PROVDOTNET, LLC

COLOCATION AND MANAGED SERVICES

REPORT OF CONTROLS AT A SERVICE ORGANIZATION RELEVANT TO SECURITY AND AVAILABILITY

AS OF
JUNE 30, 2020

TABLE OF CONTENTS

Kahn, Litwin, Renza & Co., Ltd.
Boston • Newport • Providence • Waltham

951 North Main Street, Providence, Rhode Island 02904
Phone: 401-274-2001 • Fax: 401-831-4018
Email: TrustedAdvisors@KahnLitwin.com • www.KahnLitwin.com

KLR

Certified Public Accountants and Business Consultants

I. INDEPENDENT SERVICE AUDITORS' REPORT

To the Management of
Provdotnet, LLC:

SCOPE

We have examined Provdotnet, LLC's accompanying description of its Colocation and Managed Services System found in Section IV titled "Description of Provdotnet, LLC's Colocation and Managed Services System" as of June 30, 2020 ("description") based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), ("description criteria") and the suitability of the design of controls stated in the description as of June 30, 2020, to provide reasonable assurance that Provdotnet, LLC's service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Availability ("applicable trust services criteria") set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

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

Provdotnet, LLC uses a subservice organization, Code42 Software, Inc., for cloud-based endpoint data security and recovery; a subservice organization, Zendesk, a cloud-based service provider for client help desk ticket support; a subservice organization, Intuit, Inc. (QuickBooks Online) for accounting software services including the manual processing of credit card transactions; and a subservice organization, Microsoft Office 365 (Office 365) for office productivity, email and document management services ("subservice organizations"). ("subservice organizations"). The description indicates that complementary subservice organizations' controls that are suitably designed and operating effectively are necessary, along with controls at Provdotnet, LLC, to achieve Provdotnet, LLC's service commitments and system requirements based on the applicable trust services criteria. The description presents Provdotnet, LLC's controls, the applicable trust services criteria, and the types of complementary subservice organizations' controls assumed in the design of Provdotnet, LLC's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organizations' controls.

SERVICE ORGANIZATION'S RESPONSIBILITIES

Provdotnet, LLC is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Provdotnet, LLC's service commitments and system requirements were achieved. In Section III, Provdotnet, LLC has provided the accompanying assertion titled "Management of Provdotnet, LLC's Assertion Regarding its Colocation and Managed Services System" ("assertion") about the description and the suitability of design of controls stated therein. Provdotnet, LLC 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 Provdotnet, LLC's service commitments and system requirements.

SERVICE AUDITORS' RESPONSIBILITIES

Our responsibility is to express an opinion on the description and on the suitability of design 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 to provide reasonable assurance that Provdotnet, LLC's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- obtaining an understanding of the system and the service organization's service commitments and system requirements.
- assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed.
- performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- evaluating the overall presentation of the description.

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

INHERENT LIMITATIONS

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design 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.

OTHER MATTER

We did not perform any procedures regarding the operating effectiveness of controls stated in the description and, accordingly, do not express an opinion thereon.

OPINION

In our opinion, in all material respects:

a. the description presents Provdotnet, LLC's Colocation and Managed Services System that was designed and implemented as of June 30, 2020 in accordance with the description criteria.
b. the controls stated in the description were suitably designed as of June 30, 2020 to provide reasonable assurance that Provdotnet, LLC's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date and if the subservice organizations and user entities applied the complementary controls assumed in the design of Provdotnet, LLC's controls as of that date.

RESTRICTED USE

This report is intended solely for the information and use of Provdotnet, LLC; user entities of Provdotnet, LLC's Colocation and Managed Services System as of June 30, 2020; business partners of Provdotnet, LLC subject to risks arising from interactions with the Colocation and Managed Services 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 Provdotnet, LLC.
- How Provdotnet, LLC's system interacts with user entities, business partners, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary subservice organization controls and how those controls interact with the controls at Provdotnet, LLC to achieve Provdotnet, LLC's service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use Provdotnet, LLC's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of Provdotnet, LLC'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.

Kahn, Litwin, Renza & Co., Ltd.

Boston, Massachusetts
September 24, 2020

II. REPORT OVERVIEW

A. REPORT APPLICABILITY

This report has been prepared in accordance with the requirements and guidance established in AT-C section 105, *Concepts Common to All Attestation Engagements* and AT-C section 205, *Examination Engagements* and in accordance with guidance from the AICPA for the performance and reporting on Service Organization Control ("SOC") reports, "*SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*".

B. APPLICABLE TRUST SERVICES CATEGORIES

The relevant Trust Services Categories for the Provdotnet, LLC Colocation and Managed Services System are the Security and Availability categories.

SECURITY

The trust services criteria relevant to Security address the need for information and systems to be protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the service organization's ability to achieve its service commitments and system requirements.

Security refers to the protection of:

a. *information* during its collection or creation, use, processing, transmission, and storage; and
b. *systems* that use electronic information to process, transmit or transfer, and store information to enable the achievement of the entity's service commitments and system requirements. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

AVAILABILITY

Information and systems are available for operation and use to meet the entity's objectives.

