MBO Data, LLC dba TulsaConnect

SOC 1® Type 2 Report

May 1, 2019 to April 30, 2020

Data Center Hosting Solutions System

TULSA 918.745.2333 | OKLAHOMA CITY 405.848.2020 | LITTLE ROCK 501.227.5800 | FAYETTEVILLE 479.521.9191
hogantaylor.com

Contents

I. Independent Service Auditor's Report

To Management
MBO Data, LLC dba TulsaConnect

Scope
We have examined MBO Data, LLC d/b/a TulsaConnect's (TulsaConnect or the Service Organization) description of its data center hosting solutions system (the system) throughout the period May 1, 2019 to April 30, 2020 (the description), the suitability of the design and the operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in the Service Organization's assertion. The controls and control objectives included in the description are those that management of the Service Organization believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the system that are not likely to be relevant to user entities' internal control over financial reporting.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of the Service Organization's controls are suitably designed and operating effectively, along with related controls at the Service Organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's responsibilities
In its description, the Service Organization has provided an assertion about the fairness of the presentation of the description, the suitability of the design and the operating effectiveness of the controls to achieve the related control objectives stated in the description. The Service Organization is responsible for preparing the description and its assertion, including the completeness, accuracy and method of presentation of the description and the assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Service auditor's responsibilities
Our responsibility is to express an opinion on the fairness of the presentation of the description, the suitability of the design, and the operating effectiveness of the controls to achieve the related control objectives 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, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period May 1, 2019 to April 30, 2020. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system, the suitability of the design and the operating effectiveness of controls involves performing procedures to obtain evidence about the fairness of the presentation of the description, the suitability of the design and the operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description. Our procedures also included testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved. An examination engagement of this type also includes evaluating the overall presentation of the description, the suitability of the control objectives stated therein, and the suitability of the criteria specified by the Service Organization in its assertion.

Inherent limitations

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives is subject to the risk that controls at a service organization may become ineffective.

Description of tests of controls

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

Opinion

In our opinion, in all material respects, based on the criteria described in the Service Organization's assertion:

a. The description fairly presents the system that was designed and implemented throughout the period May 1, 2019 to April 30, 2020.
b. The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period May 1, 2019 to April 30, 2020, and the user entities applied the complementary controls assumed in the design of the Service Organization's controls throughout the period May 1, 2019 to April 30, 2020.
c. The controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period May 1, 2019 to April 30, 2020, if the complementary user entity controls assumed in the design of the Service Organization's controls operated effectively throughout the period May 1, 2019 to April 30, 2020.

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 the Service Organization, user entities of the Service Organization's system during some or all of the period May 1, 2019 to April 30, 2020, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

Tulsa, Oklahoma
May 26, 2020

II. Management's Assertion of the System

We have prepared the description of MBO Data, LLC d/b/a TulsaConnect's (TulsaConnect or the Service Organization) data center hosting solutions system (the system) throughout the period May 1, 2019 to April 30, 2020 (the description), for user entities of the system during some or all of the period May 1, 2019 to April 30, 2020, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatement of user entities' financial statements.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of the Service Organization's controls are suitably designed and operating effectively, along with related controls at the Service Organization. The description does not extend to controls of the user entities.

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

a. The description fairly presents the system made available to user entities of the system during some or all of the period May 1, 2019 to April 30, 2020, for processing their transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description:
    i. Presents how the system made available to user entities of the system was designed and implemented to process relevant user entity transactions including, if applicable:
        - The types of services provided including, as appropriate, the classes of transactions processed;
        - The procedures, within both automated and manual systems, by which those services are provided including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary and transferred to the reports and other information prepared for user entities of the system;
        - The information used in the performance of the procedures including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities;
        - How the system captures and addresses significant events and conditions, other than transactions;

- The process used to prepare reports and other information for user entities;
- Services performed by subservice organizations, if any, including whether the inclusive method or the carve-out method has been used in relation to them;
- The specified control objectives and controls designed to achieve those objectives including, as applicable, complementary user entity controls assumed in the design of the Service Organization's controls; and
- Other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities and monitoring activities that are relevant to the services provided.

ii. Includes relevant details of changes to the Service Organization's system during the period covered by the description;

iii. Does not omit or distort information relevant to the Service Organization's system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors, and may not, therefore, include every aspect of the Service Organization's system that each individual user entity of the system and its auditor may consider important in its own particular environment.

b. The controls related to the control objectives stated in the description were suitably designed and operating effectively, throughout the period May 1, 2019 to April 30, 2020, to achieve those control objectives if the user entities applied the complementary controls assumed in the design of the Service Organization's controls throughout the period May 1, 2019 to April 30, 2020. The criteria we used in making this assertion were that:

i. The risks that threaten the achievement of the control objectives stated in the description have been identified by management of the Service Organization;

ii. The controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and

iii. The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Sincerely,

Mr. Jarrod Cavner, Manager of Technical Services
MBO Data, LLC d/b/a TulsaConnect

III. TulsaConnect's Description of the System

OVERVIEW

TulsaConnect is a privately held provider of data center hosting and associated managed Information Technology (IT) services. Headquartered in Tulsa, Oklahoma, TulsaConnect operates the data center division of MBO, LLC.

