SOC 2 Type 2 Report

2018

Management Assertion and Service Auditor's Report Pursuant to Reporting on Service Organization Controls 2 (SOC 2) Type 2 Examination in Accordance with AT-C Sections 105 and 205

Report Date: February 15, 2019

Examination and report by ValueMentor LLC on venus's hosted Customer Services System and the suitability of design and operating effectiveness of controls relevant to security, availability, processing integrity, confidentiality, and privacy to provide reasonable assurance that venus's service commitments and system requirements were achieved, based on the applicable trust services criteria, for the period of ***January 1, 2018 through December 31, 2018.***

Contents

Section I - Venus Management Assertion 1
Section II - Independent Service Auditor's Report 3
Scope 3
Section III - venus's Description of its Customer Services System 7
System Overview and Background 7
Types of Services Provided 7
MyRepChat 7
Event Management 7
Customer Management 7
Infrastructure and Software 7
People 8
Policies and Procedures 9
Data 9
Customer Responsibilities 9
A. Relevant Aspects of the venus Control Environment, Risk Assessment Process, Information and Communication Systems, and Monitoring 10
Control Environment 10
Integrity and Ethical Values 11
Commitment to Competence 11
Management's Philosophy and Operating Style 11
Organizational Structure and Assignment of Authority and Responsibility 12
Governance and Oversight: Human Resource Policies and Practices 12
Risk Assessment 13
Information and Communication 13
B. Policies and Procedures 13
C. Communication 14
D. Physical Security 14

E. Logical Security 14

Vulnerability Scanning and Monitoring 15

Availability Monitoring 15

TRUST SERVICES PRINCIPLES AND CRITERIA 16

Section 4 — Applicable Trust Services Principles, Criteria, and Related Controls, Tests of Controls, and Results of Tests 17

Control Objective 1 – Policies 17

Control Objective 2 – Communications 21

Control Objective 3 – Procedures 23

Control Objective 4 – Monitoring 32

Section I - venus Management Assertion

We have prepared the accompanying description of venus Service Organization's (venus's) hosted customer services system titled "venus's Description of its Customer Services System" throughout the period January 1, 2018 to December 31, 2018, 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*). The description is intended to provide report users with information about the hosted customer services system (consisting of MyRepChat, Event Management, Customer Management solutions) that may be useful when assessing the risks arising from interactions with venus's system, particularly information about system controls that venus 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, availability, processing integrity, confidentiality, and privacy (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*).

venus uses subservice organizations to provide application maintenance, payment processing and infrastructure support services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at venus, to achieve venus's service commitments and system requirements based on the applicable trust services criteria. The description presents venus's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of venus'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 venus, to achieve venus's service commitments and system requirements based on the applicable trust services criteria. The description presents venus's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of venus's controls.

The description contains the following information:

i) The types of services provided by venus.

ii) The components of the system used to provide the venus services, which are the following:
   1) Infrastructure. The physical and hardware components of the venus system (facilities, equipment, and networks).
   2) Software. The programs and operating software of related to the venus system (systems, applications, and utilities).
   3) People. The personnel involved in the operation and use of the venus system (developers, operators, users, and managers).
   4) Procedures. The automated and manual procedures involved in the operation of the venus system.
   5) Data. The information used and supported by the venus system (transaction streams, files, databases, and tables).

iii) The boundaries or aspects of the venus system covered by the description.

iv) How the venus system captures and addresses significant events and conditions.
v) The process used to p

vi) repare and deliver reports and bvczcxother information to user entities or other parties.
vii) Any applicable trust services criteria that are not addressed by a control at the venus service organization and the reasons therefore.
viii) Other aspects of venus's control environment, risk assessment process, information and communication systems, and monitoring of controls that are relevant to the services provided and the applicable trust services criteria.
ix) Relevant details of changes to the venus's system during the period covered by the description.

The description does not omit or distort information relevant to the venus's system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

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

a. the description presents venus's system ("hosted customer services system" or "MyRepChat, Event Management, Customer Management solutions") that was implemented and operating throughout the period January 1, 2018 to December 31, 2018, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period January 1, 2018 to December 31, 2018, to provide reasonable assurance that venus'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 venus's controls throughout that period.

c. the controls stated in the description operated effectively throughout the period January 1, 2018 to December 31, 2018, to provide reasonable assurance that venus'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 venus's controls operated effectively throughout that period.