The trust services criteria relevant to Availability refer to the accessibility of information used by the entity's systems, as well as the products or services provided to its customers and address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

III. MANAGEMENT OF PROVDOTNET, LLC'S ASSERTION REGARDING ITS COLOCATION AND MANAGED SERVICES SYSTEM

We have prepared the accompanying description of Provdotnet, LLC's Colocation and Managed Services System titled Description of Provdotnet, LLC's Colocation and Managed Services System as of June 30, 2020 ("description") based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), ("description criteria"). The description is intended to provide report users with information about the Colocation and Managed Services System that may be useful when assessing the risks arising from interactions with Provdotnet, LLC's system, particularly information about system controls that Provdotnet, LLC has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability ("applicable trust services criteria") set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Provdotnet, LLC uses a subservice organization, Code42 Software, Inc., for cloud-based endpoint data security and recovery; a subservice organization, Zendesk, a cloud-based service provider for client help desk ticket support; a subservice organization, Intuit, Inc. (QuickBooks Online) for accounting software services including the manual processing of credit card transactions; and a subservice organization, Microsoft Office 365 (Office 365) for office productivity, email and document management services ("subservice organizations"). ("subservice organizations"). The description indicates that complementary subservice organizations' controls that are suitably designed and operating effectively are necessary, along with controls at Provdotnet, LLC, to achieve Provdotnet, LLC's service commitments and system requirements based on the applicable trust services criteria. The description presents Provdotnet, LLC's controls, the applicable trust services criteria, and the types of complementary subservice organizations' controls assumed in the design of Provdotnet, LLC'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 Provdotnet, LLC, to achieve Provdotnet, LLC's service commitments and system requirements based on the applicable trust services criteria. The description presents Provdotnet, LLC's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Provdotnet, LLC's controls.

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

1) The description presents Provdotnet, LLC's Colocation and Managed Services System that was designed and implemented as of June 30, 2020 in accordance with the description criteria.

2) The controls stated in the description were suitably designed as of June 30, 2020 to provide reasonable assurance that Provdotnet, LLC's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date and if the subservice organizations and user entities applied the complementary controls assumed in the design of Provdotnet, LLC's controls as of that date.

IV. DESCRIPTION OF PROVDOTNET, LLC'S COLOCATION AND MANAGED SERVICES SYSTEM

A. OVERVIEW OF PROVDOTNET'S OPERATIONS

Founded in 2009, Provdotnet, LLC (Provdotnet) is a provider of colocation and limited managed services. Provdotnet is headquartered in Providence, RI, and operates three (3) colocation hosting facilities which deploy high availability colocation and interconnect services companies located throughout the United States.

Provdotnet's colocation facility locations are typically selected to provide both nearby and geographic diversity companies operating in the New York and New England States. The colocation facilities feature Necessary-Plus-1 (N+1) infrastructure redundancy. Provdotnet's customers include organizations in the Telecommunications, Government, Media and High Technology industries. Provdotnet does not provide any computing or data storage for customers as customers establish their own data center computing, security, switching, and data storage within any of Provdotnet's facilities.

Provdotnet allows businesses to launch new online services, shared computing resource services (i.e., cloud services), or new business applications to their Customer's or constituents. Provdotnet is classified as a registered Internet Service Provider ("ISP") that provides customers with internet services ranging from one megabit to ten gigabits per second.

Provdotnet provides Primary or Disaster Recovery Site services to customers needing a remote site for their backup computers and applications. Provdotnet also provides managed turnkey-like services that include providing all the necessary hardware, operating systems, internet bandwidth, engineers, and support personnel necessary to establish and maintain Customer e-commerce websites or online computer applications.

Types of services provided to Provdotnet's customers:

- Physically Secure and Environmentally Conditioned Space in a Multi-tenant/ Colocation facility for customers to house their Network Switching, Data Storage and Data Processing Equipment
- Critical Power and HVAC in an N+1 format that utilizes Multiple HVAC units, Uninterruptable Power Supplies (UPS) and back-up generators to ensure maximum uptime for customer equipment
- Native (Unsecured) Internet Access Services

B. DESCRIPTION OF SERVICES PROVIDED

Multiple Space Configurations:

The Provdotnet colocation facilities accommodate multiple space configurations. Customer configurations can be as small as "1U", limited to 1/4 or 1/2 cabinets or multiple full cabinets. Provdotnet can also provide roof and smoke-stack rights for customers to mount transmission antennae and equipment.

Carrier-neutral Network Services:

Provdotnet provides access to a number of tier 1 telecommunication carriers, including: AT&T, Verizon, Cox Communications, (formerly Abovenet), Cogent, Lightower, Fibertech and Towerstream.

Secure Access and Surveillance:

The Provdotnet colocation facilities are fully alarmed and video monitored on a 24x7x52 basis. To access the facilities, every person must provide a photo or sufficient visual identification. Provdotnet maintains an active access permissions list identifying personnel approved by each customer who may enter the facility and an electronic detailed log of all visits. A facility-wide video surveillance system is in use which is digitally recorded and stored.

Managed Services Provided

Managed IP Network:

Provdotnet provides fully managed high availability IP "blended" bandwidth using Border Gateway Protocol (BGP) to allow for fully decentralized routing.

C. PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Provdotnet designs its processes and procedures related to its Colocation and Managed Services System to meet its objectives for providing data center solutions to its clients. Those objectives are based on the service commitments that Provdotnet makes to user entities, the laws and regulations that govern the provision of its services, and the financial, operational, and compliance requirements that Provdotnet has established for the services.