MBO, LLC is a privately held company that includes third-generation Oklahoma telecommunication principals. Through its subsidiaries, MBO, LLC provides voice, video, and data services on a wholesale and retail level to clients in a four-state area. MBO owns Cimarron Telephone Company and Cim-Tel Cable, Pottawatomie Telephone Company, MBO Networks, MBO Wireless, MBO Aviation, and Lakeland Properties.

The primary sales office is located at 110 W. 7th St, Tulsa, Oklahoma 74119, and the data center locations are as follows:

- **DC-2 and DC-5**: 110 W. 7th St, Tulsa, Oklahoma 74119
- **DC-3 and DC-3B**: 4500 S. 129th E Ave, Tulsa, Oklahoma 74134
- **DC-4**: 701 N. Broadway Ave, Oklahoma City, Oklahoma 73102

SERVICES PROVIDED

TulsaConnect provides highly redundant, available, and secure data center services for a variety of client needs. The primary offered services include private cloud, shared cloud, colocation, managed and professional services, and shared web hosting.

Private Cloud

TulsaConnect supplies dedicated hardware resources (servers, firewall, and associated devices) to a single client and employs virtualization technology (such as VMware or Hyper-V) to allow for multiple virtual machines (VMs) to be run within a cloud environment. Pricing is based on the hardware resources and managed services desired. High-availability options are available including replication between multiple TulsaConnect data centers.

Shared Cloud

TulsaConnect supplies a VM instance on a shared hosting infrastructure for the client's use. Pricing is based on the physical server resources (disk, memory CPU) and services desired.

Colocation

Clients provide their own servers, network equipment, and associated devices and place them in secure racks at one of the data center locations. TulsaConnect supplies redundant power, network, and environmental control for a monthly fee. Pricing is based on the amount of space, power, network utilized, and other managed services required.

Managed and Professional Services

TulsaConnect offers several complementary managed services along with the hosting offerings. These services include data backup, systems administration, operating system (OS) install and patch updates, managed firewall and intrusion detection system, virtual private network and wide area network, and in-depth server monitoring.

Shared Web Hosting

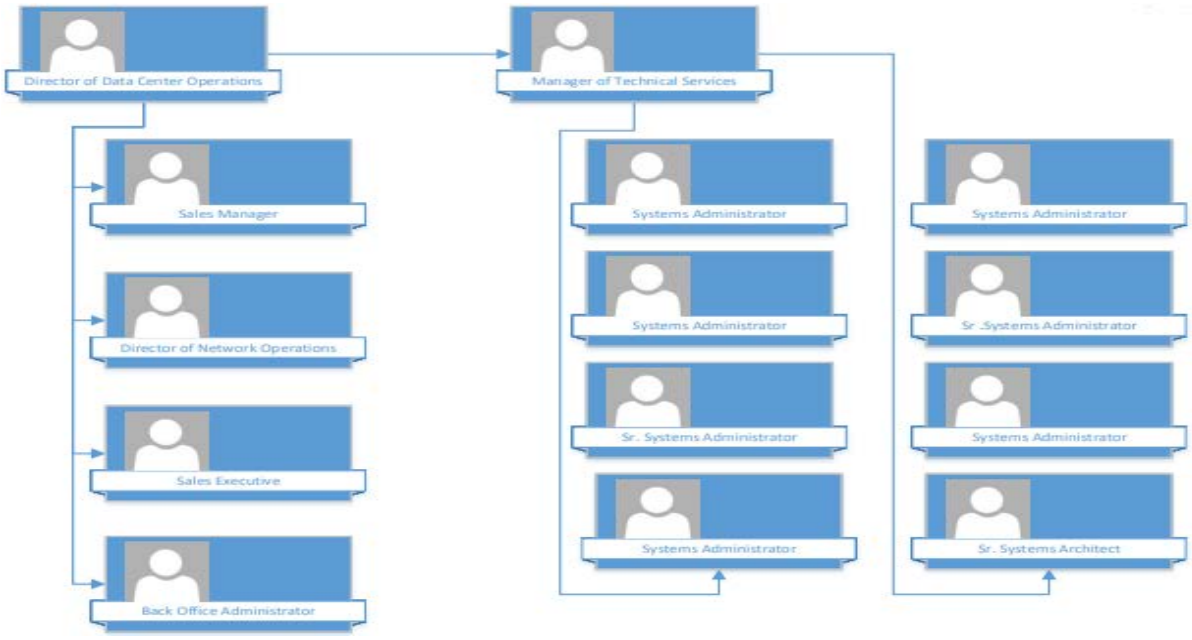
For basic needs, TulsaConnect offers shared website and email hosting services. This includes add-on items such as antivirus, anti-spam scanning for email, and website statistics packages.

CONTROL ENVIRONMENT

The objectives of internal control as it relates to TulsaConnect's data canter hosting solutions are to provide reasonable, but not absolute, assurance that controls are suitably designed and operating effectively to meet the relevant operational needs, that assets and data are protected from unauthorized access, modification, use, or disposition, and that services are conducted in accordance with management's authorization and client instructions. Management has established and maintained controls designed to monitor compliance with TulsaConnect's policies and procedures.

Organizational Structure

TulsaConnect is segregated into separate functional areas to manage client information, the processing of the information, and to ensure adequate separation of duties. TulsaConnect's organizational chart reflects appropriate segregation of duties:



Management Oversight

Management of TulsaConnect is performed by its corporate executives, who are responsible for business strategy, delivery of services, and the design and implementation of information security controls, as reviewed annually. Policies and procedures are documented and maintained in a centralized employee-accessible database. Continued administration of the development, implementation, and maintenance of policies and procedures is the shared responsibility of the Director of Data Center Operations and Manager of Technical Services.

