deployment steps.

Website Operation Services

PHP Runtime Environment

The stack of resources configured to run a website on Pantheon consists of a customer configurable runtime environment optimized to support running Drupal or WordPress. Separate stacks are configured for Development, Test and Live environments.

Global CDN

Customer websites are automatically configured to utilize our content delivery network (CDN) deployed in globally distributed points-of-presence. Content Caching, TLS termination, DDoS mitigation, load balancing and disaster recovery services are implemented by our Global CDN.

MySQL Database

Each separate environment is backed by a MySQL compatible database. The database will be either a single-server instance or configured with replica when high-availability options are selected.

Apache Solr Index and Search

Full site indexing and searching is available to customers via integrated Apache Solr search services.

Redis Object Cache

High performance application object caching is available via integrated Redis service.

Valhalla Distributed File System

Our proprietary Valhalla distributed file system serves digital assets to the PHP Runtime. Valhalla provides highly resilient cloud-based file storage that scales horizontally with websites as they scale.

Application Performance Monitoring

New Relic application performance monitoring is integrated with websites to facilitate monitoring and identifying the source of performance issues.

Pantheon Enterprise Gateway

Customers that require communication between their Pantheon hosted website and external resources from a predictable IP address range can configure a Pantheon Enterprise Gateway as a transparent proxy that works consistently and reliably from multiple runtime environments.

Digital Certificates

Pantheon automates adding and renewing Let's Encrypt Transport Layer Security (TLS) certificates for custom domains added to websites.

Disaster Recovery

Websites with the optional Disaster Recovery feature are configured with resources in an alternative data center to support a 99.99% SLA regardless of zone failure.

Automated and On-Demand Backups

Code, database and files from every Live environment are backed up daily and retained for one week. Automatically scheduled backups can be enabled for other environments as required. Individual backups can be triggered on-demand and with one-month or six-month retention periods. Backups are available for download via the Pantheon Dashboard or the Terminus CLI.

Availability Monitoring

Websites with plans that include SLA commitments are monitored for downtime. Customer Support Engineers are alerted and take corrective action when downtime is detected.

Legacy Edge

Prior to implementing the Global CDN service, customer websites were configured to use the TLS termination and caching service now called Legacy Edge. Use of the Legacy Edge service is deprecated.

Email

Pantheon supports customer websites sending email using native CMS methods.

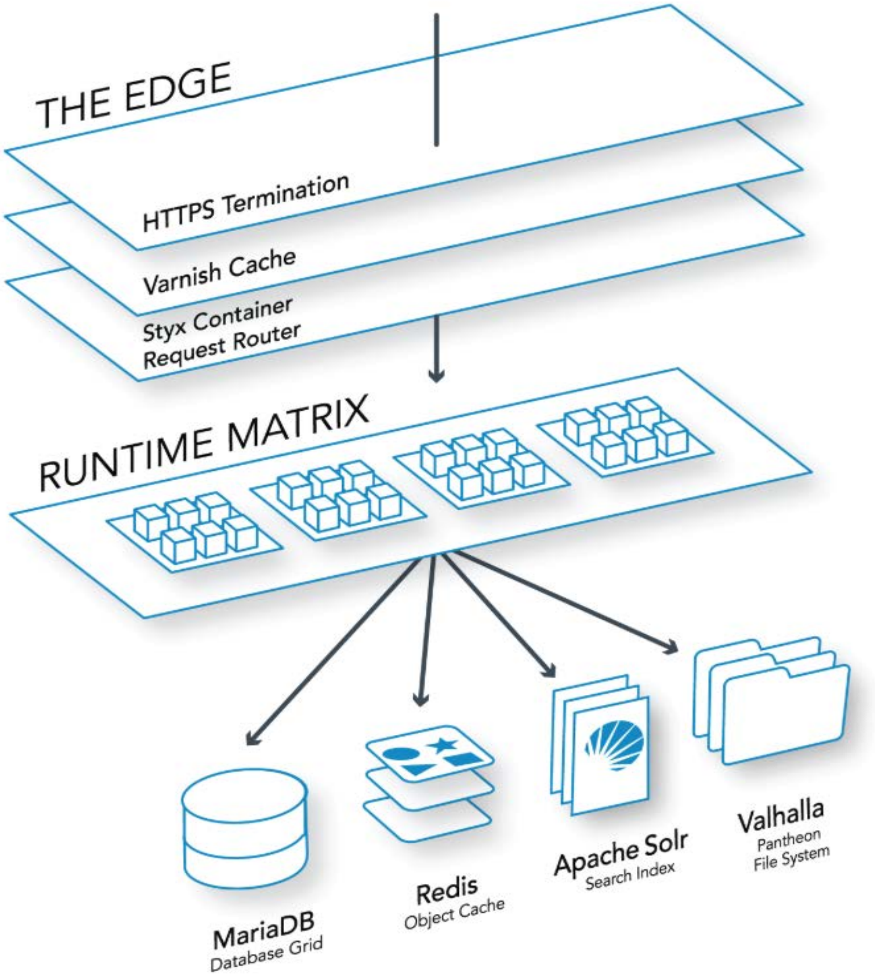


Figure 1: Website Operations Service Logical Architecture Diagram

Principal Service Commitments and System Requirements

Pantheon has communicated the following principal service commitments to their clients relevant to the (in-scope categories) of their Website Operations:

Category	Communication Mechanism	Principal Service Commitments	Related System Requirements
Security	Service Level Agreement	Maintain appropriate administrative, physical, and logical safeguards to protect the security and integrity of the Web Operations Platform and customer data in accordance with Pantheon's security policies.	• CC6.1 • CC6.2 • CC6.3
		Use formal HR processes including: background checks, annual signed acknowledgement of security policy, security awareness training, disciplinary policy and process	• CC1.1 • CC1.5
		Use formal access management processes for the request, review, approval, and provisioning of all Pantheon personnel with access to any production systems.	• CC6.1 • CC6.2 • CC6.3
		Employ least privilege security principles to permit system users to access information they need based on their role in the system while preventing access to information not needed for their assigned job duties.	• CC6.3
		Use industry standard encryption technologies to protect customer data both at rest and in transit where appropriate.	• CC6.7
		Perform annual penetration tests.	• CC7.2
		Perform weekly vulnerability scans of the environment.	• CC7.1
Availability	Service Level Agreement	Maintain a disaster recovery plan to ensure the availability of information following interruption to critical business processes.	• A1.2 • A1.3

Pantheon has also identified control processes to help achieve their principal service commitments – the primary control processes for each commitment are summarized above as "Related System Requirements."

Components of the Website Operations

Software

Pantheon's major software components can be divided into two groups of applications which share a common linkage. Hermes and Terminus interface customers and with Yggdrasil. They implement the Web Development Services. Endpoint REST, Styx, Valhalla, and Backup Workers interface with Yggdrasil. They implement the Web Operations Services.

- Hermes – A customer facing node.js web application and API endpoint that serves the Dashboard to customers and receives connections from the terminus CLI.
- Terminus – An extensible open-source command line client that talks to Hermes.

- Yggdrasil – A Cassandra database backed Python application that provides a back-end API serving the Hermes front-end. It runs workflow automation tasks and performs container orchestration.
- Endpoint REST - A python based endpoint agent that facilitates automated provisioning and management of containers
- Styx - A go based routing proxy
- FuseDAV/Valhalla – A Cassandra and Cloud Storage backed distributed file system that serves files to websites.
- Backup workers - A set of python programs that archive various forms of website data to cloud storage

Infrastructure

Pantheon deploys all services on virtual infrastructure managed by cloud service providers. Wherever possible, resources are configured programmatically with an “infrastructure-as-code” model to ensure reliable deployment of consistent configurations. Pantheon primarily deploys resources in Google Cloud Platform (GCP) across multiple zones and regions.

The Pantheon Global CDN (GCDN) leverages infrastructure managed by Fastly. Fastly has over 65 points-of-presence around the world. GCDN accelerates site performance by caching content closer to website visitors in the Fastly CDN.