Service commitments to user entities are documented and communicated in a Service Level Agreement ("SLA") (inclusive of attachments and product order forms) as well as in the description of the service offering provided online. Service commitments are generally standardized and include, but are not limited to:

- Provdotnet will provide redundant power and bandwidth for managed services;
- Provdotnet will maintain systems without affecting customer services except for pre-approved planned maintenance;
- Provdotnet availability commitments include:
    - Mean Time to Repair/Restore ("MTTR") – four (4) hours per incident
    - Availability: 99.95%
    - Mean Time to Respond: one (1) hour
- Credit provisions should availability of services due to power outage or bandwidth interruption;
- Customer option to terminate contract if SLA is not met for two (2) consecutive months; and
- Confidentiality provisions regarding proprietary technical and business information of both Provdotnet and its customers.

System requirements for user entities are documented and communicated in a Service Level Agreement ("SLA") (inclusive of attachments and product order forms).

In achieving its service commitments and system requirements, Provdotnet has implemented various controls to ensure Security and Availability; such as:

- Physical access controls to the data centers;
- Monitoring of bandwidth in and out of the data center; and
- Incident response program designed to minimize the impact of incidents and protect resources.

Provdotnet establishes operational requirements that support the achievement of service commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Provdotnet's system policies and procedures, system design documentation, and contracts with customers. 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 are hired and trained.

D. COMPONENTS OF THE SYSTEM

As defined by DC 200, a *system* consists of five (5) key components organized to achieve a specified objective. The five components are categorized as follows:

- *Infrastructure*. The physical hardware components of a system (facilities, equipment, and networks)
- *Software*. The programs and operating software of a system (systems, applications, and utilities)
- *People*. The personnel involved in the operation and use of a system (developers, operators, users and managers)
- *Procedures*. The automated and manual procedures involved in the operation of a system
- *Data*. The information used and supported by a system (transaction streams, files, databases, and tables)

The Provdotnet Colocation and Managed Services System, using the above framework, is discussed below:

Infrastructure

The physical infrastructure provided by Provdotnet falls into four (4) categories; 1) secure physical sites and buildings consisting of three (3) leased facilities with secure physical access provided to all entrances. All Provdotnet's facilities are fully alarmed with fire and intrusion detection systems, twenty four (24) hour video surveillance systems, door access systems that use proximity bio-metric reader identity-access systems, all the facilities have dual-action dry-pipe sprinkler systems site and a FM200 fire suppression system, 2) the Critical Power infrastructure consists of Industrial Electrical Switch Equipment and Transfer Switches, Uninterruptable Power Supplies ("UPS"s) and backup generators. The critical power systems are used to ensure high availability and N+1 power for customer equipment, 3) Cooling Infrastructure, consisting of multiple units at each facility is also used to ensure high availability and N+1 cooling for customer equipment, and 4) Networking Equipment to ensure high availability and N+1 internet services for customer use.

Software

The Company has several applications in use, as described below:

- **QuickBooks Online – Accounting software system**. QuickBooks Online access is restricted via a username and password. The data is secured and backed up in the Intuit data center.
- **Office 365 with applications –** The Company uses Microsoft Office 365 for its secure email system.
- **Paessler PRTG –** Network monitoring software to watch over network devices and server.
- **CrashPlan by Code 42 –** Online backup software for file based backups to a secure encrypted data center. Access to CrashPlan is protected by a username and password.
- **Axis Camera Station –** Video Surveillance software to monitor and record via cameras.
- **VMWare Hypervisor Software –** Provdotnet's internal servers are hosted on four (4) VMWare host machines running ESXi.
- **StanleyPac –** Access Control software to control authenticated user access to the facility located at the service organization's at Providence, RI headquarters.
- **Bosch EZ Controller –** Access Control software to control authenticated user access to the facility located at the service organization's ancillary Providence location.
- **Zendesk –** Ticketing System & Change Management software that allows Provdotnet employees to enter service requests and change management requests.
- **Junos Pulse –** SLL VPN Client Software that allows secure remote access to the data centers when authorized users are outside the main office.
- **DSX Door Access System –** Access Control software to control authenticated user access to the data center located in Chelmsford, MA.

People

Provdotnet's organization is designed around process ownership and the RACI model ("responsible-accountable-consulted-informed"). Key personnel have overall process ownership responsibility for all processes related to their area of responsibility. However, the RACI model enables all personnel to play different roles depending upon the circumstance and core competencies. Formal policies and standards, which are reviewed regularly, are in place and include: Information Security/Physical Access, System Implementation for new/modifications to Customer Services, Changes to Infrastructure, and Customer Incident Response and Help Desk. Policies and Standards are reviewed by Provdotnet and updated where needed.

Personnel within the Provdotnet organization are as follows:

Key Roles in & Process Ownership

General Manager/Managing Partner

The General Manager/Managing Partner ("GM") is responsible for setting the strategic direction of Provdotnet. Primary responsibilities include:

- Business development;
- Regulatory management and the management of various strategic initiatives;
- Oversight of all business and technical operations relating to the daily operations of Provdotnet data center(s); and
- Project supervision to ensure strict adherence to operating/business policies.

Director of Operations and Financial Controls

- Responsible for the management of Accounting and Financial Controls;
- Responsible for the oversight and performance of ongoing maintenance of all data center systems, including but not limited to the following: critical infrastructure, real estate, vendor relations and access systems;
- Responsible for managing all customer related issues or problems as well as providing oversight and management of all change activity;
- Reports to the GM; and
- Undergoes annual meeting to evaluate competency.