Integrity and Ethics

The Employee Handbook includes policies and procedures regarding business ethics and conduct. The handbook requires that employees conduct business operations in a manner which supports and complies with applicable laws and regulations. The handbook also includes Rules of Conduct to specify the disciplinary actions associated with acts of misconduct.

Personnel

Employee policies and procedures are provided to employees upon hire in the Employee Handbook. New employees sign a nondisclosure agreement as well as an acknowledgement of receipt of and compliance with the Employee Handbook. Background checks, phone screenings and/or in-person interviews, and reference checks are completed prior to hiring. Job descriptions are documented for each position and annual employee training includes Health Insurance Portability and Accountability Act (HIPAA) and security awareness.

Risk Assessment

Management updates a risk assessment of the control objectives and related controls described in this report on an annual basis during TulsaConnect's policies and procedures review. Management identifies threats and vulnerabilities relevant to the security of its business operations, then considers the following for each identified vulnerability:

- The likelihood of impact (i.e., the likelihood of the vulnerability being exploited), and
- The severity of impact (i.e., how damaging an exploitation of the vulnerability would be).

These estimations of impact potential and impact severity are used in conjunction to establish a risk ranking for each vulnerability. If a vulnerability is unlikely to be exploited and would have a minor impact, it is viewed as a relatively small risk. If a vulnerability is very likely to be exploited and would have a severe impact, it is viewed as a very significant risk. Other combinations of likelihood and severity (high likelihood, low impact; low likelihood, high impact; moderate likelihood, moderate impact; etc.) result in establishment of a risk ranking along this continuum.

Once the severity of risk posed by each identified vulnerability has been broadly quantified, TulsaConnect management ensures that the design and operation of its controls are sufficient to mitigate risks to an acceptable level.

The following types of risk are identified during TulsaConnect's risk assessment process:

- Operational risks associated with information systems, manual processes, and external systems,

- Financial and legal risks associated with market and organizational changes, regulatory costs, or other negligent action, and
- Technology risks associated with intrusion, system failure, and errors.

Monitoring

The management and supervisory personnel of TulsaConnect monitor performance quality and control operation as a normal part of their activities. The organization has implemented a series of key indicator management reports that measure the results of various processes involved in providing service to clients. These include reports that identify and detail various computerized information system events, such as failed access attempts, rejected items, deviations from scheduled processing, and program changes.

These reports are periodically reviewed (depending on the nature of the item being reported on) by appropriate levels of management, and action is taken as necessary. Depending on the nature, age, and amount (as applicable) of processing exceptions, they are referred to higher levels of management for review.

GENERAL IT CONTROLS

Physical Security

Within the data centers, security fences with locked gates or locked rack cabinets protect critical infrastructure components. In shared data processing areas, client equipment is secured in locked cabinets. Client cabinets have locking front and back doors and are locked when not being accessed by a client and/or TulsaConnect staff. TulsaConnect employees are the only keyholders to the client cabinets. In addition, clients are escorted while in the data centers. No clients or visitors are granted unescorted access to the Network Operations Center (NOC), uninterruptible power supply (UPS) room, or generator area. Client access to data center facilities must be pre-authorized and visitors are met by TulsaConnect personnel outside of data center points of entry.

Facilities are accessed via a TulsaConnect escort, with the exception of authorized service personnel who are working on mechanical systems. Access codes are given to permanent electrical, heating, ventilation, and air conditioning (HVAC), data cabling and other service vendors. This allows permanent vendors to address potential service impacting events while waiting for a TulsaConnect employee to arrive onsite. Access to the floor containing the Oklahoma City data center is restricted by elevator key code. The sites in Tulsa are similarly secured with escorted access.

TulsaConnect has implemented and maintains a policy on physical security of information systems, which is reviewed and authorized by management at least annually. Physical access to the corporate offices, NOC, and data centers is controlled by biometric access and/or locks. Biometric authentication is implemented at entrances that lead to areas where client or data center equipment resides. Biometric access controls recognize TulsaConnect employees via fingerprint identification. These biometric access controls record a log of individuals that entered the data center, including the date and time of access. Authorized users are registered in the system through a controlled, documented process.

When a facility entrance door is opened, a NetBotz security device takes a series of pictures of the person(s) entering and exiting the data center and sends the time-stamped pictures to TulsaConnect NOC staff via email. These logs are archived for 90 days. TulsaConnect data centers are monitored with video surveillance cameras that record on motion. This data is stored for at least 180 days.

Environmental Security

The TulsaConnect data centers are designed for and feature redundant HVAC units. Computer room air conditioning (CRAC) and chiller units comprise the system. Client cabinets are arranged in a standard hot aisle/cold aisle configuration. NetBotz appliances are used to monitor the outlet and return temperatures on CRAC units, as well as to monitor humidity and sound levels in the room.

Data centers are equipped with fire detection devices and inert gas fire suppression systems. The data centers are configured with either a water-based dual-interlock, pre-action, dry-pipe, suppression system or a gas-based system and manual fire extinguishers. These extinguishers are filled with Ansul FM36, which is specifically designed to contain data center fires without harming sensitive electronics. In addition, the extinguishers are inspected once a year.

