System and Organization Controls 3 Report

Report on Secure-24, LLC's Infrastructure Hosting Services Relevant to Security and Availability

throughout the period April 1, 2018 to March 31, 2019

Management's Assertion Regarding the Effectiveness of Its Controls Over the Infrastructure Hosting Services Based on the Trust Services Principles and Criteria for Security and Availability

May 10, 2019

We, as management of, Secure-24 are responsible for designing, implementing and maintaining effective controls over the Infrastructure Hosting Services (System) to provide reasonable assurance that the commitments and system requirements related to the operation of the System are achieved.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in Security controls, an entity may achieve reasonable, but not absolute, assurance that all security events are prevented and, for those that are not prevented, detected on a timely basis. Examples of inherent limitations in an entity's Security's controls include the following:

- Vulnerabilities in information technology components as a result of design by their manufacturer or developer
- Ineffective controls at a vendor or business partner
- Persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity

Furthermore, projections of any evaluation of effectiveness to future periods are 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.

We have performed an evaluation of the effectiveness of the controls over the system throughout the period April 1, 2018 to March 31, 2019, to achieve the commitments and system requirements related to the operation of the System using the criteria for the security and availability (Control Criteria) set forth in the AICPA's TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. Based on this evaluation, we assert that the controls were effective throughout the period April 1, 2018 to March 31, 2019 to provide reasonable assurance that:

- the System was protected against unauthorized access, use, or modification to achieve Secure-24's commitments and system requirements
- the System was available for operation and use, to achieve Secure-24's commitments and system requirements
- the System processing is complete, valid, accurate, timely, and authorized to achieve Secure-24's commitments and system requirements
- the System information is collected, used, disclosed, and retained to achieve Secure-24's commitments and system requirements

based on the Control Criteria.

Our attached description of the boundaries of the Infrastructure Hosting Services identifies the aspects of the Infrastructure Hosting Services covered by our assertion

Very truly yours,

Secure-24, LLC

Ernst & Young LLP
One Kennedy Square
Suite 1000
777 Woodward Avenue
Detroit, MI 48226-5495

Tel: +1 313 628 7100
Fax: +1 313 628 7101
ey.com

Report of Independent Accountants

Management of Secure-24, LLC

Approach:

We have examined management's assertion that Secure-24 maintained effective controls to provide reasonable assurance that:

- the Infrastructure Hosting Services System was protected against unauthorized access, use, or modification to achieve Secure-24's commitments and system requirements
- the Infrastructure Hosting Services System was available for operation and use to achieve Secure-24's commitments and system requirements.
- the Infrastructure Hosting Services System processing is complete, valid, accurate, timely, and authorized to achieve Secure-24's commitments and system requirements
- the Infrastructure Hosting Services System information is collected, used, disclosed, and retained to achieve Secure-24's commitments and system requirements

during the period April 1, 2018 through March 31, 2019 based on the criteria for security and availability in the American Institute of Certified Public Accountants' TSP Section 100A, *Trust Services Principles and Criteria, for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. This assertion is the responsibility of Secure-24's management. Our responsibility is to express an opinion 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 management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of Secure-24's relevant security and availability policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating Secure-24's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

Inherent limitations:

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 inherent limitations in its internal control, those controls may provide reasonable, but not absolute, assurance that its commitments and system requirements related to security and availability are achieved.

Building a better working world

Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity. Furthermore, projections of any evaluation of effectiveness to future periods are 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.

Opinion:

In our opinion, Secure-24's management's assertion referred to above is fairly stated, in all material respects, based on the aforementioned criteria for security and availability.

Ernst & Young LLP

May 10, 2019
Detroit, Michigan

Overview of Operations

Secure-24's Business Overview

Secure-24 provides managed cloud computing, managed private cloud services, and comprehensive IT operational services to organizations worldwide. These services are provided from the data centers located in Plymouth, MI (DCD), Southfield, MI (DCB), and a data center located in the Switch SUPERNAP facility located in Las Vegas, NV (DCE). Services are provided by way of the Managed Service Provider (MSP) domains located in the aforementioned data centers, and from staff which has access to the domain, including those located in offices in Southfield, MI, and where applicable remote and global staff, including an office in Hyderabad, India.