Chief Technology Officer

The Chief Technology Officer ("CTO") reports to the General Manager/Managing Partner and is responsible for the design, engineering and maintenance of Provdotnet's internal systems as well as technical solutions for specific customer requirements. Undergoes annual meeting to evaluate competency.

Director of Marketing and Business Development

The Director of Marketing and Business Development reports to the GM and is responsible for creating strategies to generate business for Provdotnet. These range from SEO strategies to other marketing initiatives. Responsible for developing relationships with new and existing clients to determine their needs and price out solutions. Undergoes annual meeting to evaluate competency.

Provdotnet Contractor Support Staff

Reports directly to the CTO. Responsible for undertaking day to day operational tasks needed to advance objectives set by the other members of the organization. The Support Staff are trained by the Director of Operations to adhere to the protocols of the organization.

Advisory Board (Non-operating)

The Advisory Board consists of individuals who consult with the General Manager/Managing Partner, and whose goal is to support the continued development of Provdotnet's business operations in order to meet the expanding needs of new and existing customers.

Provdotnet's Advisory Board performs a non-operating governance role on behalf of Provdotnet's stakeholders. The Advisory Board provides both technical and business advice to the General Manager/Managing Partner on strategic aspects of Provdotnet's business. The Advisory Board participates in all capital expenditure discussions, technical architecture, partnerships and strategic operations.

Procedures

Management has developed and communicated, to internal and external users, procedures to provide businesses with highly secure, reliable and interconnected facilities for their infrastructure and service delivery platforms. These procedures cover the following key Security and Availability commitments:

- Selection, documentation and implementation of security controls
- Performance of annual assessments of security controls
- Authorization, changes to, and termination of physical and logical system access
- Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system
- Incident response
- Monitoring of critical power for continuous availability
- 2N+1 power design on all system levels (Utility, UPS, PDU's and rack distribution)
- Environmental monitoring

Data

Data as defined by Provdotnet, constitutes the following:

- Access reporting of physical locations
- Critical power monitoring reports
- Environmental asset status reports
- Bandwidth use reports
- Incident management reports

E. BOUNDARIES OF THE SYSTEM

The boundaries of Provdotnet's system are restricted to and by Services and Service Level targets delivered to customers. Provdotnet provides environmentally sound, secure high availability infrastructure facilities customers to host (co-locate) their computing, networking and data storage equipment within Provdotnet's purpose-built physically secure and high availability facilities.

Provdotnet does not provide any computing, data storage or application security services and does not have access to customer data, other than monitoring-related metrics. As such, the boundaries of the Provdotnet system are restricted to systems outlined within the *Infrastructure* description in Section **D. COMPONENTS OF THE SYSTEM**.

F. RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION SYSTEMS, MONITORING AND CONTROL ACTIVITIES

Control Environment

Management Philosophy

Provdotnet's control environment reflects the philosophy of Senior Management concerning the importance of providing its customers with highly secure, reliable and interconnected facilities for their IT infrastructure and service delivery platforms. Provdotnet's key management meets periodically to evaluate and address the ongoing business risks associated with meeting those commitments. The importance of providing secure and available service is emphasized through the establishment and communication of policies and procedures and is supported by investment in resources and people to carry out its commitments. In designing its controls, Provdotnet has taken into consideration the relevance of controls to meet the relevant trust services criteria.

Policies & Standards

Formal IT Policies and Standards are in place, including: Information Security/Physical Access, System Implementation for new/modifications to Customer Services, Changes Infrastructure, Customer Incident Response and Help Desk, and are distributed to Provdotnet employees. IT Policies and Standards are reviewed by Provdotnet Management on an annual basis and updated, where needed.

Customer Contracts & Agreements

Standard Contracts and Agreements are in place between Provdotnet and its Customers which define the colocation services and maintenance performed. Contracts and Agreements cover Customer specific metrics, including: overall availability, Mean Time Between Failures ("MTBF"), Mean Time to Recovery (MTTR), data center power, temperature, humidity and access control.

Physical Security

Provdotnet's colocation facilities resides in buildings owned by Steeltex Corporation, Toro Properties and Altid Properties, respectively. Provdotnet maintains fifteen (15) year lease agreements with all three (3): Steeltex Corporation for its colocation space, which is located on the first floor of the building; the colocation space with Toro Properties is located on the 1st and 2nd floor and Altid Properties is in a discrete unit in a single story building. The entrances required for escorted access to Provdotnet's colocation facility is staffed by Provdotnet representatives who are stationed at the (lobby) entrance to the building. The entrances required for unescorted access to Provdotnet's colocation facility are controlled by biometric fingerprint readers located at the entrances to the respective buildings.

Physical Access to Colocation Facility

Access to the Provdotnet colocation hosting facilities are controlled by the following mechanisms:

- Access to the main entrance to the Provdotnet colocation facility is controlled by proximity fobs. Additionally, there is key access which is restricted to the Executive Management of Provdotnet.
- Proximity fobs and biometrics are used to restrict access within the colocation facility, with proximity fobs required for escorted access and proximity fobs and biometrics required for unescorted access.