The environmental sensors in the data centers monitor temperature and humidity and are equipped with cameras. The sensors also provide email alerts and audible alerts. The data center's camera records are maintained for a minimum of 90 days, but other historical data may be available.

Three-phase electrical power is supplied by the local utility company. The utility power feed flows through a series of automatic transfer switches, which are also connected to onsite emergency generators. During a utility power failure, the transfer switch automatically starts the onsite generator. Within 30 seconds, the onsite generator begins supplying usable electrical power to the data center.

Electrical power flows through UPS systems, which supply clean power to the critical data center loads. Each UPS system has a series of battery cabinets, which are designed to support the critical data center load while the generator starts up in the event of utility power failure. Systems are configured with the intent to maintain at least 40 minutes of battery runtime on each UPS system.

Onsite emergency generators are in place and operational to supply full load electrical power in the event of a public utility power grid failure. A secondary external generator connection point is installed on the outside of each building in which data centers are housed. The secondary emergency power connection point allows TulsaConnect to attach a trailer-mounted diesel generator in the event of a primary generator failure.

Diesel generators are automatically exercised weekly. A dry contact is triggered via a NetBotz appliance to alert support personnel when the test starts and ends.

Logical Access

Policies and procedures are documented and maintained in a centralized employee-accessible database. Management is responsible for the continued administration of the development, implementation, and maintenance of policies and procedures to direct, guide and authorize logical access control.

Logical access to the local area network (LAN) used to support the data center operations is restricted to authorized TulsaConnect personnel. A user ID and password combination is required to access network resources and file systems. For remote access to the support network, a virtual private network (VPN) connection is required.

TulsaConnect personnel access is granted on a least privilege concept. Network and application access requires approval from the Director of Data Center Operations or Manager of Technical Services. System Administrators are assigned unique user accounts, and default accounts are disabled or deleted.

A password policy is in place to enforce the use of complex passwords. Passwords must be at least ten characters in length and include characters from three of the following four categories:

- English uppercase characters (A through Z),
- English lowercase characters (a through z),
- Base ten digits (zero through nine), and
- Nonalphanumeric characters.

Network Security

Policies and procedures are documented and maintained in a centralized employee-accessible database. Management is responsible for the continued administration of the development, implementation, and maintenance of policies and procedures to direct, guide and authorize the operation of network security.

The perimeter of the TulsaConnect support network is protected by a dedicated firewall. Data center traffic from the outside is routed to client specific subnets using external internet protocol (IP) addresses. The client controls rules below this initial routing. The firewall rule set has been configured in accordance with a default-deny concept. TulsaConnect's support network firewall utilizes antivirus, intrusion prevention systems (IPS) and geo-IP filtering technology as additional layers of protection.

Access to administrative functions on the TulsaConnect systems is restricted to authorized personnel. Remote access authorization is provided by the Director of Data Center Operations to TulsaConnect personnel with a supportable business need for remote access.

Access to TulsaConnect systems is segregated through the use of a network switching mechanism. Clients are connected to a Cisco 6509-E routing switch. Each port is configured in a Layer 3 configuration, with the exception of clients with multiple ports in which case a virtual local area network (VLAN) is created and the IP subnet is created on the VLAN interface.

Data center clients are assigned a unique IP subnet that does not overlap with other client subnets. Clients are provisioned on a separate switch port, which is configured in Layer 3 mode. Clients are provided external IPs as required. Justification includes things like Secure Sockets Layer (SSL) certificates or Terminal Servers. An appropriately sized network block to meet client requirements is requested from the Director of Network Engineering. The Director of Network Engineering determines which IP block to use and gives the information back to the System Administrator who requested it.

Vulnerability Management and Monitoring

Policies and procedures are documented and maintained in a centralized employee-accessible database. Management is responsible for the continued administration of the development, implementation, and maintenance of policies and procedures to direct, guide and authorize the operation of systems monitoring for faults and incidents.

Daily data center walkthroughs are performed to inspect for client server warning lights. Antivirus tools protect servers and network resources, administrative workstations, and data center networks. TulsaConnect data centers use DefenderMX software for email scanning services. Incoming email messages are automatically scanned for virus and malware threats. Virus definitions are updated daily.

Change Management

Policies and procedures are documented and maintained in a centralized employee-accessible database. Management is responsible for the continued administration of the development, implementation, and maintenance of policies and procedures to direct, guide and authorize the operation of change management. The primary contact mechanism for customer support is via email. Issues submitted via email are documented, prioritized, and tracked through the Help Desk application. Clients may also contact support via telephone. Client issues may require a follow up email for documentation purposes. Additionally, planned and emergency maintenance of facility-wide UPS systems are communicated to the customer via email.

Backup and Recovery

Policies and procedures are documented and maintained in a centralized employee-accessible database. Management is responsible for the continued administration of the development, implementation, and maintenance of policies and procedures to direct, guide and authorize the operation of data backup.

Backup job failures are logged by the backup software and are investigated in a timely manner. TulsaConnect personnel monitor the status of jobs on a routing basis. The backup software displays a report with the most recent backup success/failure status.

SERVICE CONTROLS

Service Levels

Policies and procedures are documented and maintained in a centralized employee-accessible database. Management is responsible for the continued administration of the development, implementation, and maintenance of policies and procedures to direct, guide and authorize service levels of network security.