Section II - Independent Service Auditor's Report

Scope

We have examined venus Service Organization's (venus's) accompanying description of its hosted customer services system, including application maintenance, payment processing and infrastructure support services provided by and controls operated by Amazon Web Services (AWS), Twilio and BrainTree Subservice Organizations (AWS, Twilio, BrainTree), titled "venus's Description of its Customer Services System" throughout the period January 1, 2018 to December 31, 2018, 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*), and the suitability of the design and operating effectiveness of venus's controls, stated in the description throughout the period January 1, 2018 to December 31, 2018, to provide reasonable assurance that venus's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (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*).

As indicated in the description, venus employees work from virtual/home offices, and hence no physical office visits were performed as part of our evaluation.

AWS, Twilio and BrainTree are independent subservice organizations providing application maintenance, payment processing and infrastructure support services to venus. The description includes those elements of the relevant services provided to venus and the controls designed by venus, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of venus's controls. Our examination did not include such complementary subservice organization controls and we have not evaluated the suitability of the design or operating effectiveness of such controls. (However, it is noted that a SOC 3 audit report on the Amazon Web Services System Relevant to Security, Availability, and Confidentiality was produced for our review, along with a Twilio Cloud Communication Security whitepaper describing "security mechanisms to protect physical, network and application components of the platform, coupled with transparency about security practices and compliance best practices".)

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

Service Organization's Responsibilities

venus is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls, as complemented by subservice organization and user entity controls, within the venus system to provide reasonable assurance that venus's service commitments and system requirements were achieved. venus has provided the accompanying assertion

titled "venus Management Assertion" about the description and the suitability of design and operating effectiveness of controls stated therein. venus 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.

Our examination of the description of venus's system and the suitability of the design and operating effectiveness of the venus controls involved the following:

- Obtaining an understanding of the venus system ("hosted customer services system" or "MyRepChat, Event Management, Customer Management solutions") and venus'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 the applicable trust services criteria.
- Evaluating the operating effectiveness of controls stated in the description to provide reasonable assurance that venus achieved its service commitments and system requirements based on the applicable trust services criteria.

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 venus'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 the section titled, "Applicable Trust Services Principles, Criteria, and Related Controls, Tests of Controls, and Results of Tests. No control exceptions were noted.

Opinion

In our opinion, in all material respects,

a. the description presents venus's system (hosted customer services system) that was implemented and operating throughout the period January 1, 2018 to December 31, 2018 in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period January 1, 2018 to December 31, 2018 to provide reasonable assurance that venus'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 venus's controls throughout that period.

c. the controls stated in the description operated effectively throughout the period January 1, 2018 to December 31, 2018 to provide reasonable assurance that venus's service commitments and system requirements were achieved based on the applicable trust services criteria, if complimentary subservice organization and user entity controls assumed in the design of venus's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in the section titled, "Applicable Trust Services Principles, Criteria, and Related Controls, Tests of Controls, and Results of Tests," is intended solely for the information and use of venus, user entities of venus's system during some or all of the period January 1, 2018 to December 31, 2018, business partners of venus subject to risks arising from interactions with the venus system, 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 venus.
- How venus'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 venus controls to achieve venus's service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use venus's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of venus'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.

ValueMentor, LLC
Chantilly, VA
February 15, 2019

Section III - venus's Description of its Customer Services System

System Overview and Background

venus was founded in 2006 under the name tikiwade, with the objective of providing a simple tool that managed one hometown event. In 2016, the company name was changed to venus, and the platform grew to provide enterprise-grade technology solutions for both small and large firms. venus provides web-based services with capabilities to manage all aspects of a client's interaction. These solutions are delivered via web-based, hosted services that have been designed to help ensure excellence in execution, quality management, and customer satisfaction.

Industries served by venus include Banking, Financial Services, Insurance, Telecommunications, Tax, Legal, Event Management.

Types of Services Provided

venus provides a full suite of technology-based products:

MyRepChat

In today's digital world, the ability to communicate with clients through text message is integral to the client/advisor relationship. MyRepChat was created by a Financial Advisor and a Registered Principal for the benefit of Financial Advisors to provide a compliant messaging solution to effectively and efficiently communicate with clients. With MyRepChat, the objective is not to be an option within a bundled technology package, but rather be the very best at enabling our customers to communicate with their clients at an affordable cost.

Event Management

venus's event management solution allows customers to: plan an event, manage attendee sign up, manage vendor sign up and location mapping, establish worker schedules, and provide mobile access for effective management during the event.

Customer Management

venus's customer management solution allows users to manage groups of customers, tag customers, email the customer group, generate mailing labels, and create customer ID card, in addition to other capabilities.