- Additional doors with secured access via mechanical keypads, lockbox/keys are utilized to restrict and control access to private Customer suites.
- Access to other non-Customer areas within the colocation facility are controlled by proximity fobs, biometric readers as well as padlocks. This includes power and utility equipment.
- Building keys for the main entrance to the colocation facility are issued to individuals per authorization of management as part of the hiring process, and a list of who maintains these keys is kept by management.

Physical Access to Customer Areas

Physical access to dedicated colocation facility customer areas is limited to authorized individuals, including employees, contractors and vendors of Provdotnet. Individual customer equipment is physically secured in a locked data center, and dedicated equipment cabinets and/or cages are available to customers (upon request to Provdotnet) in order to further restrict access to customer equipment.

Visitor Access to Colocation Facility

To enter Provdotnet's main lobby, visitors are required to ring the bell and announce themselves to Provdotnet personnel prior to being granted access to the main reception area. The main lobby acts as a man trap to restrict access to the main colocation hosting facility.

Once within the main lobby, visitors are required to sign in, noting their company, arrival time, purpose of their visit, and are required to present a photo ID at the security desk in the reception area. Visitors must be escorted by authorized Provdotnet personnel to their destination and are supervised at all times by Provdotnet personnel.

Authorizing Access to Customer Equipment

Access to Customer equipment must adhere to the following guidelines:

- Equipment, information and/or software cannot be taken offsite without prior authorization from the Customer.
- A formal release form (authorized by Customer management) is required to gain physical access to Customer areas.
- Once access is authorized by the Customer, all access to Customer areas by non-Provdotnet personnel is supervised by Provdotnet employees.
- Customer access requests are sent from pre-authorized Customer representatives via email to Provdotnet's Facilities Manager or General Manager/Managing Partner who will enable access.

Termination of Physical Access for Customers

Customer's physical security deactivation requests are sent from pre-authorized Customer representatives via email to the Provdotnet Facilities Manager, who will then disable or delete access rights within the physical access control system. Provdotnet maintains access and termination requests on their Customer Management System.

Monitoring of Physical Access:

The Provdotnet colocation facility is monitored by security cameras located at various points throughout the building colocation hosting facility. The video feeds are accessible remotely over the web. Real time (live) monitoring of camera coverage is performed by Provdotnet employee personnel. Video media history is maintained for a minimum period of sixty (60) days.

Provdotnet personnel also performs daily walkthroughs of the colocation facilities during the work week, as well as ongoing monitoring of video surveillance throughout each day and/ or when escorted access is being provided.

Review of Physical Access

Security system access logs are generated and maintained electronically by the security system software and are reviewed by the Provdotnet General Manager for unauthorized access attempts or unusual activity as follows:

- Access to the colocation facility (per incident both daily and weekly); and
- Individual door access is reviewed by the Facilities Manager weekly and/or as needed.

In addition to the security logs, each alarm activation and deactivation creates an email alert that is reviewed and maintained by Provdotnet.

Intruder Alarm System

An intruder alarm system is in place that is managed and monitored by a central alarm monitoring company (Electronic Alarms Systems, Inc.). Colocation facility building doors and entrance points are alarmed, and motion detectors are present at critical locations in the building and customer equipment areas alert the central monitoring station.

Power Redundancy

The Provdotnet colocation facilities are equipped with electrical systems that provide N+1 redundancy configurations. Power is provided to the Customer racks and/or cabinets via multiple separate Power Distribution Units ("PDU"s).

Telecommunications Data & Voice Redundancy

There are multiple fiber links to the colocation facility and redundant data circuits are in place to re-route data traffic in the event of a failure to a primary circuit.

In the event of a commercial power failure, redundant Uninterruptible Power Supply ("UPS") units are in place. UPS systems can receive power from both commercial power feeds and standby generators, and are designed to provide power to a fully loaded colocation hosting facility until power can be transferred to the on-site diesel generators.

Backup Power Generator

In the event of a commercial power failure, respective onsite 250, 350, 400, and 1000 KVA diesel generators exist to provide power to the colocation hosting facility. Upon detection of a power outage, automatic switchover from commercial power to the standby generator is handled by a transfer switch and the UPS system - to ensure that there are no disruptions to customer equipment. A multi-day supply (approximately eight-ten (8-10) days under full load) of diesel fuel is securely stored on-site and is backed by guaranteed fuel delivery by local fuel suppliers.

Maintenance & Testing of Power Redundant Systems

Semi-annual maintenance (including annual load testing) is performed on both the UPS units as well as the diesel generator to ensure functionality by the Facilities Manager. The diesel generators are also exercised weekly.

Fire Suppression & Detection

An air sampling smoke detection system and conventional fire detection devices are in place within the colocation hosting facilities. The colocation hosting facilities are also equipped with a dry pipe - pre-action fire suppression system.

Climate Control

The colocation hosting facilities are equipped with Computer Room Air Conditioning ("CRAC") units to meet N+1 redundancy requirements. The colocation hosting facility aims to provide air conditioning to maintain the cold aisle temperature at 73 +/- 5 degrees Fahrenheit with 35% +/- 5% humidity. Maintenance is performed on CRAC units at least on an annual basis by an outside contractor.

Environmental Monitoring

Monitoring sensors are configured to automatically notify a third party and Provdotnet technicians via email alerts, and audible and visual alarm, should any adverse temperature and/or humidity conditions occur outside of the configured range.