Prior to the deployment of new client services, the rights and responsibilities of the client and TulsaConnect are clearly communicated through the signing of a service agreement and a general services agreement. TulsaConnect does not guarantee service levels but does have provisions for claw back.

COMPLEMENTARY USER ENTITY CONTROLS

TulsaConnect's services are designed with the assumption that certain controls are implemented by user entities. In certain situations, the application of specific controls at the user entity is necessary to achieve control objectives included in this report.

This section describes additional controls that should be in operation at user entities to complement the TulsaConnect controls. User entity control recommendations include:

- User entities should implement sound and consistent internal controls regarding general IT system access and system usage appropriateness for internal user entity components associated with TulsaConnect.
- User entities should ensure timely removal of user accounts for users who have been terminated and were previously involved in material functions or activities associated with TulsaConnect's services.
- Transactions for user entities relating to TulsaConnect's services should be appropriately authorized, secure, timely, and complete.
- For user entities sending data to TulsaConnect, data should be protected by appropriate methods to ensure confidentiality, privacy, integrity, availability, and nonrepudiation.
- User entities should implement controls requiring additional approval procedures for critical transactions relating to TulsaConnect's services.
- User entities should report to TulsaConnect in a timely manner material changes to their overall control environment that may adversely affect services being performed by TulsaConnect.
- User entities are responsible for notifying TulsaConnect in a timely manner of changes to personnel directly involved with services performed by TulsaConnect. These personnel may be involved in financial, technical or ancillary administrative functions directly associated with services provided by TulsaConnect.
- User entities are responsible for adhering to the terms and conditions stated within their contracts with TulsaConnect.
- User entities are responsible for developing, and if necessary, implementing a business continuity and disaster recovery plan (BCDRP) that aids in the continuation of services provided by TulsaConnect.

The list of user entity control considerations presented above do not represent a comprehensive set of the controls that should be employed by user entities. Other controls may be required at user entities. Therefore, each client's system of internal controls must be evaluated in conjunction with the internal control structure described in this report.

CONTROL OBJECTIVES SPECIFIED BY TULSACONNECT

TulsaConnect's control objectives and related controls are an integral part of its system description. The objectives and related controls are contained within Section IV – Tests of Operating Effectiveness and Results of Tests Performed by the Service Auditor.

IV. Tests of Operating Effectiveness and Results of Tests Performed by the Service Auditor

This section includes the objectives and related controls which are the responsibility of TulsaConnect. The control tests and results of tests are the responsibility of the service auditor. The tests performed include inquiry of appropriate personnel and corroboration with management, observation of the application, performance, or existence of the control, inspection of documents and reports indicating performance of the control, and/or reperformance of the control. In addition, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

Objective 1 Controls provide reasonable assurance that management maintains segregation of duties and is responsible for oversight and consistent implementation of security practices.			
Control Specified by TulsaConnect		***Testing Performed by HT***	***Test Results***
1.01	Management is responsible for business strategy, delivery of services, and the design and implementation of information security controls including annual review of related policies and procedures.	Inspected Policies and Procedures Manual to verify strategy, services, and controls were reviewed and updated annually.	No exceptions noted.
1.02	Organizational structure is grouped into functional areas to ensure adequate separation of duties around the management and processing of client information.	Inspected organizational chart to verify separate functional areas support sufficient segregation of duties within the organization.	No exceptions noted.

Objective 1 Controls provide reasonable assurance that management maintains segregation of duties and is responsible for oversight and consistent implementation of security practices.			
Control Specified by TulsaConnect		***Testing Performed by HT***	***Test Results***
1.03	TulsaConnect policies and procedures are documented and maintained in a centralized employee-accessible knowledge base. Continued administration of the development, implementation, and maintenance of policies and procedures is the shared responsibility of the Director of Operations and Manager of Technical Services.	Inspected Policies and Procedures Manual to verify policies and procedures were formally documented and reviewed by the Director of Operations and Manager of Technical Services. Inspected centralized knowledge base system to verify policies and procedures were made available to employees.	No exceptions noted. No exceptions noted.
1.04	Employee policies and procedures are documented in the Employee Handbook and acknowledged by employees as part of the hiring process.	Inspected Employee Handbook to verify employee policies and procedures were formally documented. Attempted to select a sample of new hires to verify Employee Handbooks were acknowledged during the hiring process.	No exceptions noted. Not tested: Per discussion with management, there were no new employees hired during the period.
1.05	Confidentiality and privacy policies are included in the Employee Handbook and employees sign a nondisclosure agreement, acknowledgement of receipt, and acceptance of compliance upon hire.	Inspected Employee Handbook to verify employee confidentiality and privacy policies were formally documented. Attempted to select a sample of new hires to verify confidentiality and privacy policies were acknowledged upon hire.	No exceptions noted. Not tested: Per discussion with management, there were no new employees hired during the period.

Objective 1 Controls provide reasonable assurance that management maintains segregation of duties and is responsible for oversight and consistent implementation of security practices.			
Control Specified by TulsaConnect		***Testing Performed by HT***	***Test Results***
1.06	Annual employee training includes HIPAA and security awareness.	Selected a sample of employees and inspected training attendance to verify employees received HIPAA and security training.	No exceptions noted.