Secure-24 hosted solutions are designed to be highly available and scalable and to incorporate leading-edge technology. We provide customers with full-service technical offerings, from design to production support, with a focus on high availability, security, and disaster recovery practices. To provide support to our customers, Secure-24 has developed optimized, repeatable policies and processes to manage our application hosting projects. The processes we use to execute our operations are based on Information Technology Infrastructure Library (ITIL) and Control Objectives for Information and Related Technologies (COBIT), the industry standards for best practice information management processes. Components of the system described in the report will cover the infrastructure, software, people, policies and procedures, and data. Security policies, processes and services are designed and certified to meet ISO 27001:2013.

Below are the service areas, depth of services and technologies available to Secure-24 customers:

- IT Administration and support
  - Technical Support
  - Level 1 Help Desk
  - ITIL ITSM Toolset
  - Active Directory/LDAP
  - Desktop as a Service
  - Endpoint Management
- Enterprise Managed Cloud (Virtual and Dedicated)
  - Infrastructure as a Service
  - Server Operating Systems
  - Enterprise Storage and Retention
  - Data Protection and Recovery
  - Dedicated Virtual and Physical Firewall
  - IPS/IDS
  - Load Balancing
  - Private Connectivity

- Application Hosting and Technical Application Support
  - Enterprise Resource Planning (ERP)
    - SAP
    - Oracle EBS
    - JD Edwards
    - Peoplesoft
    - QAD
  - Business Intelligence
    - Hyperion
    - Oracle BI
    - Business Objects
  - Communications/Other
    - Microsoft Applications
  - Database Administrator Support
  - Vendor Advanced Technical Solutions
- Wide Area Networking
  - Site-2-Site VPN and MPLS
  - Carrier Management
- DBA Services
  - Database Administrator (DBA) Support
- Vendor Advances Technical Solutions
  - SAP HANA
    - HANA Appliance – SAP BASIS
    - HANA Virtualized – SAP BASIS
  - ORACLE
    - Private Cloud Infrastructure (PCA)
- Customer IT Device Support
  - Mobile Device Management
  - Remote Management – OS and Network
- Managed Security Services
  - Virtual Security Expert Services (Virtual CISO)
  - Vulnerability Testing
  - Advanced Network and Host Level Security
  - Endpoint Protection (SEP ATP)
  - Security Incident Event Management (SIEM)

Principal Service Commitments and System Requirements

Secure-24 designs its processes and procedures related to its Information Security Management System (ISMS) to meet its objectives for its managed cloud services, IT operations, applications hosting, managed security services, and IT consulting services. Those objectives are based on the service commitments that Secure-24 makes to user entities, the laws and regulations that govern the provision of ISMS services, and the financial, operational, and compliance requirements that Secure-24 has established for the services. The ISMS services of Secure-24 are subject to the following security and privacy requirements (as applicable to each customer):

- Health Insurance Portability and Accountability Act Administrative Simplification (HIPAA and HITECH)
- Internal Revenue Service IRS-1075 (FTI)
- Export Control (ITAR and EAR)
- Sarbanes-Oxley Act of 2002 (PL 107-204 2002 HR 3763) – Section 404 (PCAOB (Public Company Accounting Oversight Board))
- Sarbanes-Oxley Act of 2002: Section 409 (PCAOB)
- Securities and Exchange Act, Sections 32(a) and (b) (SEC)
- Federal Information Security Management Act (FISMA) of 2002 (FTC)
- 6 CFR Part 29 Procedures for Handling Critical Infrastructure Information – Department of Homeland Security
- State privacy security laws and regulations in the jurisdictions in which Secure-24 operates

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- ISMS and Regulatory Policy and Procedure Employee Training Program
- Employee Background Checks
- Drug Screening
- Security Awareness Training
- Least Privileged Physical and Logical Access
- Physical Access Denied Parties Scanning
- Password Complexity Standards
- Data Encryption Across Multiple Data Centers
- Disaster Recovery
- Business and Privacy Impact Assessments
- Vendor Risk Management
- ISMS/Control Risk Assessments
- Internal Audit of Controls
- Security Incident Management
- Change Management
- Anti-Virus, Vulnerability, and SIEM Security Management

Secure-24 establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Secure-24's system policies and procedures, system design documentation, customer contracts, and contracts with third party services. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and

developed, how the system is operated, how the internal business systems and networks are managed and how employees and contracted staff members are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the ISMS.

Infrastructure

Private cloud services and remote management services are provided to users using highly available (N +1) enterprise IT infrastructure equipment located in the data center locations in Plymouth, MI and Southfield, MI. Services are provided using a range of hardware, including Cisco, Oracle, and IBM servers, VMware and Oracle Hypervisors, Oracle, NetApp, Pure and EMC Storage Area Networks (SANs) and backup, and Networking Equipment from multiple providers. Secure-24 regularly assesses technical innovations in computing, storage, and network, and it updates its infrastructure.