The building's environmental conditions (i.e., climate control components) are monitored utilizing APC and Liebert environmental monitoring systems which are configured to automatically notify Provdotnet technicians via email and/or text message should adverse conditions arise.

Water Detection Devices

Water detection devices are located in the colocation facilities to alert Provdotnet Management via email in the event of a potential flood condition occurring.

Help Desk System

The Zendesk system and/or Help and System Support Desk Associates record, track, monitor and resolve all Customer related incidents by priority (i.e., High, Medium or Low), per customer contracts and agreements. This is performed in one of two ways: (1) either customer problems are submitted through the customer support portal, automatically creating problem tickets within Provdotnet's Help Desk system; or, (2) customers call the Help Desk support line generating a notification to a Provdotnet Help Desk and System Support Desk Associate, who in turn completes a Help Desk ticket within Provdotnet's Help Desk system.

Alerts generated by internal monitoring systems are reviewed and managed by Provdotnet Help Desk and System Support Desk Associate personnel. They set up tickets on the Help Desk System based on their Assessment of the alerts generated.

Performance Monitoring

Open Source Security Information Management (PRTG Monitoring) is used by Provdotnet, and is a collection of tools designed to aid network administrators in incident management, computer security, intrusion detection and prevention.

The internal network is monitored using PRTG Monitoring for server health, uptime, performance, resource issues, bandwidth and disk. Alerts generated by the systems are forwarded through the Help Desk to a Provdotnet Help and System Support Desk Associate for review and follow-up.

Remote Hands Services

Provdotnet offers "Remote Hands Services" in their colocation hosting facility for their Customers. Remote Hands Services includes basic on-site first-line maintenance and support, but may be expanded to include more advanced services on an individual case-by-case basis. These services include:

- Visual inspection of devices to assess equipment status;
- Rebooting routers, servers or other Customer equipment - where the Customer provides written directions for the Provdotnet technician; and
- Disconnecting systems from the network in the event of a network security event.

Only pre-authorized Provdotnet Customer representatives can request and approve Remote Hands Services. Remote Hands Services are performed by the Provdotnet Help and System Support Desk Associate under the direction of the Customer.

Remote Access

Pulse VPN is used to provide secure access to remote PCs and Servers for end-user support from other locations.

Customer Support

If a Help and System Support Desk Associate is unable to perform Remote Hands Service requests immediately, the Customer will be notified and the services will be scheduled to be performed once the Associate becomes available. Remote Hands Service requests are queued and monitored for timely response.

Intrusion Detection System

Intrusion Detection Systems are in place to detect and report unusual activity on the network. Alerts are sent out to a designated Provdotnet Help and System Support Desk Associate for any significant threats detected. Issues requiring remediation are logged in the Help Desk System for follow-up and review.

Cable & Wire Management

Cables and wires connected to computer equipment and peripherals within the colocation facility are placed out of the way of normal traffic. The cabling is located within a conduit routed above the floor.

Logical Security

Firewall & Routers

Provdotnet's internal networks are protected by a failover cluster of Juniper Networks SSG320M firewalls and Intrusion Detection Devices which serve to protect our core network. Routing is handled by redundant Cisco ASR edge routers paired with high availability enabled Cisco 6509 routing cores. These provide for proper redundancy and automated failover for the connections to our internal network.

Provdotnet Facilities Management technical staff is responsible for managing and maintaining firewalls and routers protecting colocation hosting facilities from external attacks. User authentication, via a user ID and password, is required prior to gaining access to perform changes to network configurations. Changes to the firewall are maintained and auto-logged in the firewall management system. Provdotnet has a policy whereby the change is documented in the Help Desk system and a copy of the configuration file (prior to the change) is archived.

Change Management

Minor Infrastructure Changes

Minor infrastructure changes are documented via a Ticket in the Help Desk System and require formal authorization from the General Manager and Managing Partner. The Ticket includes concurrence (i.e., the authorization) from the Customer and Provdotnet operations, and a description of the change.

Major Infrastructure Changes

Major infrastructure changes are documented via a ticket in the Help Desk System and require formal authorization and approval from the General Manager and Managing Partner. The Ticket includes concurrence (i.e., the authorization) from the Customer and Provdotnet operations, and includes a detailed description of the change, back out plans, evidence of testing, post-implementation approval, and evidence that the change was properly made.

Other Considerations

Provdotnet maintains business loss and liability insurance coverage.

Risk Assessment

Provdotnet Management and supervisory personnel regularly review the risks that may threaten the achievement of criteria for the Security and Availability principles set forth in *TSP 100, Trust Services Principles and Criteria for Security, Availability Processing Integrity, Confidentiality and Privacy (AICPA, Trust Services Principles and Criteria).* Key members of Management assess risks surrounding Security and Availability on an ongoing basis through regular readiness assessment meetings, where actual and perceived vulnerabilities are addressed and remediated, as necessary.

Monitoring

Provdotnet Management and supervisory personnel monitor the quality of internal control performance via frequent observance, interaction and performance of their assigned duties. Reporting of any deficiencies noted from ongoing monitoring of processes and procedures, are communicated to the relevant management personnel.

Provdotnet's activities are subject to review by the Management team. The Management team evaluates compliance with policy and regulations, and the Board of Directors is consulted as to both strategic, operational issues and technical issues at least once per quarter.