Infrastructure and Software

The primary infrastructure and software used to provide venus's hosted customer services system (MyRepChat, Event Management, Customer Management solutions) include the following systems:

System	OS	Public IP Address
Load Balancer (PROD)	N/A	xx.xx.xx.xx
Load Balancer (TEST)	N/A	xx.xx.xx.xx
PROD Server 1	Ubuntu 16	N/A

System	OS	Public IP Address
PROD Server 2	Ubuntu 16	N/A
TEST Server 1	Ubuntu 16	N/A
Database (PROD) – Postgres 9.4	N/A	N/A not internet facing
Database (TEST) – Postgres 9.4	N/A	N/A not internet facing
Scheduled Message Processing Server	Ubuntu 16	N/A
Public venus	WordPress	xx.xx.xx.xx
Public MyRepChat	WordPress	xx.xx.xx.xx
VPN Server	Open VPN	xx.xx.xx.xx

We also use AWS SQS, Cloud Watch, SES, and CodeCommit. These are services subscribed from Amazon Web Services (AWS) and thereby managed by AWS. Note: AWS Cloud Formation creates entire systems from a script, and the IP addresses of the systems are not fixed. Additionally, we use Twilio for messaging application development and maintenance, and BrainTree for payment processing.

People

venus is currently a relatively small company. Growth in staff is directly correlated with growth in our customer base. At present, the following areas are addressed by the following team member(s):

- Executive Management: Provides general oversight, and strategic planning and direction.
- Development Team: Responsible for handling the software development and maintenance.
- Quality Assurance Team: Ensures the software does what it is supposed to do, and communicates with customers to ensure any feedback to the contrary is immediately recorded and remedied.
- System Administrators: Responsible for software installation/configuration, operations, and maintenance of systems hardware and software relevant to our systems.
- Customer Support: Serves customers by providing product and service information that includes resolving product and service issues.
- Audit and Compliance: Performs regularly-scheduled audits relative to defined policies, procedures and standards; provides continuous improvement feedback; and assesses legal and regulatory requirements.

Policies and Procedures

Formal IT policies and procedures exist that describe computer operations, change control, and data communication standards. All teams are expected to adhere to the venus policies and procedures that define how services should be delivered. The IT policies and procedures (in addition to organizational policies, procedures and the venus Employee Handbook) are located on the venus shared folder and can be accessed by any team member.

Data

Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations, with specific requirements formally established in customer contracts. Customer data is captured and utilized by venus in delivering its technology solutions. Such data includes, but is not limited to, the following:

- Alert notifications and monitoring reports generated from the commercial monitoring applications located at the subservice organizations.
- Alert notifications received from automated backup systems.
- Vulnerability or security alerts received from various sources, including security subscriptions, scanning tools, IDS alerts, or automated patching systems.
- Incident reports documented via the subservice organizations' ticketing systems.

Customer Responsibilities

venus's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Principles related to venus's services to be solely achieved by venus control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls and procedures to complement those of venus's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Principles described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to venus.
2. User entities are responsible for notifying venus of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record (unless venus is contracted to provide those data archiving services to the user entity).

4. User entities are responsible for ensuring the supervision, management, and control of the use of venus services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize venus services.
6. User entities are responsible for providing venus with a list of approvers for security and system configuration changes related to data transmission.
7. User entities are responsible for immediately notifying venus of any actual or suspected information security breaches, including compromised user accounts and interfaces used for integrations and secure file transfers.

A. Relevant Aspects of the venus Control Environment, Risk Assessment Process, Information and Communication Systems, and Monitoring

1. **Control Environment**. Sets the tone for the venus organization, influencing the control consciousness of employees and management. It is the foundation for all other components of internal control, providing service organization discipline and structure.
2. **Control Activities**. The policies, procedures and related execution (automated and manual) that help make sure that venus management's directives are carried out.
3. **Information and Communication**. Systems, both automated and manual, that support the identification, capture, and exchange of venus information in a form and timeframe that enable our employees and management to carry out their responsibilities.
4. **Monitoring**. The ongoing processes that assesses the quality of internal control performance over time.
5. **Risk Assessment**. Our identification and analysis of relevant risks to the achievement of our objectives or impact to our company, partners or customers, forming a basis for determining how the risks can be most effectively managed.

venus internal control components include controls that may have a pervasive effect on the organization or may affect specific processes or applications, or both. Some of the components of internal control include controls that have more of an effect at the entity level, while other components include controls that are primarily related to specific processes or applications. When evaluating internal control, we apply a risk-based approach to consider and effectively manage the interrelationships among the relevant components.

Control Environment

The internal control objectives related to venus's Customer Services System are to provide reasonable, but not absolute, assurance that controls are suitably designed and operating effectively to meet our risk appetite. This means that assets are protected from unauthorized use or disposition, that transactions are executed in accordance with management's authorization and client instructions, and that customer data is secure.