Objective 2 Controls provide reasonable assurance that employees understand their responsibilities and are suitable for the roles for which they are considered.			
Control Specified by TulsaConnect		***Testing Performed by HT***	***Test Results***
2.01	Job descriptions for employee positions are formally documented to define and communicate responsibilities, qualifications, and requirements.	Selected a sample of position titles and inspected job descriptions to verify responsibilities, qualifications, and requirements were formally documented.	No exceptions noted.
2.02	Employee policies and procedures are documented in the Employee Handbook and acknowledged by employees as part of the hiring process.	Inspected Employee Handbook to verify employee policies and procedures were formally documented. Attempted to select a sample of new hires to verify Employee Handbooks were acknowledged during the hiring process.	No exceptions noted. Not tested: Per discussion with management, there were no new employees hired during the period.
2.03	Confidentiality and privacy policies are included in the Employee Handbook and employees sign a nondisclosure agreement, acknowledgement of receipt, and acceptance of compliance upon hire.	Inspected Employee Handbook to verify employee confidentiality and privacy policies were formally documented. Attempted to select a sample of new hires to verify confidentiality and privacy policies were acknowledged upon hire.	No exceptions noted. Not tested: Per discussion with management, there were no new employees hired during the period.

Objective 2 Controls provide reasonable assurance that employees understand their responsibilities and are suitable for the roles for which they are considered.			
Control Specified by TulsaConnect		***Testing Performed by HT***	***Test Results***
2.04	Background checks are obtained during the hiring process to confirm candidate eligibility.	Attempted to select a sample of new hires to verify background checks were conducted during the hiring process.	Not tested: Per discussion with management, there were no new employees hired during the period.
2.05	Reference checks are performed by TulsaConnect or recruiter prior to hiring to confirm candidate qualifications.	Attempted to select a sample of new hires to verify references were checked during the hiring process.	Not tested: Per discussion with management, there were no new employees hired during the period.
2.06	Annual employee training includes HIPAA and security awareness.	Selected a sample of employees and inspected training attendance to verify employees received HIPAA and security training.	No exceptions noted.

Objective 3 Controls provide reasonable assurance that physical assets are adequately protected against environmental hazards and related damage, and that physical access to the computer equipment, system infrastructure, and storage media is limited to authorized personnel.			
Control Specified by TulsaConnect		***Testing Performed by HT***	***Test Results***
3.01	Policies and procedures are documented and maintained to direct, guide, and authorize physical security.	Inspected Policies and Procedures Manual to verify physical security policies and procedures were formally documented.	No exceptions noted.
3.02	Customer and vendor access to data center facilities is pre-authorized and visitors are met by TulsaConnect personnel outside of data center points of entry to be escorted in to the data center.	Observed facility entrances and discussed with management to verify visitor access is escorted by TulsaConnect personnel.	No exceptions noted.

Objective 3 Controls provide reasonable assurance that physical assets are adequately protected against environmental hazards and related damage, and that physical access to the computer equipment, system infrastructure, and storage media is limited to authorized personnel.			
Control Specified by TulsaConnect		***Testing Performed by HT***	***Test Results***
3.03	Data center entrances require biometric identification of TulsaConnect personnel.	Observed the use of biometric access door locks and inspected NetBotz monitoring footage for each location. Inspected physical security system access lists for each location to verify access was restricted to authorized biometrics.	No exceptions noted. No exceptions noted.
3.04	Temporary access codes are given to authorized permanent service personnel when work on mechanical systems is being performed.	Inspected data center physical security system access lists and logs for each location to verify limited access codes were given to authorized vendors and that use of the codes was logged.	No exceptions noted.
3.05	When a facility entrance door is opened, a NetBotz security device takes a series of pictures of the area and sends the time-stamped images to TulsaConnect NOC staff via email. These logs are archived for 90 days.	Selected a sample of dates for the last 90 days during the period and inspected email notifications to verify door alerts for each data center were logged and stored.	No exceptions noted.
3.06	TulsaConnect Data Centers are monitored with video surveillance cameras that record on motion and store images for at least 180 days.	Inspected data center surveillance files for each location to verify recordings were stored for at least 180 days. Observed cameras for each location to verify video surveillance was in place.	No exceptions noted. No exceptions noted.
3.07	Customer equipment in data center areas is secured in locked cabinets. TulsaConnect employees have keys to customer cabinets or racks.	Inspected locked rack cabinets at each data center location to verify access to customer equipment was secure and restricted by key lock.	No exceptions noted.

Objective 3 Controls provide reasonable assurance that physical assets are adequately protected against environmental hazards and related damage, and that physical access to the computer equipment, system infrastructure, and storage media is limited to authorized personnel.			
Control Specified by TulsaConnect		***Testing Performed by HT***	***Test Results***
3.08	Data centers are designed for and feature redundant HVAC units, which are properly maintained.	Observed HVAC units to verify they were in place at each data center. Inspected HVAC service reports for each data center to verify units were regularly maintained.	No exceptions noted. No exceptions noted.
3.09	Environmental sensors are installed in the data centers and send alerts based on parameters for motion, temperature, humidity, air flow, and door position.	Observed NetBotz monitoring units to verify sensors were in place at each data center entrance. Inspected NetBotz alert dashboard monitoring to verify environmental sensors were installed in each data center.	No exceptions noted. No exceptions noted.
3.10	Data centers are equipped with fire detection and suppression devices, including annually-serviced fire extinguishers.	Observed the placement of fire sensors and inert gas fire suppression systems to verify equipment was in place at each data center. Inspected fire extinguisher maintenance tags at each data center to verify equipment was inspected and properly maintained.	No exceptions noted. No exceptions noted.
3.11	Data centers and critical systems in administrative offices are equipped with UPS units, which are properly maintained.	Observed UPS units to verify equipment was in place at each data center. Inspected annual UPS Preventative Maintenance Reports to verify UPS systems at each data center were maintained in accordance with equipment service plans.	No exceptions noted. No exceptions noted.