As we have no physical servers, Pantheon operates under a shared responsibility model with our cloud services providers who are responsible for physical security, electrical and mechanical infrastructure, network infrastructure and virtualized servers. Pantheon is responsible for configuring, managing, patching and retiring cloud resources.

Data

Pantheon maintains a large logging and monitoring infrastructure. System and application logs are aggregated and enhanced by a logstash cluster then forwarded to a Elasticsearch Logging-as-a-Service provider (logz.io) for real time monitoring and alerting and Amazon S3 for historical records. Logs are retained at our logging provider for 14 days and one year in cold storage at S3.

Customers upload code, data and files to Pantheon as part of normal operations. All customer data stored within the system is classified confidential. As such, it is governed by confidentiality agreements executed between Pantheon and customers or vendors. Pantheon’s information classification and handling requirements are defined in the Pantheon Information Classification and Handling policy. The policy has three categories. They are: public, internal and confidential. Confidential data requires the highest level of security in accordance with relevant security policies, regulations and contractual requirements.

Customer websites generate access data that is aggregated to develop unique visitor and page view statistics displayed in the Customer dashboard. Web server access logs are also generated and retained. Customers wishing to collect and review these logs can retrieve them from their web servers via SFTP.

Records regarding all customer websites, the location of their containers, the memberships of teams developing them and lots of other related data are stored in the Cassandra database backing the Yggdrasil application.

People

Pantheon has a staff of approximately 100 employees organized in the following functional areas to implement and manage Pantheon's internal controls over security and availability:

- Management – responsible for overall security, ensuring enforcement of controls, approving risk assessment, selection and prioritization of risks to mitigate and provide oversight of the Pantheon control environment. Management's role is also to ensure that people are appropriately trained and that systems and processes are in place to meet system uptime, system-wide security, and consistent service execution.
- Engineering – responsible for development of applications, system images, and fixes for deployment, second tier response to application issues, and troubleshooting application incidents. Also, responsible for implementing and operating controls to maintain compliance with all relevant security policies and standards for their area of responsibility, initiation of trouble tickets based on operation triggers, second tier response to operation and security incidents, implementation of approved changes, and troubleshooting incidents.
- Customer success – responsible for fielding customer calls regarding Pantheon customer environments, initiation of trouble tickets based on customer requests, and communicating with customers regarding any scheduled or unscheduled outages or issues through the customer service representatives.
- IT – responsible for provisioning and de-provisioning access rights for all personnel, user right entitlement changes and reviews, provisioning and maintaining laptop and desktop computers, all local office infrastructure and supporting enterprise application users.
- Security – responsible for performing risk assessments and defining control objectives, monitor performance of security controls, initiation of trouble tickets based on security triggers, first and second tier response to security incidents, and operation of security monitoring, measurement, and testing tools.

Procedures

Pantheon has put a set of policies and procedures into place to help ensure the security and availability commitments can be met. Information security policies and procedures define how internal data, systems, and resources are secured and protected from unauthorized access, attempted intrusions, and service disruptions. In addition to the information security policies and procedures, standard operating procedures are documented by departments responsible for specific automated and manual procedures involved in the operation of the Web Operations Platform. Along with standard operating procedures, management has enacted control procedures needed to affect those standards

Subservice Organizations

Pantheon uses third-party service providers (subservice organizations) to assist in the delivery of their Website Operations service. Pantheon has assumed that certain controls have been implemented by the subservice organizations that are necessary, in combination with Pantheon's own controls, to provide reasonable assurance that Pantheon's service commitments and system requirements are achieved based on the applicable trust services criteria.

Below is a listing of the subservice organizations used by Pantheon, as well as the expected complementary subservice organization controls (CSOCs). Please refer to the description content within "Monitoring Activities" for activities performed by Pantheon to monitor these subservice organizations.

Subservice Organization	Service(s) Provided	Expected CSOCs and Applicable Trust Services Criteria
Google Cloud Platform	Virtualized Network, Compute and Storage facilities used to implement the majority of Web Development Services and Web Operations Services	• Managing logical access to the network, virtualization management and storage services for its cloud hosting services where Pantheon Web Operations Platform systems reside. (CC6.3) • Implementing controls for restricting physical access to backup media, system components and data center facilities where Pantheon Web Operations Platform systems reside. (CC6.4) • Ensuring measures to protect against physical and environmental factors impacting availability of data centers and service offerings. (CC6.4) • Implementing controls for the transmission, movement and removal of the underlying storage devices for its cloud hosting services where Pantheon Web Operations Platform systems reside. (CC6.5) • Managing the redundant infrastructure utilized and configured by Pantheon for recovery operations. (A1.2)
Amazon Web Services	Virtualized Storage facilities for platform backup data and platform network Domain Name Service (DNS)	• Managing logical access to the network, virtualization management and storage services for its cloud hosting services where Pantheon Web Operations Platform systems reside. (CC6.3) • Implementing controls for restricting physical access to backup media, system components and data center facilities where Pantheon Web Operations Platform systems reside. (CC6.4) • Implementing controls for the transmission, movement and removal of the underlying storage devices for its cloud hosting services where Pantheon Web Operations Platform systems reside. (CC6.5)

Subservice Organization	Service(s) Provided	Expected CSOCs and Applicable Trust Services Criteria
		• Ensuring measures to protect against physical and environmental factors impacting availability of data centers and service offerings. (A1.2)
Fastly	Virtualized Network facilities used to implement Global CDN service	• Managing logical access to the network, virtualization management and storage services for its cloud hosting services where Pantheon Web Operations Platform systems reside. (CC6.3) • Implementing controls for restricting physical access to backup media, system components and data center facilities where Pantheon Web Operations Platform systems reside. (CC6.4) • Implementing controls for the transmission, movement and removal of the underlying storage devices for its cloud hosting services where Pantheon Web Operations Platform systems reside. (CC6.5) • Ensuring measures to protect against physical and environmental factors impacting availability of data centers and service offerings. (A1.2) • Managing the redundant infrastructure utilized and configured by Pantheon for recovery operations. (A1.2)
Rackspace	Virtualized Network, Compute and Storage facilities used to implement Legacy Edge and Email service	• Managing logical access to the network, virtualization management and storage services for its cloud hosting services where Pantheon Web Operations Platform systems reside. (CC6.3) • Implementing controls for restricting physical access to backup media, system components and data center facilities where Pantheon Web Operations Platform systems reside. (CC6.4) • Implementing controls for the transmission, movement and removal of the underlying storage devices for its cloud hosting services where Pantheon Web Operations Platform systems reside. (CC6.5) • Ensuring measures to protect against physical and environmental factors impacting availability of data centers and service offerings. (A1.2)

Third-Party Monitoring

The Information Security Team obtains and reviews SOC 2 reports from critical subservice organizations prior to enrolling for service and annually after on-boarding. The team will work with service providers to address identified risks promptly and communicate risks to management.

Trust Services Categories, Related Criteria and Controls

The Security and Availability categories and applicable trust services criteria were used to evaluate the suitability of design and operating effectiveness of controls stated in the description. The applicable trust services criteria and related controls are included in Section IV of this report – however, while in Section IV, they are an integral part of Pantheon’s description of their Website Operations.

Controls Relevant to Security

Control Environment

Management Philosophy

Pantheon's control environment reflects the philosophy of senior management concerning the importance of security and availability of our Web Operations Platform.

Pantheon's Information Security Compliance Committee meets quarterly to review changes in the enterprise risk posture. The committee oversees the security activities of Pantheon. The committee is charged with establishing overall security policies and procedures for Pantheon. The importance of security is emphasized within Pantheon through the establishment and communication of policies and procedures and is supported by investment in resources and people to carry out the policies. In designing its controls, Pantheon has taken into consideration the relevance of controls to meet the trust criteria.