Management has established and maintains controls designed to monitor compliance with established venus policies and procedures. The remainder of this subsection discusses the “tone at the top” as set by venus management; the integrity, ethical values, and competence of venus employees; the policies and procedures the guide controlled execution by our employees and management; the risk management process and monitoring; and the roles of significant control groups. The internal control structure is established and refreshed based on venus’s assessment of inherent and residual risk facing the organization.

Integrity and Ethical Values

venus believes that the effectiveness of controls correlates with the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of venus's control environment, affecting the design, administration, and monitoring of its service organization components. Integrity and ethical behavior are the product of venus's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formally documented organizational policy statements and codes of conduct communicate entity values, behavioral standards and consequences to personnel.
- Policies and procedures are effectively communicated by requiring employees to sign an acknowledgment form indicating they have been given access to the employee handbook and understand their responsibility for adhering to the policies and procedures contained within.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- Background checks are performed for employees as a component of the hiring process.

Commitment to Competence

venus's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.
- Training is provided to maintain the skill level of personnel in certain positions.

Management's Philosophy and Operating Style

venus's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's

attitudes toward information processing, confidential and privacy-related data, accounting functions, and personnel.

Specific control activities that the service organization has implemented in this area are described below:

- Employees are periodically briefed on regulatory and industry changes affecting the services provided by venus.
- Executive management meetings are held to discuss major initiatives and issues that affect the business as a whole.

Organizational Structure and Assignment of Authority and Responsibility

venus's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed that suits its needs. This organizational structure is based, in part, on the size and the nature of the service organization's activities.

venus's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the service organization's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Governance and Oversight: Human Resource Policies and Practices

venus's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top-quality personnel who ensure the service organization is operating at maximum efficiency. venus's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- Employee onboarding checklists have been created to ensure new employees receive the necessary information.
- New employees are required to sign an acknowledgment form in the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment.
- Evaluations for each employee are performed on an annual basis.
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist.

Risk Assessment

venus's risk assessment process identifies and manages risks that could potentially affect venus's ability to provide reliable services to user organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. venus identifies the underlying sources of risk, measures the impact on the organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process has identified risks resulting from the nature of the services provided by venus and its subservice organizations, and management has implemented various measures designed to manage these risks. Risks identified in this process include the following:

- Operational Risk Management: Manages changes in the environment, staff, management personnel or technology partners.
- Strategic Risk Management: Manages new technologies, changing business models, and shifts within the industry.
- Compliance Management: Manages legal and regulatory changes.

Information and Communication

Information and communication is an integral component of venus's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At venus, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

B. Policies and Procedures

venus has the following security procedures and policies in place, which are owned by the Director of Information Security:

- Acceptable Use Policy
- Cellular Phone and BYOD (Bring Your Own Device) Policy
- Data Backup and Recovery Policy
- Business Continuity Management Policy
- Access Control Policy
- Information Classification Policy
- Information Handling Policy
- Information Exchange Policy
- Configuration and Change Management Policy
- Information Disposal Policy
- Network Security Management Policy
- Password Policy

- E-mail and Messaging Security Policy
- Remote Access Policy
- Telecommuting Security Policy
- Malicious Code Protection Policy
- Information Risk Management Policy
- Third Party Security Management Policy
- Physical Security Policy
- Log Management and Monitoring Policy
- Anti-Bribery and Corruption Policy
- Security Awareness, Training, and Education Policy
- Information Security Incident Reporting and Response Policy

C. Communication

venus maintains an extensive sets of controls to manage effective communication internally (with personnel) and externally (with customers, partners, and other specific entities). A description that delineates the boundaries of the venus system is available to external users via the entity's website. A documented organizational chart is in place to communicate organizational structures, lines of reporting, and areas of authority. Reporting relationships and organizational structures are reviewed periodically by management.

venus roles and responsibilities are defined in written job descriptions and communicated to personnel. Management reviews the job descriptions periodically and makes updates, if necessary. Employees are required to review, sign and accept the employee handbook and code of conduct agreement upon hire. Newly hired employees are required to undergo information security training upon hire and annually thereafter. Policies and procedures are documented for significant processes and are available on the entity's intranet.

Customer responsibilities are documented in contracts, and general guidelines are outlined and communicated via the entity's website. Internal and subservice organization processes are monitored through service level management procedures to help ensure compliance with service level commitments and agreements. Security and privacy commitments are communicated to external users via the entity's website.

D. Physical Security

The cloud hosting services supporting the venus system are provided by AWS and monitored by management; these services are included in the scope of this review.