Objective 3 Controls provide reasonable assurance that physical assets are adequately protected against environmental hazards and related damage, and that physical access to the computer equipment, system infrastructure, and storage media is limited to authorized personnel.			
Control Specified by TulsaConnect		***Testing Performed by HT***	***Test Results***
3.12	Onsite emergency generators are properly maintained and in place to supply full load electrical power in the event of a public utility power grid failure.	Observed onsite emergency generators to verify equipment was in place at each data center. Selected a sample of quarters and inspected generator work orders for each data center to verify maintenance and repairs were conducted.	No exceptions noted. No exceptions noted.
3.13	Onsite emergency generators are automatically exercised on a weekly basis.	Selected a sample of weeks and inspected email alerts for each data center to verify generators were exercised weekly.	No exceptions noted.
3.14	External generator connection points for a trailer-mounted diesel generator are installed on the outside of each data center building in the event of a primary generator failure.	Observed external generator connections to verify secondary emergency power points were in place at each data center.	No exceptions noted.

Objective 4 Controls provide reasonable assurance that system availability is maintained and that systems operate in a consistent and predictable manner.			
Control Specified by TulsaConnect		***Testing Performed by HT***	***Test Results***
4.01	Policies and procedures are documented and maintained to direct, guide, and authorize system availability and data center facility operations in a consistent, predictable manner.	Inspected Policies and Procedures Manual to verify system availability and data center operations policies and procedures were formally documented.	No exceptions noted.
4.02	Policies and procedures are documented and maintained to direct, guide, and authorize client support operations.	Inspected Policies and Procedures Manual to verify customer support policies and procedures were formally documented.	No exceptions noted.

Objective 4 Controls provide reasonable assurance that system availability is maintained and that systems operate in a consistent and predictable manner.			
Control Specified by TulsaConnect		***Testing Performed by HT***	***Test Results***
4.03	Daily data center walkthroughs are performed to inspect for customer server warning lights.	Selected a sample of dates and inspected walkthrough logs for each data center to verify onsite monitoring inspections were performed and documented daily.	No exceptions noted.
4.04	Environmental sensors are installed in the data centers and send alerts based on parameters for motion, temperature, humidity, air flow, and door position.	Observed NetBotz monitoring units to verify sensors were in place at each data center entrance. Inspected NetBotz alert dashboard monitoring to verify environmental sensors were installed in each data center.	No exceptions noted. No exceptions noted.
4.05	Data centers are designed for and feature redundant HVAC units, which are properly maintained.	Observed HVAC units to verify they were in place at each data center. Inspected HVAC service reports for each data center to verify units were regularly maintained.	No exceptions noted. No exceptions noted.
4.06	Data centers are equipped with fire detection and suppression devices, including annually-serviced fire extinguishers.	Observed the placement of fire sensors and inert gas fire suppression systems to verify equipment was in place at each data center. Inspected fire extinguisher maintenance tags at each data center to verify equipment was inspected and properly maintained.	No exceptions noted. No exceptions noted.

Objective 4 Controls provide reasonable assurance that system availability is maintained and that systems operate in a consistent and predictable manner.			
Control Specified by TulsaConnect		***Testing Performed by HT***	***Test Results***
4.07	Data centers and critical systems in administrative offices are equipped with UPS units, which are properly maintained.	Observed UPS units to verify equipment was in place at each data center. Inspected annual UPS Preventative Maintenance Reports to verify UPS systems at each data center were maintained in accordance with equipment service plans.	No exceptions noted. No exceptions noted.
4.08	Onsite emergency generators are properly maintained and in place to supply full load electrical power in the event of a public utility power grid failure.	Observed onsite emergency generators to verify equipment was in place at each data center. Selected a sample of quarters and inspected generator work orders for each data center to verify maintenance and repairs were conducted.	No exceptions noted. No exceptions noted.
4.09	Onsite emergency generators are automatically exercised on a weekly basis.	Selected a sample of weeks and inspected email alerts for each data center to verify generators were exercised weekly.	No exceptions noted.
4.10	External generator connection points for a trailer-mounted diesel generator are installed on the outside of each data center building in the event of a primary generator failure.	Observed external generator connections to verify secondary emergency power points were in place at each data center.	No exceptions noted.

Objective 5 Controls provide reasonable assurance that logical access to programs, data, and operating systems is restricted to authorized personnel.			
Control Specified by TulsaConnect		***Testing Performed by HT***	***Test Results***
5.01	Policies and procedures are documented and maintained to direct, guide, and authorize logical security and user access provisioning.	Inspected Policies and Procedures Manual to verify logical security policies and procedures were formally documented.	No exceptions noted.
5.02	System access is granted to TulsaConnect personnel on a least privilege concept and user groups are assigned based on job description.	Inspected Active Directory security group privileges to verify access was assigned and restricted to authorized personnel.	No exceptions noted.
5.03	Logical access to data center operations systems is restricted to authorized TulsaConnect Personnel.	Inspected Active Directory user listing to verify logical access was restricted to authorized personnel.	No exceptions noted.
5.04	System Administrators are assigned unique user accounts on the TulsaConnect support network.	Inspected Domain Administrators security group to verify individuals were assigned unique user accounts.	No exceptions noted.
5.05	Access to administrative functions on TulsaConnect systems is restricted to authorized personnel.	Inspected Active Directory list of Domain Administrators to verify access was restricted to authorized personnel.	No exceptions noted.
5.06	The TulsaConnect Active Directory security policy is configured to enforce password length, complexity, expiration, and history requirements.	Inspected TulsaConnect support network password policy configurations to verify length, complexity, expiration, and history requirements were enabled.	No exceptions noted.