Information and Communication

Changes that impact customers, employees and stakeholders are communicated through formal correspondence and electronic press/email releases issued by the Company. Provdotnet holds an annual training session to communicate and reinforce the adherence of organizational procedures and policies as provided in the annual operations control document and the potential consequences of non-adherence. Also, Provdotnet regularly assesses and addresses their readiness and ability to deliver on their commitments of Security and Availability, by holding periodic meetings to ensure all systems are operating effectively and all corrective measures occur in a timely manner. Customer complaints/requests are managed through an automated ticket system and followed through to completion.

Control Activities

Control activities are part of the process by which Provdotnet achieves its business objectives. Provdotnet has applied a risk management approach to the organization in order to select and develop control activities.

Provdotnet’s control objectives and related control activities included in Section V, “Description of Controls” of this report are designed to eliminate the redundancy that would result from listing the items in this section and repeating them in Section V. Although the control criteria and related control activities are included in Section IV, they are, nevertheless, an integral part of Provdotnet’s system description.

G. SUBSERVICE ORGANIZATIONS

Provdotnet uses the following subservice organizations in the delivery of its Colocation and Managed Services System to its customers:

Code42 Software, Inc. – Provdotnet utilizes Code42 Software, Inc. for cloud-based endpoint data security and recovery services.

Zendesk – Zendesk is a cloud-based software as a service provider for client help desk ticket support.

Intuit, Inc. – Provdotnet utilizes Intuit, Inc. (QuickBooks Online) for accounting software services including the manual processing of credit card transactions

Microsoft Office 365 – Provdotnet utilizes Microsoft (Office 365) for office productivity, email and document management services.

Provdotnet's subservice organizations are outside of the scope of this examination and report. The TSP criteria impacted by the subservice organizations, either in totality or in conjunction with Provdotnet Advantage Suite™ controls are listed in the chart on the following pages.

Where available, Provdotnet, LLC regularly receives Service Organization Control ("SOC") reports for these organizations and reviews the impact of these reports on its overall internal control environment in addition to other vendor management procedures.

The TSP criteria impacted by the subservice organizations, either in totality or in conjunction with Provdotnet's controls, are listed in the chart on the following pages:

TSP Criteria	Description	Code42 Software, Inc.	Zendesk	Intuit, Inc.	Microsoft Office 365
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	X	X	X	X
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	X	X	X	X
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	X	X	X	X
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	X	X	X	X
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	X	X	X	X
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	X	X	X	X
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	X	X	X	X

Subservice Organization Complementary Controls

Provdotnet obtains and reviews the annual Service Organization Control ("SOC") examinations of those entities that undergo SOC examinations. In addition, as part of its Risk Management process, Provdotnet performs a comprehensive vendor management review of each of its subservice organizations to assess their capabilities to address the Provdotnet business needs and its requirements for Security and Availability.

The subservice organizations are expected to have the following complementary controls in providing services to Provdotnet:

Code42 Software, Inc., Zendesk, Intuit, Inc., Microsoft Office 365

As cloud solution providers, these vendors are expected to have industry standard, best practice controls governing the following aspects of their operations:

- Logical access controls into its environment,
- Physical access controls over the infrastructure interfacing with Provdotnet,
- Monitoring controls over their respective environments, including intrusion detection and inspection (as applicable) and network performance controls,
- Disaster recovery policies and procedures, and
- Other policies governing operations.

H. COMPLIMENTARY USER ENTITY CONTROL CONSIDERATIONS

In order for Provdotnet Customer's to benefit from the controls described in this report, Customer's must determine whether the following controls are in place and functioning. Furthermore, the following list of controls addresses only those controls relating to Provdotnet's Colocation and Managed Services. This list is not intended to be a complete listing of the controls that provide a basis for the assertions underlying Provdotnet's Colocation and Managed Services.

Provdotnet customers, through their agreements with Provdotnet, have selected unique levels of services, and therefore, not all Customer user control considerations may apply to each Customer user organization.

Colocation and managed services customers are expected to establish the following controls and ensure they are operating effectively. (These controls are intended to cover any and all customer provided equipment, including but not limited to: UPS, fans, other mechanical and electrical equipment, and computer and networking systems):

1. Customer user organizations are responsible for understanding and complying with their contractual obligations to Provdotnet and monitoring adherence to Contracts and Agreements maintained with Provdotnet.

2. Customer user organizations are responsible for managing and controlling logical access to their systems.

3. Customer user organizations are responsible for determining whether Provdotnet's security infrastructure is appropriate for its needs and for notifying Provdotnet of requested modifications.

4. Customer user organizations are responsible for adhering to Provdotnet's security procedures and informing their affected vendors and/or subcontractors of their related responsibilities.

5. Where customer user organizations provide their own or leased equipment, user organizations are responsible for ensuring their own equipment and resident data is secured, including physical precautions such as locked cabinets. Provdotnet assumes security only for Provdotnet systems, information and equipment.

6. Customer user organizations have the option of providing their own UPS equipment, if not contracted through Provdotnet for use of its UPS equipment. When stated in the Contract, Customer user organizations are responsible to maintain the appropriate type and level of insurance to cover damage and/or loss of their own equipment, software and data.

7. Customer User organizations are responsible for informing Provdotnet in a timely manner of any security, confidentiality and regulatory requirements, which include, but are not limited to: HIPAA/HITECH and Payment Card Industry (PCI) standards which may affect the services provided by Provdotnet. Customer user organizations are responsible to promptly notify Provdotnet of changes made to technical or administrative contact information.