E. Logical Security

As a virtual company, venus has no internal network and instead relies on their employees having internet access and several providers for various services. Some of the service providers are:

- Microsoft (Office 365)
- Vtiger (CRM)

- JetBrains (You Track)
- Twilio (Communications)
- BrainTree (Payments)
- AWS (DNS, Production Systems, Source Code Control, etc.)

When an employee is onboarded, the venus hiring manager must fill out an access checklist to indicate which systems the employee will need to access. venus IT then grants the employee access and maintains a spreadsheet of the employees and their access. When an employee leaves, venus IT then uses the spreadsheet to deactivate the employee's access. A quarterly review/audit of the spreadsheet and related system access is performed.

Authorized employees may access the system from the internet through the use of leading VPN technology. Employees are authenticated through the use of a token-based two-factor authentication system.

F. Monitoring

Vulnerability Scanning and Monitoring

venus conducts annual security reviews and vulnerability assessments using pen-test.com. Results and recommendations are communicated to and addressed by venus management.

pentest-tools.com is also used to perform an external vulnerability assessment annually.

Availability Monitoring

Incident response policies and procedures are in place to guide venus personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents and incident response procedures are in place to identify and respond to incidents on the network. venus monitors the capacity utilization of computing infrastructure for customers to ensure that service delivery matches service level agreements. venus evaluates the need for additional infrastructure capacity in response to the growth of existing customers and/or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

- Service Response Times
- Database Storage and Response Time

venus has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor-recommended operating system patches. venus authorized personnel review proposed operating system patches to determine whether the patches are applied. Authorized personnel are responsible for determining the risk of applying or not applying patches based upon the security and availability impact to the systems and any critical applications hosted on them. venus staff validate that all patches have been installed and, if applicable, that reboots have been completed.

TRUST SERVICES PRINCIPLES AND CRITERIA

In-Scope Trust Services Principles:

Common Criteria (to the Security Principle)
The security principle refers to the protection of the system resources through logical and physical access control measures in order to enable the entity to meet its commitments and system requirements related to the security, availability, processing integrity, confidentiality, and privacy. Controls over the security of a system prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of data or system resources, misuse of software, and improper access to, or the use of, alteration, destruction, or disclosure of information.

Integration with Risk Management:

The environment in which the system operates; the commitments, agreements, and responsibilities of venus's Customer Services System; as well as the nature of the components of the system result in risks that the criteria will not be met. venus addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, venus's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Section 4 — Applicable Trust Services Principles, Criteria, and Related Controls, Tests of Controls, and Results of Tests

Control Objective 1 – Policies

CO1 – venus defines and documents its policies for the security of its systems.

No.	Criteria	Control	Tests Performed	Testing Results
1.1	venus's security policies are established and periodically reviewed and approved by a designated individual or group.	venus's information security policy addresses IT, it is approved by the CEO and CTO, and is reviewed by both annually.	Inspected the security policies to ascertain that procedures governing IT for the in-scope technology and locations were included. Interviewed the CTO who has the additional responsibility of Information Security Officer. Inspected the documents related to the annual review of the policies	CTO has an additional charge of Information Security Officer. CTO and CEO review the policy annually. The last review of policies was done on 05/15/2018. No exceptions noted.
1.2	venus's security policies include, but may not be limited to the following areas:	venus's security policies address the following:		
	a. Identifying and documenting the security requirements of authorized users.	Thoroughly documented security requirements of authorized users.	Inspected the security policies to ascertain they included the areas specified.	Admin level access to systems is restricted to CTO and one other staff member.

s

No.	Criteria	Control	Tests Performed	Testing Results
				No exceptions noted.
	b. Classifying data based on criticality and sensitivity and that classification is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements.	Data classification, based on criticality and sensitivity, that is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements.	Inspected the security policies to ascertain they included the areas specified. Inspected the classification labels documented and reviewed the sample set of documents.	Data has been classified as Public, Confidential - Internal Use Only, Private and Trade Secret. No exceptions noted.
	c. Assessing risks on a periodic basis.	Documented requirements, guidelines and criteria for periodic risk assessment.	Inspected the security policies to ascertain they included the areas specified. Interviewed the CTO about the periodicity and reviewed the results.	Periodic access reviews are conducted, and confirmed with CTO that last access review was conducted in August 2019. No exceptions noted.
	d. Preventing unauthorized access.	Documented requirements and guidelines to prevent unauthorized access.	Inspected the security policies to ascertain they included the areas specified.	Refer a & c. No exceptions noted.
	e. Adding new users, modifying the access levels of existing users,	Documented access control requirements and guidelines that address adding new users,	Inspected the security policies to ascertain they included the areas specified.	Noted that all access requests are routed through CTO and