Defined organizational structures are made available to internal employees illustrating reporting lines within information systems and management departments. Pantheon performs employee assessment and defines employee goals annually/quarterly

Communication and Information

Pantheon has an information security policy to help ensure that employees understand their individual roles and responsibilities concerning processing and controls to ensure significant events are communicated in a timely manner. An inventory is in place to identify assets associated with information systems to determine accountability and ownership of assets. These include formal and informal training programs and the use of email to communicate time-sensitive information and processes for security and system availability purposes that notify key personnel in the event of problems. All training is required to be completed within thirty (30) days of initiation. Engineering employees are required to complete secure coding training annually. Roles and responsibilities are defined in documented job descriptions to support security commitments. Job descriptions are reviewed on a periodic basis for needed changes or applicable updates.

Pantheon has multiple channels for communicating with external parties. Customer communication procedures are documented on our intranet servers; a monthly "change log" is published to subscribers; a public "status page" is available to display historical uptime performance data as well as post alerts regarding performance or availability issues; salesforce.com CRM contains information that can be used to selectively address different customer populations, and the Pantheon Dashboard with integrated ticket management. Each of our subservice organization has a support function that supports our engineering opening tickets. Management maintains contracts with relevant external parties, including business partners, customers, service providers, and vendors.

Risk Assessment

Pantheon regularly reviews the risks that may threaten the achievement of its service commitments and system requirements related to security based on the applicable trust services criteria set forth in TSP section 100, 2017 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

The Information Security Team assesses risks on an ongoing basis. When performing these assessments, the risk level for a threat/vulnerability is expressed as a function of the likelihood of an attempt to exploit a given vulnerability and the magnitude of the impact should the vulnerability be exploited. This is done during monthly meetings with engineering personnel to produce a monthly assessment. This activity in addition to reviewing and acting upon security event logs and performing vulnerability scans provides data used to create a formal quarterly risk assessment report.

A copy of this report is presented to the Enterprise Risk Committee each quarter to surface risk to senior management and allow committee members to factor risk reduction into forward planning. The Enterprise Risk Committee charter has been established to outline the responsibilities and due diligence of the committee

The Information Security Compliance Committee considers developments in technology and the impact of applicable laws and regulations on Pantheon's security policies as part of its annual policy review. Management considers security requirements when selecting, implementing, and managing third-party solutions.

Changes in security threats and risks are reviewed by Pantheon, and updates to existing control activities and information security policies are performed as necessary. Management segregates duties and areas of responsibility to reduce opportunities for unauthorized or accidental misuse of data.

Monitoring Activities

In addition to the daily oversight, weekly vulnerability scans and use of log monitoring, management provides further security monitoring through annual internal audits information security posture relative to the Cloud Security Alliance Cloud Controls Matrix.

Vendor Monitoring

Written policies and procedures are in place establishing guidelines in regards to third party providers. All agreements for critical vendors must be reviewed by the legal department prior to the signing of the agreement contract. The Information Security Team obtains and reviews SOC 2 reports from critical subservice organizations prior to enrolling for service and annually after on-boarding. The team will work with service providers to address identified risks promptly and communicate risks to management.

Evaluating and Communicating Deficiencies

Defects or weaknesses in internal controls may surface from many sources including monitoring procedures, internal audits, penetration testing and other sources

Control Activities

Security Management

Pantheon has a dedicated information security team consisting of a Director of Information Security a team of Security Engineers responsible for the management of information security throughout the Company. They hold positions on the Information Security Compliance Committee and are required to annually sign and acknowledge their review of the information security policies. They are responsible for developing, maintaining, and enforcing Pantheon's information security policies. The Information Security policy is reviewed annually by the Director of Information Security, CTO, and COO, and it is approved by the Information Security Compliance Committee.

As the information security team maintains security, it monitors known incidents and patches as well as results from recent vulnerability assessments and addresses necessary changes to the policies and procedures. Such changes can include a reclassification of data, a reassessment of risk, changes in incident response plans, and a verification of responsibilities for authorizing and monitoring accesses. Changes are reviewed and communicated during weekly Security Team meetings and through system alerts. Internal audit plan is reviewed and approved by the Audit Committee on an annual basis. Annual updates are provided to the audit committee.

During annual security training and awareness programs, management ensures communication of the latest security policies as well as written job descriptions for security management.

Additionally, management is responsible for ensuring business associate agreements are current for third parties and for updating the annual IT risk assessment.

Security Policies

Pantheon has created a body of written policies to establish a common understanding of rules and procedures governing development, deployment, operation and management of the Pantheon Web Operations Platform. These policies are managed by the Director of Information Security. A complete list of the policy titles follows:

Acceptable Use	Incident Management & Response
Access Control	Information Classification and Handling
Asset Management	Information Security
Backup	Network Security
Business Continuity	Physical Security
Change Management	Third-Party Management
Employee Privacy	Vulnerability Management
Human Resources	

Personnel Security

Background checks are performed on new all new employees. They are required to review and acknowledge their receipt of relevant security policies. Once employed, employees are subject to Pantheon's procedures for accessing systems and sanctions for violating Pantheon's information security policy. Employees are instructed to report potential security incidents to the IT Team.

Logical and Physical Access

Logical Security

Pantheon management has established controls to ensure that access to the Web Operations Platform production environment is restricted to those who require access based on role and business justification. The Director of Engineering or Director of Information Security approve the assignment of production access permissions to internal users based upon job responsibilities. Engineering personnel are responsible for administering and enforcing access rights to the production environment as well as user provisioning/de-provisioning related activities.

Pantheon information security policies and standard operating procedures are documented and available to employees on the team collaboration software, Confluence, for all Company personnel to review and understand their responsibility for adhering to the associated organizational standards and security requirements. These policies are reviewed by the Information Security Compliance Committee on at least an annual basis. In addition, personnel are required to complete security awareness training as part of the on-boarding process and each calendar year to help ensure awareness of security policies and procedures. The Pantheon information security team tracks completion of the annual security awareness training to ensure all employees have completed the training.

Antivirus protection technologies are used on workstations to ensure the detection and prevention of malware. The antivirus software is configured to check for definition updates.

Access Authentication and Authorization

Access to system information is protected by multiple authentication and authorization mechanisms. The production environment is administered remotely and all access must be performed through connections secured by strong authentication. Internal users authenticate to production servers over secure shell (SSH) encryption protocol using uniquely assigned SSH key-pair in which the private key is enabled only with the internal user’s unique username and SSH key stored in a hardware token.

Access to production resources is controlled using permissions associated with Pantheon engineering staff and strictly controlled system accounts. Access to migrate changes to the production environment is restricted to appropriate personnel. After a user account and public-private keys have been generated, the accounts, including the groups the individual belongs to, are propagated to the production servers using Chef, a configuration management tool. Chef is used to ensure that all servers have a consistent configuration and access rights are up to date. Management has restricted the ability to create accounts in the production environment as well as administrative access privileges within the production environment to authorized engineering personnel.

Pantheon uses the Okta IDaaS solution to manage access to corporate resources which include, but are not limited to, G-Suite, GitHub, Confluence, Jira, BambooHR, Salesforce and logz.io. Password requirements for Company's network and application system is defined in the Company's Information Security Policy. Each user is assigned a unique user ID, password, and a second-factor authentication method via Okta. The IT team is responsible for managing access rights within Pantheon org. Administrative access is restricted to authorized IT personnel.

Pantheon Application Access Authentication and Authorization

Pantheon utilizes the Pantheon Dashboard application to provision or de-provision customer organizations. Once the customer organization is provisioned, the customer is responsible for administering their Company team member access entitlements. This includes, but is not limited to, user administration activities (provisioning, de-provisioning, delegating administrative access, and reviewing access entitlements) and establishing configuration settings, which may include SAML authentication.

Access Requests and Access Revocation

Pantheon has established an on-boarding process for hiring new employees to minimize the risk of inadvertent failure and to help ensure that new employees understand the policies for maintaining a secure workplace. All employees are required to sign an electronic acknowledgment indicating that they have received, read, and agree to adhere to the established guidelines outlined in the employee handbook and the information security policy. Pantheon requires performance of background verification checks for employees at the time of hire. Background checks include examination of criminal conviction records and social security number (SSN) verification, address history, and previous employment.