Software

Secure-24 provides cloud services using the hardware identified under the heading "Infrastructure," which supports a hypervisor software and operating system software. Secure-24 primarily supports Windows and Linux operating systems, and may support the installation and/or availability of customer owned applications. These are provided from private common and/or dedicated platforms that are maintained and managed by Secure-24. Secure-24 will also provide server backups, management of dedicated customer firewalls, and managed load-balancing.

Data

Customer data is managed and stored in consideration with relevant data protection regulations. Systems are designed so that customers may only access systems or instances assigned to them. Customer data is managed and stored in a range of database technologies. Customers retain control and ownership of their own data and are responsible for content, use of their content, and development, and may elect for Secure-24 to be responsible for the availability, performance and maintenance of the database technology.

Data is stored on media which meets Secure-24 policies for retention, encryption, replication, rotation and removal of medial. Storage devices which have reached the end of their useful life are removed using the media disposal process, which includes a Media Destruction Policy that must be followed which allows for the secure disposal of media.

Security

Secure-24 maintains a separation between the infrastructure required for performing services as a managed service provider and Secure-24's Corporate environment. The Managed Service Provider (MSP) boundary is separated utilizing separate infrastructure and separate logical access mechanisms, including independent multifactor authentication, which prevents direct access to customer environments. Secure-24 uses role-based security architecture and requires Secure-24 users of corporate, MSP and customer domains to be identified and authenticated prior to the use of any system resources. Managers are responsible for approving access to the resources which employees have access to and for performing periodic reviews of access by role.

Security services and procedures are conducted according to the following policies:

- Security Roles and Responsibilities
- Acceptable-Use Policy
- Privacy Policy

- Disciplinary and Sanctions Policy
- Mobile Device Policy
- Encryption Policy
- Network Access/Configuration Policy
- Password Policy
- Patch Management Policy
- Enterprise Security Policy
- Data Classification Policy
- Internet DMZ Equipment Policy
- Media Destruction Policy
- Remote Access/VPN Policy
- Router Security Policy
- Server Security Policy
- Software Policy
- User Account Policy
- Wireless Communication Policy
- Vendor employee security responsibilities

People

Secure-24's organizational structure is maintained and reviewed by executive management with the objective of maintaining entity-wide objectives that are planned, executed, controlled, and monitored. Secure-24's Board of Directors (the Board) recognizes their responsibility to foster a strong ethical environment, and regularly performs reviews to determine that business affairs are conducted with integrity and with the highest standards of personal and corporate conduct. Key training and Security Awareness training is delivered to employees annually. Services are provided by Secure-24's Network Operations, Security, Support, Sales, Billing, Account Management, Product Development, Information Technology (IT), Facilities, and Executive Management teams.

Policies and Procedures

Formal IT, security and privacy policies and procedures exist that describe incident response, change management, logical and physical security and access, network security, backup and encryption, and system security standards. Personnel are expected to adhere to Secure-24's policies and procedures that define how services should be delivered. These are located on the company's intranet and can be accessed by any Secure-24 team member. Policies and procedures are updated as needed, or by the required review date, whichever comes first. Security policies, security training, and regulatory training are required to be reviewed annually. In 2017, an Information Security Management System (ISMS) meeting ISO 27001:2013 standard was implemented and certified to the standard. The ISMS is scheduled to completely replace the Information Security Policy Manual in 2018. Changes to policies and procedures are distributed to employees and contracted staff members, who must acknowledge that they have received the information and/or training.

Automation, monitoring and management of procedures is conducted via the ticketing system, ServiceNow, which is ITIL based and has been configured by Secure-24 to meet the standards and documentation requirements set by Secure-24 policies, and client contracts.

Availability

Secure-24 hosted solutions are designed to maintain availability and recovery necessary to meet customer SLAs. Monitoring for system availability, system states that may impact availability, and system performance is in place and is communicated and managed according to the monitoring management processes. Incident management procedures are in place to react to and minimize service interruptions. Recommended capacity thresholds also alert customers and Secure-24 to review resource utilization before resource consumption impacts performance and availability.

Secure-24 data center are architected to provide N+1 services to all environments, and management reviews capacity monitoring regularly to ensure the availability of components and to conduct capacity planning. Recovery components across locations and continuity procedures are maintained, reviewed and performed regularly to evaluate emerging continuity risks.