s

No.	Criteria	Control	Tests Performed	Testing Results
	and removing users who no longer need access.	modifying the access levels of existing users, and removing users who no longer are authorized access.	Interviewed the CTO regarding access request management.	managed by the CTO. No exceptions noted.
	f. Assigning responsibility and accountability for system security	Documented roles and responsibilities for confidentiality and related security.	Inspected the security policies to ascertain they included the areas specified. Verified by reviewing that following anti-virus software are used: - Windows: McAfee or Microsoft Defender - Mac: ClamXAv - Firewall is turned on - Auto-updates are turned on	No exceptions noted.
	g. Assigning responsibility and accountability for system changes and maintenance.	Documented roles and responsibilities for system changes and maintenance.	Inspected the job description of CTO to verify that the responsibility is assigned and fulfilled.	No exceptions noted.
	h. Testing, evaluating, and authorizing system components before implementation.	Documented requirements and guidelines for testing, evaluating, and authorizing system components before implementation, including segregation of duties.	Inspected job description of CTO to verify that the responsibility is assigned and fulfilled.	No exceptions noted.

s

No.	Criteria	Control	Tests Performed	Testing Results
	i. Addressing how complaints and requests relating to security are resolved.	Documented requirements and guidelines for addressing and resolving security complaints and requests.	Inspected the security policies to ascertain they included the areas specified. Inspected the procedure that YouTrack is used to report and resolve system and security issues.	No exceptions noted.
	j. Identifying and mitigating security breaches and other incidents.	Documented requirements and guidelines for handling confidentiality and related security breaches and other incidents.	Inspected the security policies to ascertain they included the areas specified. Inspected the Cyber Incident Response Plan document.	No exceptions noted. However, it shall be noted that there were no cyber incidents reported during the engagement period.
	k. Providing training and other resources to support its system security policies.	Documented requirements and guidelines for providing security-related training and other resources to support system confidentiality and related security policies.	Inspected the security policies to ascertain they included the areas specified. Interviewed the CTO regarding whether security awareness training is conducted via the third party solution (INTERPROIQ) annually.	No exceptions noted.
	l. Providing for handling of exceptions and situations not specifically addressed in its security policies.	Documented guidelines for handling of exceptions and situations not specifically addressed in its security policies.	Inspected the security policies to ascertain they included the areas specified.	No exceptions noted.
	m. Providing for identification of and consistency with	Documented guidelines for identifying and complying with applicable laws and regulations,	Interviewed CTO to determine whether the company has any industry-related regulatory	No exceptions noted.

s

No.	Criteria	Control	Tests Performed	Testing Results
	applicable laws and regulations, defined commitments, service level agreements, and other contractual requirements.	defined commitments, service level agreements, and other contractual requirements.	requirements other than data security.	
	n. Providing for sharing information with third parties.	Documented requirements and guidelines for sharing information with third parties.	Inspected the security policies to ascertain they included the areas specified.	No exceptions noted.
1.3	Responsibility and accountability for developing and maintaining venus's system security policies, and changes and updates to those policies, are assigned.	venus assigns responsibility and accountability for developing and maintaining system security policies to the CTO.	Inspected the CTO job description to determine whether the descriptions include responsibilities for the maintenance and enforcement of venus's security policy.	No exceptions noted.

Control Objective 2 – Communications

CO2 – venus communicates its defined system security policies to responsible parties and authorized users.

No.	Criteria	Control	Tests Performed	Testing Results
2.1	venus has prepared an objective description of the system and its boundaries and communicated such	venus provides a description of its system, system boundaries, and system processes that includes infrastructure, software, people, and procedures to those people who request it.	Inspected published descriptions of venus's system, system boundaries, and system processes todetermine whether the description addressed infrastructure, software,	No exceptions noted.

s

No.	Criteria	Control	Tests Performed	Testing Results
	description to authorized users.		people, procedures, and data for the in-scope technology.	
2.2	The security obligations of users and venus's security commitments to users are communicated to authorized users.	venus provides ongoing security training to its employeesthrough department meetings and/or emailed instructions. venus's IT employees are required to annually sign and acknowledge their review of the information security policy. venus's policies relating to security are reviewed with new employees as part of their orientation, and new employees are required to sign and acknowledge their review of the employee handbook.	Inspected sample of security meeting minutes to determine whether employees received ongoing security training. For a sample of IT employees, inspected their employee acknowledgments to determine the employees acknowledged their review of the information security policy. For a sample of newly hired employees, inspected the new hire employee acknowledgment forms to determine they signed and acknowledged their review of the employee manual, which included the security policies.	No exceptions noted.
2.3	The process for informing venus about breaches of the system security and for submitting complaints is communicated to authorized users.	venus's security awareness program trains employees how to identify and report possible security breaches. System alerts, including planned outages and known issues, are communicated via email.	Inspected the security awareness training program material, which described how to identify and report possible security breaches. Inspected selected system alert emails to determine whether system alerts are communicated to system users.	No exceptions noted.