A formal process has been established for managing user accounts and controlling access to Pantheon’s resources. IT personnel are responsible for assigning and maintaining access rights to the corporate systems based on the individual’s job role and department. All access to the production environment is managed by the Engineering team. Upon notification of an employee termination, HR personnel provide IT personnel a termination notice via email to ensure that employees do not retain system access after their termination date. The IT team will create a Jira issue to track de-provisioning of critical systems. The teams responsible for all systems promptly remove any corporate and/or production environment access for the terminated employee. Management requires all access requests to be formally documented to ensure all activities are completed. In addition, to help ensure access privileges are appropriate, IT personnel and the engineering team complete an audit of the corporate and production environment accounts on a quarterly basis. If any individual is identified to have inappropriate access, the issue is remediated immediately.

Electronic badge reader authentication is required for access to the main entrance. Visitors to Pantheon facilities must be escorted by Pantheon employees at all times and are required to check in and out upon arrival and departure. On an annual basis, Patheon management reviews the list of personnel with access to the Pantheon facilities. Badge access to operations facilities is revoked in a timely manner in accordance with physical security standards.

System Operations

Data Replication, Backup and Disaster Recovery

Automated systems are in place to manage recurring processes such as production jobs and data backups. Resources required for disaster recovery and high availability are replicating data to multiple databases on separate availability zones and to cloud storage. Pantheon's system monitoring tools are configured to automatically alert the engineering department if replication lag time falls significantly behind production databases. Pantheon's engineering team investigates all alerts and resolves delays promptly. Critical applications and services are distributed across multiple nodes to eliminate single points of failure.

Customer website data in Pantheon Web Operations Services is backed up daily to Google Cloud Storage. These backups are available to customers for download, export or self-service rollback / recovery. They also contain data that may be used to recover from unplanned unavailability of cloud resources.

Pantheon utilizes regular database backups recorded to Amazon S3 for production Web Development Services backup data. As part of the Amazon S3 service offering, all data stored within Amazon S3 includes cross-region replication which automatically replicates the data across different AWS regions. Pantheon performs a test restore of platform backup data on an annual basis to ensure that systems can be recovered in the event of a catastrophic failure.

Recovery plans are documented in disaster recovery plan which defines the roles and responsibilities of relevant personnel involved in executing recovery procedures. Disaster recovery procedures are developed and documented based on a formal risk assessment to identify threats to availability of the Pantheon systems. The recovery procedures are tested on an annual basis. A Disaster Recovery feature has been established and configured for Pantheon's Web Operations Services solution to support customer websites running in multiple availability zones. In the event one zone becomes unavailable, a complete copy the customer site is ready for activation in another zone. Secondary site established and are kept in a warm state, ready to be failed over to. Environmental controls at the Google Cloud and Amazon datacenters are monitored by each cloud provider. Pantheon monitor using SOC reports or other forms of validation.

Incident Response

Incident response and escalation policies and procedures are in place to efficiently and effectively manage unexpected incidents impacting the business. The incident response process defines activities for identifying and mitigating security breaches, and managing communications with Pantheon cloud personnel and customers. The actions taken to resolve and contain the incidents are documented in our Incident Command repository in our Team Drive. When an issue is detected, the On-Call Engineer will examine and attempt to troubleshoot the issue and escalate the issue if needed.

Intrusion detection system / intrusion prevention system is configured to identify, log and report potential security breaches and other incidents which could impact security of systems. Events are monitored and evaluated by the information security team.

Pantheon utilizes online collaboration tools and email for communicating and collaborating to resolve any identified incidents. The information security team is responsible for the identification, resolution, and communication of all security related incidents to all possibly impacted parties. Customers are responsible for reviewing incident and service level reports provided by Pantheon, where applicable and reporting any issues based on terms of the service agreement.

Significant incidents will be followed by a formal post-mortem incident retrospective that includes a continuous improvement "Kaizen" to identify improvements to processes or systems that would avoid the problem, detect it sooner or recover more quickly. Identified improvements are recorded in Jira issues for action by engineering team members.

System Monitoring

Pantheon monitors the internal control environment as a routine part of operations. Pantheon has implemented a set monitoring tools that record performance and capacity data for the production environment and production support systems. Minor issues raise a visible alert on an On-Call Engineer Dashboard. Alerts that require urgent attention or manual intervention will initiate a notification process that starts with automatically paging the On-Call Engineer and escalates to the Director of Engineering if necessary.

Event logging

Logz.io, a SaaS-based log collector and parsing service, is used extensively to collect logs and monitor for anomalous system conditions as well as for forensic analysis after an incident. All servers send all system logs as well as all application logs to logz.io. Logs for production systems are continuously monitored for evidence of suspicious activity or unauthorized access. Alerts are set to send messages to the Security Team if certain thresholds of various messages are exceeded.

Vulnerability Assessments and Penetration Tests

Vulnerability assessments of the production network and the web application are performed continuously on a weekly cycle to identify potential security vulnerabilities. If a potential or actual security vulnerability is encountered, security personnel assess the severity, work to identify the cause and remediate consistent with our vulnerability management policy. In addition, penetration testing is performed annually by a third-party vendor to identify security weaknesses. Security personnel retain the penetration testing reports, monitor the results of the assessment within the report and create remediation plans to remedy potential vulnerabilities.

Encryption

To protect data while in transit, customer sessions to the Pantheon web servers are transmitted utilizing Hypertext Transfer Protocol Secure (HTTPS) and Transport Layer Security (TLS) encryption protocols and allow for strong encryption. Pantheon utilizes a trusted certificate authority to issue a TLS digital certificate to inform users that the Pantheon website is secure. Pantheon utilizes 256-bit AES volume encryption provided by cloud service providers to protect data at rest when it is available.

Change Management

Pantheon utilizes the agile software development methodology for application and API development. Formal Software Development Life Cycle (SDLC) is in place for new development and program enhancement. Program change documents and security best practices including policies, procedures, and guidance documents are documented on the Pantheon wiki. Planned releases are performed on a bi-weekly sprint schedule with releases first deployed to a “preview” (sandbox) environment. Releases or changes deployed to production are generally for bug fixes or new system functionality. All production changes are documented and tracked in a ticketing system. Separate development, test and production environments are maintained. By policy, changes are tested in the test environment prior to implementation. The production change request process enforces and records request authorization, code review, automated testing (where applicable), migration approval, and implementation. Changes are deployed to production via an automated build-test-deploy pipeline after approval. Only authorized developers have access to source code repository (Github) to modify code as required

Approved changes are performed or managed directly by authorized engineering personnel. Emergency changes undergo a variety of testing ranging from peer testing to automated testing prior to the release into production and approvals may occur after the fact based on the severity of the issue being addressed.

Firewalls/Security Groups are setup with specific rules to only allow access to authorized parties. All changes to the Firewall/Security Groups must follow the normal change management process.

Patch Management

A formal infrastructure change management policy is in place that defines and implements rules regarding information systems and infrastructure. Information security and engineering personnel monitor for recommended critical patches and upgrades on an on-going basis to mitigate damage to Pantheon operations resulting from exploitation of published vulnerabilities. The three main inputs for identifying vulnerabilities are by reviewing security notifications from authorized technology / vendor/ or security sources, through internal and external network and application tests, and/or by a customer or externally reported security issue.

When a potential vulnerability has been identified, security and engineering personnel will assess the vulnerability and determine the applicability and necessity for implementing selected patches and upgrades based on risk. If a patch is deemed necessary to mitigate the detected vulnerability, Information security and engineering personnel will create a Jira ticket to manage and track the patch installation until resolution.

Deployment of patches will follow the standard review-build-test-deploy process to ensure comprehensive patch coverage and reliable provisioning of infrastructure with all required patches.

Controls Relevant to Availability

Pantheon utilizes multiple systems to continuously monitor security events, latency, packet loss, hops, network performance, and virtual server performance in its production environment. The systems are designed to prioritize events that need immediate attention as well as tracking potentially critical issues and general system health. Further, Pantheon has configured the enterprise monitoring applications to notify personnel in the event of any issues that will impact system availability. Documented escalation procedures are in place to initiate corrective actions for routine issues. Personnel utilize online collaboration tools to view and respond to critical alerts relating to issues in real-time.