Objective 6 Controls provide reasonable assurance that network security and monitoring procedures are in place to identify and report unauthorized access attempts, and that clients understand the limits of the TulsaConnect service and their responsibility to implement network security controls.			
Control Specified by TulsaConnect		***Testing Performed by HT***	***Test Results***
6.01	Policies and procedures are documented and maintained to direct, guide, and authorize network security operations and monitoring.	Inspected Policies and Procedures Manual to verify network security and monitoring policies and procedures were formally documented.	No exceptions noted.
6.02	Policies and procedures are documented and maintained to direct, guide, and authorize network-level security for customer services.	Inspected Policies and Procedures Manual to verify network security service level policies and procedures were formally documented.	No exceptions noted.
6.03	Prior to the deployment of new client services, the rights and responsibilities of the client and TulsaConnect are clearly communicated through the signing of a Customer Service Agreement and a General Services Agreement.	Selected a sample of new clients and inspected signed agreements to verify rights and responsibilities were clearly communicated.	No exceptions noted.
6.04	Access to administrative functions on TulsaConnect systems is restricted to authorized personnel.	Inspected Active Directory list of Domain Administrators to verify access was restricted to authorized personnel.	No exceptions noted.
6.05	The perimeter of the TulsaConnect support network is protected by a dedicated firewall.	Inspected firewall rulesets for each location to verify dedicated firewalls were in place to protect the TulsaConnect support network.	No exceptions noted.
6.06	The firewall ruleset is configured in accordance with a default-deny concept.	Inspected TulsaConnect firewall rules for each location to verify default-deny configurations.	No exceptions noted.
6.07	TulsaConnect systems access is segregated through the use of a network switching mechanism.	Inspected network diagram to verify customer data comes into each data center and is routed to a customer firewall.	No exceptions noted.

Objective 6 Controls provide reasonable assurance that network security and monitoring procedures are in place to identify and report unauthorized access attempts, and that clients understand the limits of the TulsaConnect service and their responsibility to implement network security controls.			
Control Specified by TulsaConnect		***Testing Performed by HT***	***Test Results***
6.08	Data center customers are assigned unique IP subnets.	Inspected network diagram and internal communications to verify customer IP subnets are unique.	No exceptions noted.

Objective 7 Controls provide reasonable assurance that systems, processes, and software are tested periodically to ensure that security is maintained over time and after changes.			
Control Specified by TulsaConnect		***Testing Performed by HT***	***Test Results***
7.01	Policies and procedures are documented and maintained to direct, guide, and authorize systems monitoring operations.	Inspected Policies and Procedures Manual to verify systems monitoring policies and procedures were formally documented.	No exceptions noted.
7.02	Daily data center walkthroughs are performed to inspect for customer server warning lights.	Selected a sample of dates and inspected walkthrough logs for each data center to verify onsite monitoring inspections were performed and documented daily.	No exceptions noted.
7.03	Antivirus tools protect servers and network resources, administrative offices, and data center networks.	Inspected firewall network security appliance services summary, configurations, licensing status, and consoles to verify antivirus tools were in place.	No exceptions noted.
7.04	Incoming email messages are automatically scanned for virus and malware threats.	Inspected system configurations to verify incoming email scanning was enabled.	No exceptions noted.

Objective 8 Controls provide reasonable assurance that routine, customer-requested, and emergency change management issues are communicated to the customer.			
Control Specified by TulsaConnect		***Testing Performed by HT***	***Test Results***
8.01	Policies and procedures are documented and maintained to direct, guide, and authorize change management operations.	Inspected Policies and Procedures Manual to verify change management policies and procedures were formally documented.	No exceptions noted.
8.02	Client issues submitted via email and phone are tracked through the HelpSpot application.	Selected a sample of customer support tickets and inspected change documentation to verify issues were tracked in HelpSpot.	No exceptions noted.
8.03	Planned and emergency maintenance of facility-wide UPS system is communicated to customers via email.	Inspected email notifications to verify planned and emergency maintenance was communicated with the customer.	No exceptions noted.

Objective 9 Controls provide reasonable assurance that data is backed up in a secure manner for offsite retrieval and backup details are logged.			
Control Specified by TulsaConnect		***Testing Performed by HT***	***Test Results***
9.01	Policies and procedures are documented and maintained to direct, guide, and authorize data backup operations.	Inspected Policies and Procedures Manual to verify data backup, replication, and recovery policies and procedures were formally documented.	No exceptions noted.
9.02	Data backups are performed daily based on client specifications and detail reports are logged in a ticketing system.	Selected a sample of dates and servers and inspected backup reports to verify backups were performed and details were logged.	No exceptions noted.

PRIVATE AND CONFIDENTIAL

Use or reproduction of this report by unauthorized parties is strictly prohibited.