s

No.	Criteria	Control	Tests Performed	Testing Results
2.4	Changes that may affect system security are communicated to management and users who may be affected.	Planned changes to system components are reviewed, scheduled, and communicated to management as part of the weekly IT maintenance process.	Inspected a sample of weekly IT maintenance schedules and communications to determine whether planned system changes were included and reviewed/signed off by IT management.	System outages are communicated vide e-mails. No exceptions noted.

Control Objective 3 – Procedures

CO3 – venus has operating procedures to achieve its documented system security objectives, in accordance with its defined policies.

No.	Criteria	Control	Tests Performed	Testing Results
3.1	Procedures exist to: (1) identify potential threats of disruption to system operation that would impair system security commitments, and (2) assess the risks associated with the identified threats.	A company-wide risk assessment is performed annually by management, which includes the following: • Determining business objectives, including security commitments. • Evaluating the effect of environmental, regulatory, and technological changes on venus's system security.	Inspected the annual risk assessment documentation to determine whether it included the specified procedures.	No exceptions noted.

s

No.	Criteria	Control	Tests Performed	Testing Results
		• Identifying threats to operations, including security threats using information technology asset records. • Analyzing risks associated with the threats. • Determining a risk mitigation strategy. • Developing or modifying and deploying controls consistent with the risk mitigation strategy.		
3.2	**Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters:**			
	a. Logical access security measures to restrict access to information resources not deemed to be public.	Access to venus's network is restricted through the use of defined application and database user roles. Access granted to users is authorized by CEO. venus's user role assignments are reviewed by CTO annually.	Inspected user access for a sample of users and determined access was authorized and consistent with their role. Inspected a sample of user access reviews noting the review was performed annually.	No exceptions noted.

s

No.	Criteria	Control	Tests Performed	Testing Results
	b. Identification and authentication of users.	Unique user identification numbers, names, and passwords are required to authenticate all users to venus's network. Password parameters consist of the following: • Passwords have a minimum of eight characters including uppercase/lower case and number. • Passwords expire every 180 days.	Inspected the password parameters for the system to determine whether the password parameters were configured with the following specifications: • Passwords have a minimum of eight characters including uppercase/lower case and number. • Passwords expire every 180 days.	No exceptions noted.
	c. Registration and authorization of new users.	In order for venus's employees to obtain network access, a helpdesk ticket must be submitted authorizing such access. Proper segregation of duties is considered in granting access privileges based on the user's job role.	Inspected the user access requests for a sample of employees requiring access to the system to determine whether the access was authorized and provided with the proper segregation of duties.	No exceptions noted.
	d. The process to make changes and updates to user profiles.	Only authorized company personnel are able to create or modify user access and user access privileges.	Inspected a report identifying individuals with access to create or modify user access privileges to determine whether the access was limited to authorized personnel.	No exceptions noted.

s

No.	Criteria	Control	Tests Performed	Testing Results
		HR department provides IT personnel with a termination checklist to follow upon employee termination (offboarding). IT reconciles the report against current system privileges to determine if access has been appropriately removed or disabled.	Inspected a sample of termination checklists and user accounts to determine user access was appropriately removed or disabled.	
	e. Restriction of access to system configurations, super-user functionality, master passwords, powerful utilities, and security devices.	Administrative access to venus's firewall is restricted to the CTO. All firewall configuration changes are logged and are reviewed by the security administration team.	Inspected the firewall system configuration and access listing to determine access was restricted to authorized personnel and changes were logged.	No exceptions noted.
3.3	Procedures exist to protect against unauthorized access to system resources.	venus uses a firewall to prevent unauthorized system access. The company conducts annual security reviews and vulnerability assessments using pen-test.com. Results and recommendations are	Inspected the network diagram to determine whether system design included firewalls to prevent unauthorized network access. Inspected the security review and vulnerability assessment reports to determine the assessments were performed and communicated.	No exceptions noted.