Capacity monitoring is performed to ensure that resource utilization is within acceptable limits and below maximum utilization for a required resource. Capacity utilization is reviewed every two weeks to ensure critical resource capacity is available to accommodate expected growth without interruption.

Complementary User Entity Controls

The Pantheon Website Operations control structure is designed with the assumption that certain controls would be implemented by user entities. This section describes user entity controls identified by Pantheon as necessary to achieve certain applicable trust services criteria.

The user entity controls described below should not be regarded as a comprehensive list of all controls which should be employed by user entities. There may be additional controls that would be appropriate to address Security and Availability concerns which are not identified in this report. Each user entity is responsible for the identification, implementation and operating of appropriate controls to address their specific concerns as related to Pantheon's Website Operations.

Complementary User Entity Controls	Relevant Trust Services Criteria
Customers are responsible for ensuring their information security requirements are considered in the deployment, configuration, and modification of their instance of Web Operations Platform services.	Common Criteria 2
Customers are responsible for applying updates to core CMS	Common Criteria 2
Customers are responsible for establishing policies and procedures for installing and maintaining third-party extensions such as Drupal Modules and WordPress Plugins.	Common Criteria 2
Customers are responsible for opting into the Data Processing Amendment as appropriate.	Common Criteria 2
Pantheon will provide updated distributions of Content Management System (CMS) software for convenience. Customers are solely responsible for updating and maintaining the security of all code deployed into Pantheon.	Common Criteria 6
Customers are responsible for provisioning website resources and team member roles consistent with organizational policies.	Common Criteria 6
Customers are responsible for enrolling for SAML authentication consistent with organizational authentication policies.	Common Criteria 6
Customers are responsible for reviewing users' access rights periodically to ensure they are consistent with organizational policies.	Common Criteria 6
Customers are responsible for removing users' access rights consistent with organizational policies.	Common Criteria 6
Customers are responsible for establishing responsibilities and procedures to respond to relevant information security incidents pertaining to the use of Pantheon services.	Common Criteria 7
Customers should train administrators and developers on their responsibilities and organizational procedures for identifying, handling, and responding to security incidents pertaining to the use of Pantheon services.	Common Criteria 7
Customers should contact Pantheon if there are any issues with service availability or security including unauthorized use of their password or account	Common Criteria 7
Customers are responsible for ensuring that individuals creating and/or updating profiles or administrative access have the proper authorization.	Common Criteria 8

Complementary User Entity Controls	Relevant Trust Services Criteria
Customers are responsible for ensuring any application software which they deploy onto Pantheon follows their specific software change management policies and procedures.	Common Criteria 8
Customers are responsible for reviewing and testing feature and product releases and evaluating their impact consistent with the organization's needs.	Common Criteria 8
Customers are responsible for ensuring that customer data is exported and deleted from the Pantheon prior to account termination.	Common Criteria 8
Customers are responsible to maintain their own archival copies of code, data and files.	Availability
Customers with strict Recovery Time Objective (RTO) requirements should consider opting in to Site Disaster Recovery service	Availability

SECTION IV: Trust Services Criteria, Related Controls, and Tests of Controls Relevant to Security and Availability

Overview of Crowe LLP's Test Procedures

Our examination was restricted to the control activities specified by Pantheon Systems, Inc.'s (Pantheon or service organization or Company) management in Sections III and IV of this report to address the applicable trust services criteria. Our examination did not extend to any other control procedures, including those that may be described in Section III but not listed in Section IV.

The following table clarifies certain terms that may be used within this section to describe the nature of the tests of controls performed:

Type of Testing	Description
Observation	Observed the application, performance or existence of the specified controls as described.
Inspection	Inspected manually or systematically maintained documentation to evidence performance of the specified controls.
Reperformance	Reperformed the specified controls as performed by management to compare our independent results to those of management.

As Crowe conducted inquiry with appropriate Pantheon personnel for all controls, inquiry was not listed specifically by each control within Section IV.

In addition, when using information produced by Pantheon, we performed procedures as required by AT-C section 205 to validate whether the information was sufficiently reliable for our purposes by obtaining evidence about the completeness and accuracy of such information, as well as evaluating whether the information produced was sufficiently precise and detailed for our purposes.

Common Criteria Relevant to Security, Availability, Confidentiality, Processing Integrity, and Privacy

Trust Services Criteria	Pantheon's Controls	Tests of Controls	Results
CC 1 – Control Environment			
CC 1.1 The entity demonstrates a commitment to integrity and ethical values.	Background screening is conducted on all new hires full-time employees prior to employment.	Inspected background checks for a sample of new employees to determine if background screening checks were completed.	**Exception Noted:** 3 of 5 sampled new hires did not have a completed background check.
	Roles and responsibilities are defined in documented job descriptions to support security commitments.	Inspected job descriptions for a sample of roles from the organization chart to determine if responsibilities are defined.	No exceptions noted.
	Pantheon requires all employees to formally acknowledge their understanding of the Employee Handbook and Code of Conduct on an annual basis.	Inspected policy acknowledgements for a sample of current employees to determine if they acknowledged the Employee Handbook and Code of Conduct.	No exceptions noted.
CC 1.2 The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Enterprise Risk Committee meets on a quarterly basis to discuss organizational objectives and initiatives, including Information Technology (IT).	Inspected meeting minutes for a sample of quarters to determine if the Enterprise Risk Committee met to discuss organizational objectives and initiatives, including Information Technology (IT).	No exceptions noted.

Trust Services Criteria	Pantheon's Controls	Tests of Controls	Results
CC 1 – Control Environment			
	The Enterprise Risk Committee reviews and approves the policies around information security.	Inspected Pantheon policies and standards to determine if policies and standards are up to date and cover the following areas: • Information Security Policy • Access control • Physical security • Vendor risk management • Incident management • Business continuity • Data privacy Inspected the policy revision control log to determine if policies were reviewed in the past year by the Enterprise Risk Committee.	No exceptions noted.
CC 1.3 Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Defined organizational structures are made available to internal employees illustrating reporting lines within information systems and management departments.	Inspected organizational charts to determine if charts are made available to employees and reporting lines are established.	No exceptions noted.
	Roles and responsibilities are defined in documented job descriptions to support security commitments.	Inspected job descriptions for a sample of roles from the organization chart to determine if responsibilities are defined.	No exceptions noted.
CC 1.4 The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	A security awareness training program has been implemented to communicate security policies to all employees. All training is required to be completed within thirty (30) days of initiation.	Inspected training completion for a sample of new employees to determine if they have completed the Security and Awareness training within 30 days of hire date.	No exceptions noted.
	Engineering employees are required to complete secure coding training annually.	Inspected training completion for a sample of engineering employees to determine if they have completed the technical training.	No exceptions noted.

Trust Services Criteria	Pantheon's Controls	Tests of Controls	Results
CC 1 – Control Environment			
CC 1.5 The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Pantheon requires all employees to formally acknowledge their understanding of the Employee Handbook and Code of Conduct on an annual basis.	Inspected policy acknowledgements for a sample of current employees to determine if they acknowledged the Employee Handbook and Code of Conduct in the current period.	No exceptions noted.
	Pantheon performs employee assessment and defines employee goals annually.	Inspected performance evaluations for a sample of active employees to determine if a performance evaluation was completed in the current period.	No exceptions noted.