s

No.	Criteria	Control	Tests Performed	Testing Results
		communicated to and addressed by management.		
3.4	Procedures exist to protect against infection by computer viruses, malicious code, and unauthorized software.	venus uses anti-virus software on all Windows-based desktops, laptops, and servers. These systems are configured to query the anti-virus depository daily to retrieve the latest ant-virus definitions.	Inspected the anti-virus software configurations to determine the software was configured to retrieve the latest anti-virus definitions on a daily basis.	No exceptions noted.
Criteria related to execution and incident management used to achieve objectives:				
3.5	Procedures exist to identify, report, and act upon system security breaches and other incidents.	User entities are provided with instructions for communicating potential security breaches to the Information Security team. When a potential security incident is detected, a defined incident management process is initiated by authorized personnel. Corrective actions are implemented in accordance with defined policies and procedures.	Inspected the instructions provided to user entities to determine whether they included protocols for communicating potential security breaches. Inspected the written incident management procedures to determine whether the procedures included a process for handling the security incident.	No exceptions noted.
3.6	Procedures exist to classify data in accordance with	venus has a defined information classification	Inspected the data classification policy to determine whether there	No exceptions noted.

s

No.	Criteria	Control	Tests Performed	Testing Results
	classification policies and periodically monitor and update such classifications are necessary.	scheme for the labeling and handling data. The company classifies data into four levels - Public, Confidential - Internal Use Only, Private and Trade Secret.	was a documented classification scheme for labeling and handling data.	
3.7	Procedures exist to provide that issues of non-compliance with security policies are promptly addressed and that corrective measures are taken on a timely basis.	Security incidents are reported to management and follow the Incident Response Policy. Employees found to be in violation of venus's Information Security policy are subject to disciplinary action up to and including termination of employment.	Inspected the security policy to determine the policy included procedures for employees in violation of the policy. Confirmed there were no security incidents during the audit period.	No exceptions noted.
3.8	Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system security policies to enabled authorized access	venus has a formalized security and system development methodology that includes system planning, design, testing, implementation, maintenance, and disposal or de-commissioning.	Inspected the security and system development methodology policy to determine it included project planning, design, testing implementation, maintenance, and disposal or de-commissioning.	No exceptions noted.

s

No.	Criteria	Control	Tests Performed	Testing Results
	and to prevent unauthorized access.			
3.9	Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting security have the qualifications and resources to fulfill their responsibilities.	venus has written job descriptions specifying the responsibilities and academic and professional requirements for key job positions. Hiring procedures include a comprehensive screening of candidates for key positions and consideration of whether the candidate's credentials are commensurate with the position. New personnel are offered employment, subject to background check results.	For a sample of positions, inspected written job descriptions to determine the job descriptions included responsibilities and academic and professional requirements. For a sample of new employees, inspected the results of background checks to determine a background check was performed.	Background checks are completed through McDowell Agency. No exceptions noted.
3.10	Procedures exist to maintain system components, including configurations consistent with the defined system security policies.	venus maintains a documented change management and patch management process. Servers are reviewed monthly by the Security Administration team to determine if required	Inspected the change and patch management policies to determine there were documented procedures. For a sample of months, inspected management's server review documentation to determine the security patches were applied.	No exceptions noted.

s

No.	Criteria	Control	Tests Performed	Testing Results
		vendor security patches have been applied.		
3.11	Procedures exist to provide that only authorized, tested, and documented changes are made to the system.	venus maintains a formally documented change management process. Changes to hardware, operating system, and system software are authorized, tested (when applicable), and approved by appropriate personnel priorto implementation. Changes in system infrastructure and software are developed and tested in separate development and test environments before implementation. Additionally, developers do not have the ability to migrate changes to production environment.	Inspected the change management policy for hardware, operating system, and system software to determine whether procedures were documented to include authorization, tested, and approved prior to implementation. Inspected documentation of system infrastructure architecture to determine whether separate development and test environments existed from the production environment. Inspected the access list to the change management tools to determine whether access to migrate changes to production was appropriate based on job responsibilities and that developers did not have the ability to migrate changes into the production environment.	No exceptions noted.
3.12	Procedures exist to provide that emergency changes are documented and authorized timely.	Emergency changes follow the standard change management process, but at an accelerated timeline.	There were no emergency changes during the audit period.	No exceptions noted.

s

No.	Criteria	Control	Tests Performed	Testing Results
		Prior to initiating an emergency change, all necessary approvals are obtained and documented.		

S

Control Objective 4 – Monitoring

CO4 – venus monitors the system and takes action to maintain compliance with its defined system security policies.

No.	Criteria	Control	Tests Performed	Testing Results
4.1	venus system security is periodically reviewed and compared with the defined system security policies.	External vulnerability assessments are performed on an annual basis, and management initiates corrective actions for identified vulnerabilities.	Inspected a sample of vulnerability assessment reports noting monthly performance.	pentest-tools.com is used to perform an external vulnerability assessment annually. No exceptions noted.

s