Trust Services Criteria	Pantheon's Controls	Tests of Controls	Results
CC 2 – Information and Communication			
CC 2.1 The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	The Compliance team meets on a quarterly basis to monitor applicable laws and regulations for potential impact to internal controls and organizational objectives.	Inspected Compliance team meeting agendas for a sample of quarters to determine if legal and regulatory changes are being reviewed for impact to internal controls and organizational objectives.	No exceptions noted.
	Security event logs are generated, correlated, and analyzed to identify risks that impact the security of applications, infrastructure, and operations.	Inspected the monitoring application, configurations, and log results to determine if security monitoring applications are in place and appropriately configured.	No exceptions noted.
	Formal Software Development Life Cycle (SDLC) is in place for new development and program enhancement. The policy is reviewed on an annual basis.	Inspected documented policies and procedures to determine that there is a formal SLDC plan in place and it is approved annually.	No exceptions noted.
	An annual control self-assessment is conducted by Internal Audit in conjunction with the various control/process owners to ensure the accountability and accuracy of the internal control framework.	Inspected the most updated internal audit report to determine if a self-assessment was performed.	No exceptions noted.
CC 2.2 The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Policies and standards are available to all employees via intranet.	Inspected the intranet to determine if corporate policies and standards are located on the Pantheon intranet and available for employees to access.	No exceptions noted.
	Roles and responsibilities are defined in documented job descriptions to support security commitments.	Inspected job descriptions for a sample of roles from the organization chart to determine if responsibilities are defined.	No exceptions noted.
	A security awareness training program has been implemented to communicate security policies to all employees. All training is required to be completed within thirty (30) days of initiation.	Inspected training completion for a sample of new employees to determine if they have completed the Security and Awareness training within 30 days of hire date.	No exceptions noted.

Trust Services Criteria	Pantheon's Controls	Tests of Controls	Results
CC 2 – Information and Communication			
CC 2.3 The entity communicates with external parties regarding matters affecting the functioning of internal control.	Management maintains contracts with relevant external parties, including business partners, customers, service providers, and vendors.	Inspected the Communication Policy / Procedures to determine if there are rules defined for external communications. Inspected contracts for a sample of new vendors and customers to determine if contracts have been established.	No exceptions noted.
	On a monthly basis the Communication team sends out newsletters to clients to notify and alert on any application changes such as regulatory updates.	Inspected newsletters for a sample of months to determine if application and regulatory updates are communicated to clients.	No exceptions noted.

Trust Services Criteria	Pantheon's Controls	Tests of Controls	Results
CC 3 – Risk Assessment			
CC 3.1 The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	On a quarterly basis, the Risk Committee meets to identify map risks to the Company objectives for the upcoming quarter.	Inspected Risk Committee meeting minutes for a sample of quarters to determine if management identified risks and mapped to Company objectives.	No exceptions noted.
	An Information Security Risk Assessment is completed on monthly basis that evaluates technical and organizational assets and the threats to those assets. The risk assessment is updated and approved monthly	Inspected the risk assessment for a sample of months to determine if management performed an information security risk assessment to evaluate internal and external threats to organizational assets.	No exceptions noted.
CC 3.2 The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	The Enterprise Risk Committee charter has been established to outline the responsibilities and due diligence of the committee.	Inspected the Enterprise Risk Committee charter to determine it is in place and documented.	No exceptions noted.
	An Information Security Risk Assessment is completed on monthly basis that evaluates technical and organizational assets and the threats to those assets. The risk assessment is updated and approved monthly.	Inspected the risk assessment for a sample of months to determine if management performed an information security risk assessment to evaluate internal and external threats to organizational assets.	No exceptions noted.
CC 3.3 The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Management segregates duties and areas of responsibility to reduce opportunities for unauthorized or accidental misuse of data.	Inspected the Access Control Policy to determine if appropriate requirements for segregation of duties are documented and up-to-date.	No exceptions noted.
	An Information Security Risk Assessment is completed on monthly basis that evaluates technical and organizational assets and the threats to those assets. The risk assessment is updated and approved monthly.	Inspected the risk assessment for a sample of months to determine if management performed an information security risk assessment to evaluate internal and external threats to organizational assets.	No exceptions noted.

Trust Services Criteria	Pantheon's Controls	Tests of Controls	Results
CC 3 – Risk Assessment			
CC 3.4 The entity identifies and assesses changes that could significantly impact the system of internal control.	Management considers security requirements when selecting, implementing, and managing third-party solutions.	Inspected the Third-Party Management Policy to determine if it contains detailed on-boarding and off-boarding requirements when managing third-party solutions.	No exceptions noted.
	On a quarterly basis, the Risk Committee meets to identify map risks to the Company objectives for the upcoming quarter.	Inspected Risk Committee meeting minutes for a sample of quarters to determine if management identified risks and mapped to Company objectives.	No exceptions noted.
	Information Security Governance Committee regularly meets quarterly to discuss IT initiatives and projects and monitors for changes in the environment.	Inspected Information Security Governance Committee meeting minutes for sample of quarters to determine if the Committee met to discuss IT initiatives and projects and monitors for changes in the environment.	No exceptions noted.

Trust Services Criteria	Pantheon's Controls	Tests of Controls	Results
CC 4 – Monitoring Activities			
CC 4.1 The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Weekly internal and external vulnerability scans are conducted. Any findings are assessment impact and severity and remediation efforts are formally documented and tracked.	Inspected vulnerability scans for a sample of weeks to determine if internal and external vulnerability scans were performed and issues tracked to remediation.	No exceptions noted.
	Management contracts a third party to complete annual penetration tests. Results and recommended for improvement are reported to management.	Inspected the results of the most recent penetration test and inspected documentation to determine if management tracks the remediation of any issues identified.	No exceptions noted.
	Annual control self-assessment is conducted by Internal Audit in conjunction with the various control/process owners to ensure the accountability and accuracy of the internal control framework.	Inspected the most updated internal audit report to determine if a self-assessment was performed in the current period.	No exceptions noted.
	Internal audit plan is reviewed and approved by the Audit Committee on an annual basis. Annual updates are provided to the audit committee.	Inspected the most updated internal audit plan is in place and has been reviewed by the Audit Committee on an annual basis.	No exceptions noted.
CC 4.2 The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	All significant findings noted during Internal Audit procedures are discussed during quarterly Risk Committee meetings.	Inspected Risk Committee meeting minutes for sample of quarters to determine if significant findings were discussed.	No exceptions noted.
	Weekly internal and external vulnerability scans are conducted. Any findings are assessment impact and severity and remediation efforts are formally documented and tracked.	Inspected vulnerability scans for a sample of weeks to determine if internal and external vulnerability scans were performed and issues tracked to remediation.	No exceptions noted.
	Management contracts a third party to complete annual penetration tests. Results and recommended for improvement are reported to management.	Inspected the results of the most recent penetration test and inspected documentation to determine if management tracks the remediation of any issues identified.	No exceptions noted.

Trust Services Criteria	Pantheon's Controls	Tests of Controls	Results
CC 5 – Control Activities			
CC 5.1 The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Information Security Governance Committee is responsible for reviewing and ensuring security policies are accurate and up-to-date.	Inspected Pantheon policies and standards to determine if policies and standards are up to date and cover the following areas: • Anti-virus policy • Server hardening procedures • End of life procedures • Encryption policies and procedures • Data classification, handling, retention	No exceptions noted.
	A security awareness training program has been implemented to communicate security policies to all employees. All training is required to be completed within thirty (30) days of initiation.	Inspected training completion for a sample of new employees to determine if they have completed the Security and Awareness training within 30 days of hire date.	No exceptions noted.
CC 5.2 The entity also selects and develops general control activities over technology to support the achievement of objectives.	Security event logs are generated, correlated, and analyzed to identify risks that impact the security of applications, infrastructure, and operations.	Inspected the monitoring application, configurations, and log results to determine if security monitoring applications are in place and appropriately configured.	No exceptions noted.
	Pantheon maintains multiple levels of system access based upon each employee's role and responsibilities. When a new hire starts HR will notify IT of the employee's start date and job title. IT will provision access to defined role based groups based on the job title in HR email.	Inspected request forms for sample of new hires to determine if access was requested by HR and provisioned based on job responsibility to the Pantheon infrastructure.	No exceptions noted.
	IT is notified of terminations by email from HR. Access is removed/disabled from the network, and in-scope applications upon notification.	Inspected termination forms for a sample of terminations to determine if HR notified IT in a timely manner and access removal was documented in a HelpIT ticket.	No exceptions noted.

Trust Services Criteria	Pantheon's Controls	Tests of Controls	Results
CC 5 – Control Activities			
CC 5.3 The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Information Security Governance Committee is responsible for reviewing and ensuring security policies are accurate and up-to-date.	Inspected Pantheon policies and standards to determine if policies and standards are up to date and cover the following areas: • Anti-virus policy • Server hardening procedures • End of life procedures • Encryption policies and procedures • Data classification, handling, retention	No exceptions noted.
	Policies and standards are available to all employees via intranet.	Inspected the intranet to determine if corporate policies and standards are located on the Pantheon intranet and available for employees to access.	No exceptions noted.

Trust Services Criteria	Pantheon's Controls	Tests of Controls	Results
CC 6 – Logical and Physical Access			
CC 6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	An inventory is in place to identify assets associated with information systems to determine accountability and ownership of assets.	Inspected the asset inventory to determine if assets are identified, inventoried, and accounted for.	No exceptions noted.
	Access to the Company's network require a user identification, a password and multi-factor authentication.	Inspected configuration settings to determine if access the network requires a unique user name, a password, and that multi-factor authentication is in place for the environment.	No exceptions noted.
	Password requirements for Company's network and application system is defined in the Company's Information Security Policy.	Inspected system reports showing network password parameters to determine if passwords are configured according the password policy.	No exceptions noted.
CC 6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Pantheon maintains multiple levels of system access based upon each employee's role and responsibilities. When a new hire starts HR will notify IT of the employee's start date and job title. IT will provision access to defined role based groups based on the job title in HR email.	Inspected request forms for sample of new hires to determine if access was requested by HR and provisioned based on job responsibility to the Pantheon infrastructure.	No exceptions noted.
	Privileged and administrative access to the network, in-scope applications and databases is restricted to appropriate individuals based on job role.	Inspected the list of users with privileged access to the network and in-scope applications to determine if access is restricted appropriately based on job role.	No exceptions noted.
	IT is notified of terminations by email from HR. Access is removed/disabled from the network, and in-scope applications upon notification.	Inspected termination forms for a sample of terminations to determine if HR notified IT in a timely manner and access removal was documented in a HelpIT ticket.	No exceptions noted.

Trust Services Criteria	Pantheon's Controls	Tests of Controls	Results
CC 6 – Logical and Physical Access			
	Quarterly user access reviews are performed to determine whether user access is limited to the authorized personnel.	Inspected user access reviews for a sample of quarters to determine if the reviews was completed. Inspected a current user access listing to determine if the changes requested in the review were completed.	No exceptions noted.
CC 6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Access to migrate changes to the production environment is restricted to appropriate personnel.	Inspect list of users with access to migrate changes to the production environment to determine if access is appropriate.	No exceptions noted.
	Access to Pantheon's network is setup within G suite. Access to Pantheons' network is denied when access to is removed.	Inspected the G suite and OKTA configuration to determine if users were required to be added to a group to be able to access the Pantheon network remotely Inspected authentication documentation to Pantheons' network is denied when access to is removed.	No exceptions noted.
	Privileged and administrative access to the network, in-scope applications and databases is restricted to appropriate individuals based on job role.	Inspected the list of users with privileged access to the network and in-scope applications to determine if access is restricted appropriately based on job role.	No exceptions noted.
CC 6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Electronic badge reader authentication is required for access to the main entrance.	Inspected badge listing to determine if access is restricted to Pantheon employees. Observed that electronic badge reader authentication is required for access to the main entrance.	No exceptions noted.
	Visitors to Pantheon facilities must be escorted by Pantheon employees at all times and are required to check in and out upon arrival and departure.	Inspected visitor sign in sheet to determine if visitors are required to check in and out.	No exceptions noted.

Trust Services Criteria	Pantheon’s Controls	Tests of Controls	Results
CC 6 – Logical and Physical Access			
	On an annual basis, Patheon management reviews the list of personnel with access to the Pantheon facilities.	Inspected a report to determine if a physical user access review was performed. Inspected a current user access listing to determine if the changes requested in the review were completed.	No exceptions noted.
CC 6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity’s objectives.	Badge access to operations facilities is revoked in a timely manner in accordance with physical security standards.	Inspected termination forms for sample of terminated employees to determine if access to Pantheon facilities was revoked in a timely manner.	No exceptions noted.
	On an annual basis, Patheon management reviews the list of personnel with access to the Pantheon facilities.	Inspected a report to determine if a physical user access review was performed in the current period. Inspected a current user access listing to determine if the changes requested in the review were completed.	No exceptions noted.
CC 6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Firewalls/Security Groups are setup with specific rules to only allow access to authorized parties. All changes to the Firewall/Security Groups must follow the normal change management process.	Inspected firewall rules to determine if Firewalls/Security Groups are setup with specific rules to only allow access to authorized parties. Inspected change management tickets for a sample of firewall rule changes to determine if it followed the normal change management process.	No exceptions noted.
	Access to the Company’s network require a user identification, a password and multi-factor authentication.	Inspected configuration settings to determine if access the network requires a unique user name, a password, and that multi-factor authentication is in place for the environment.	No exceptions noted.
	Password requirements for Company's network and application system is defined in the Company's Information Security Policy.	Inspected system reports showing network password parameters to determine if passwords are configured according the password policy.	No exceptions noted.

Trust Services Criteria	Pantheon's Controls	Tests of Controls	Results
CC 6 – Logical and Physical Access			
CC 6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Inbound transactions are transmitted over HTTPS connections secured with TLS. Transmission of the sensitive information is prohibited over the public network (acceptable use policy). If required, information shall be encrypted prior to transmit.	Inspected system configurations for both inbound and outbound connections to determine if remote data transmissions over the public internet are encrypted.	No exceptions noted.
CC 6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Antivirus protection technologies are used on workstations to ensure the detection and prevention of malware. End points are configured to check for definition updates.	Inspected settings for a sample of production application servers to determine that anti-virus software was installed on each production application server sampled. Inspected configuration settings to determine if the malware system is configured to update anti-virus definitions on a daily basis	No exceptions noted.

Trust Services Criteria	Pantheon's Controls	Tests of Controls	Results
CC 7 – System Operations			
CC 7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Weekly internal and external vulnerability scans are conducted. Any findings are assessment impact and severity and remediation efforts are formally documented and tracked.	Inspected vulnerability scans for a sample of weeks to determine if internal and external vulnerability scans were performed and issues tracked to remediation.	No exceptions noted.
	Intrusion detection system / intrusion prevention system is configured to identify, log and report potential security breaches and other incidents which could impact security of systems. Events are monitored and evaluated by the information security team.	Inspected the IDS/IPS system to determine if the system is configured to auto-generate alert notification to appropriate personnel	No exceptions noted.
	Security event logs are generated, correlated, and analyzed to identify risks that impact the security of applications, infrastructure, and operations.	Inspected the monitoring application, configurations, and log results to determine if security monitoring applications are in place and appropriately configured.	No exceptions noted.
	Logging is enabled on Pantheon Cloud system to ensure identification of potential threats that would impair system security. Appropriate log events are configured and alerts are sent to personnel to ensure appropriate action.	Inspected the log monitoring system to determine if devices are configured for log monitoring and alerting.	No exceptions noted.
CC 7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Management contracts a third party to complete annual penetration tests. Results and recommended for improvement are reported to management.	Inspected the results of the most recent penetration test in the current period and inspected documentation to determine if management tracks the remediation of any issues identified.	No exceptions noted.
	Weekly internal and external vulnerability scans are conducted. Any findings are assessment impact and severity and remediation efforts are formally documented and tracked.	Weekly internal and external vulnerability scans are conducted. Any findings are assessment impact and severity and remediation efforts are formally documented and tracked.	No exceptions noted.

Trust Services Criteria	Pantheon's Controls	Tests of Controls	Results
CC 7 – System Operations			
CC 7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Incident response plan formally documented and approved annually. All incident handling must follow the formal policy and be documented accordingly.	Inspected the Incident Response Plan to determine if the plan provided for identification of incidents and subsequent containment, notification, eradication, recovery, and root-cause analysis and that it was approved annually. Inspected tickets for a sample of incidents to determine if the incident was responded to in accordance with policy.	No exceptions noted.
CC 7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Documented escalation procedures are in place in the event of a security breach or other incident.	Inspected Incident Response policies and procedures to determine if security escalation procedures were included.	No exceptions noted.
	Incident response plan formally documented and approved annually. All incident handling must follow the formal policy and be documented accordingly.	Inspected the Incident Response Plan to determine if the plan provided for identification of incidents and subsequent containment, notification, eradication, recovery, and root-cause analysis and that it was approved annually. Inspected tickets for a sample of incidents to determine if the incident was responded to in accordance with policy.	No exceptions noted.
CC 7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.	Annual security awareness training includes incident recovery plan training on threat likelihood and magnitude, lack of availability of key personnel, and relevant system components.	Inspected security awareness training to determine if includes the threat likelihood and magnitude, lack of availability of key personnel, and relevant system components. Inspected annual Incident response training to determine if it is provided and completed by all personnel on an annual basis.	No exceptions noted.

Trust Services Criteria	Pantheon's Controls	Tests of Controls	Results
CC 7 – System Operations			
	Incident response plan formally documented and approved annually. All incident handling must follow the formal policy and be documented accordingly.	Inspected the Incident Response Plan to determine if the plan provided for identification of incidents and subsequent containment, notification, eradication, recovery, and root-cause analysis and that it was approved annually. Inspected tickets for a sample of incidents to determine if the incident was responded to in accordance with policy.	No exceptions noted.

Trust Services Criteria	Pantheon's Controls	Tests of Controls	Results
CC 8 – Change Management			
CC 8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Formal Software Development Life Cycle (SDLC) is in place for new development and program enhancement	Inspected documented policies and procedures to determine that there is a formal SLDC plan in place and it is approved annually.	No exceptions noted.
	A formal infrastructure change management policy is in place that defines and implements rules regarding information systems and infrastructure.	Inspected the infrastructure change management policy to determine if rules for supporting and maintaining the production environment are documented and up-to-date.	No exceptions noted.
	Infrastructure system and configuration changes are documented, tested, and approved prior to implementation in accordance with change control policies and procedures.	Inspected tickets for a sample infrastructure changes to determine if the changes were authorized, tested, and approved prior to being implemented in production	No exceptions noted.
	Requests for development changes to the system are documented, tested and approved prior to implementation in accordance with change control policies and standards.	Inspected tickets for a sample of application changes to determine if changes were authorized, tested in a segregated testing environment, and approved prior to being implemented in production.	No exceptions noted.
	Development, QA, and production environments are physically and/or logically separated.	Inspected the IP address listing and network diagram to determine that the development, QA, and production environments are logically separated.	No exceptions noted.
	Only authorized developers have access to source code repository (Github) to modify code as required.	Inspected a system generated listing of users with access to the source code repository to determine if access was restricted based on job responsibility	No exceptions noted.
	A report showing all code changes to the production environment is reviewed on a bi-weekly sprint review	Inspected code change reviews for a sample of weeks to determine if the review was performed.	No exceptions noted.

Trust Services Criteria	Pantheon’s Controls	Tests of Controls	Results
CC 9 – Risk Mitigation			
CC 9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Information Security Governance Committee is responsible for reviewing and ensuring security policies are accurate and up-to-date.	Inspected Pantheon policies and standards to determine if policies and standards are up to date and cover the following areas: • Anti-virus policy • Server hardening procedures • End of life procedures • Encryption policies and procedures • Data classification, handling, retention	No exceptions noted.
	Policies and standards are available to all employees via intranet.	Inspected the intranet to determine if corporate policies and standards are located on the Pantheon intranet and available for employees to access.	No exceptions noted.
	A security awareness training program has been implemented to communicate security policies to all employees. All training is required to be completed within thirty (30) days of initiation.	Inspected training completion for a sample of new employees to determine if they have completed the Security and Awareness training within 30 days of hire date.	No exceptions noted.
CC 9.2 The entity assesses and manages risks associated with vendors and business partners.	Written policies and procedures are in place establishing guidelines in regards to third party providers.	Inspected the Third-Party Management Policy to determine if written procedures are in place establishing guidelines with regards to third party providers.	No exceptions noted.
	All agreements for critical vendors must be reviewed by the legal department prior to the signing of the agreement contract.	Inspected contracts for a sample of new vendors to determine if the contract was reviewed by the legal department.	No exceptions noted.

Trust Services Criteria	Pantheon’s Controls	Tests of Controls	Results
CC 9 – Risk Mitigation			
	Annually Pantheon will request and review applicable SOC reports from third party vendors that provide services to service offering products. The review will include an evaluation of the opinion from the service auditor, control exceptions, and review of the complementary user entity controls.	Inspected SOC report review for a sample of vendors to determine if management performed a review of the SOC report in the current period along with complementary user entity control considerations.	No exceptions noted.

Additional Criteria Relevant to Availability

Trust Services Criteria	Pantheon's Controls	Tests of Controls	Results
A 1.1 The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	On an bi-weekly basis a capacity planning meeting is held to determine resource and capacity utilization and to enable the implementation of additional capacity, as necessary to help meet the availability commitment requirements. Any action items from this meeting are recorded and tracked to completion.	Inspected meeting minutes for a sample of bi-weekly meetings to determine if capacity meeting was held and action items tracked.	No exceptions noted.
	Monitoring tools are in place to monitor critical systems, critical hardware, critical applications, and resource usage to assist with meeting the availability commitment requirements. These tools notify the operations team with alerts that could be in one or more forms (i.e. emails, text messages, phone calls).	Inspected Grafana monitoring solutions in place and noted that the solution has been configured to send relevant system alerts to the Engineering team.	No exceptions noted.
A 1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	Annually Pantheon will request and review applicable SOC reports from third party vendors that provide services to service offering products. The review will include an evaluation of the opinion from the service auditor, control exceptions, and review of the complementary user entity controls.	Inspected SOC report review for sample of vendors to determine if management performed a review of the SOC report in the current period along with complementary user entity control considerations.	No exceptions noted.
	Secondary site established and are kept in a warm state, ready to be failed over to.	Inspected the service agreements in place with the primary and secondary sites to verify that the sites are established using other power grids and are ready to be failed over to.	No exceptions noted.
	Critical applications and services are distributed across multiple nodes to eliminate single points of failure.	Inspected settings to determine if critical applications and services are distributed across multiple nodes to eliminate single points of failure.	No exceptions noted.

Trust Services Criteria	Pantheon’s Controls	Tests of Controls	Results
	Database servers are configured with multiple standbys.	Inspected configuration and verified settings are in place so that database servers are configured with multiple standbys.	No exceptions noted.
	The system is configured to securely replicate data from databases and nightly backups to a Google Cloud.	Inspected backup schedule and sample of backup logs for Google Cloud to verify that the system is configured to securely replicate data.	No exceptions noted.
A 1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.	Recovery plans are documented in disaster recovery plan which defines the roles and responsibilities of relevant personnel involved in executing recovery procedures.	Inspected the written Disaster Recovery and Business Continuity Plan and verified roles and responsibilities of relevant personnel involved in executing recovery procedures is defined.	No exceptions noted.
	A Disaster Recovery Plan exists to ensure the required level of continuity for business operations during an adverse situation.	Inspected the Disaster Recovery Plan to validate that a formal plan exists and is updated and approved on an annual basis.	No exceptions noted.
	Disaster recovery plans are tested annually in accordance with the Company's system policies. Testing results and change recommendations are reported to management.	Inspected test results to determine if plan was tested on an annual basis and results and recommendations escalated to management.	No exceptions noted.

SECTION V: Other Information Provided by Pantheon Systems, Inc. That is Not Covered by the Service Auditor's Report (Unaudited)

Management's Responses to Identified Exceptions

The information included below is presented by Pantheon to provide additional information to their customers and is not part of Pantheon's description of their Website Operations. The information presented here has not been subjected to Crowe's examination procedures and, accordingly, Crowe expresses no opinion on it.

Pantheon's Control	TSC Reference	Results	Management's Response
Background screening is conducted on all new hires full-time employees prior to employment.	CC1.1	3 of 5 sampled new hires did not have a completed background check.	Pantheon will complete background screens for employees that we could not screen during the global pandemic once screening services resume normal operations.