8. Customer user organizations are responsible for maintaining and providing Provdotnet with an updated list of authorized personnel, vendors and contractors.

9. Customer user organizations are responsible to promptly notify Provdotnet in writing to remove terminated employees who are authorized to either direct service changes or to anyone with access to Provdotnet colocation facilities.

10. Customer user organizations are responsible for ensuring that only authorized individuals have knowledge of their designated personal identification credentials, authentication questions, and all other information with an assigned account.

11. Customer user organizations are responsible for maintaining their own system(s) of record.

12. Customer user organizations are responsible for developing their own business continuity and disaster recovery plans that address their inability to access or utilize Provdotnet.

13. Customer user organizations are responsible for ensuring the security and integrity of any data or information in storage and/or transmitted via their service or over the Internet (e.g., encryption controls). Provdotnet does not maintain access customer data.

14. Customer user organizations are responsible for ensuring that adequate mechanisms are in place to monitor and protect information passing through their network. Customer user organizations are responsible for using their own series of firewalls and routers to provide additional protection.

15. Customer user organizations are responsible for developing policies and procedures to protect their systems from unauthorized or unintentional use, modification, addition or deletion.

16. Customer user organizations are responsible for creating and communicating specific escalation procedures to Provdotnet for problems to their network hosts and services, and are responsible for notifying Provdotnet of any changes to escalation procedures in a timely manner.

17. Customer user organizations are responsible for implementing their own access and password controls for their infrastructure and ensuring the confidentiality of any user IDs and passwords. Provdotnet does not maintain access to customer user organization infrastructure.

18. Customer user organizations are responsible for ensuring that the impact of scheduled maintenance activities to their production processes and jobs is sufficiently mitigated.

19. Customer user organizations are responsible for notifying or denying requested infrastructure configuration changes in a timely manner.

20. Customer user organizations are responsible for notifying Provdotnet of suspected or actual network or service problems in a timely manner.

21. Outside of contracted monitoring services of Customer user organizations are responsible for implementing monitoring controls to detect and alert the customer user organization of known and/or suspected security breaches or other incidents (e.g., power failure) affecting service(s), or supporting infrastructure either provided by Provdotnet or the Customer user organization. If a security breach and/or incident occur, the Customer user organization is responsible for communicating such events to the appropriate personnel in a timely manner.

I. TRUST SERVICES CRITERIA AND RELATED CONTROLS

Although the trust services criteria and related controls are presented in Section V, "Description of Controls", they are an integral part of the Provdotnet system description.

J. CHANGES TO THE SYSTEM DURING THE PERIOD

There were no changes that are likely to affect report users' understanding of how the Colocation and Managed Services System is used to provide the service as of June 30, 2020.

V. DESCRIPTION OF CONTROLS

A. PURPOSE AND OBJECTIVES OF THE INDEPENDENT AUDITORS' EXAMINATION

This report on controls placed in operation is intended to provide interested parties with sufficient information regarding the security and control structure of Provdotnet's services and to provide information about the effectiveness of the design of controls. This report, when combined with an understanding of the controls at user organizations, is intended to permit an evaluation of the internal controls surrounding the security of Provdotnet's systems and may potentially reduce user organization auditors' assessed level of control risk below the maximum for certain management assertions.

This report, when coupled with an understanding of the controls in place at user entities of Provdotnet, is intended to assist in the assessment of the total internal control surrounding user entity applications.

This report has been prepared in accordance with the requirements and guidance established in AT-C section 105, *Concepts Common to All Attestation Engagements* and AT-C Section 205, *Examination Engagements* and in accordance with guidance from the AICPA for the performance and reporting on Service Organization Control ("SOC") reports, "*Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy"* ("SOC 2 Reports").

It is each interested party's responsibility to evaluate this information in relation to the controls in place to obtain an overall understanding of the internal controls and assess control risk. The portions of the controls provided by the user entities and Provdotnet must be evaluated together. If effective user entity controls are not in place, Provdotnet controls may not compensate for such weaknesses.

Our examination included discussions with appropriate management, supervisory, and staff personnel, and inspection of documents and records relative to the Trust Services Security and Availability principles and criteria.

Provdotnet's description of controls is the responsibility of Provdotnet management. Our responsibility is to express an opinion that the controls are in place to provide reasonable, but not absolute, assurance that the controls specified by Provdotnet were adequate in their design as of the report date.

B. APPLICABLE TRUST SERVICES CRITERIA RELEVANT TO SECURITY

Control Environment	
CC1.1	***The entity demonstrates a commitment to integrity and ethical values.***
TSC Reference Number	**Controls Provided by Provdotnet, LLC**
CC1.1.1	Management monitors personnel compliance with the code of conduct through processes that are covered in the annual operations overview and control document. The sanctions policy is applied to personnel who violate the code of conduct.
CC1.1.2	Personnel are required to read and accept the code of conduct and practices upon their hire and to formally reaffirm them annually thereafter.
CC1.1.3	Agreements are established with third parties or subcontractors that include clearly defined terms, conditions, and responsibilities for third parties and subcontractors.
CC1.1.4	Prior to employment, new hires are verified against regulatory screening databases and/or are sanctioned by owner/family member.

CC1.2	***The Board of Directors demonstrates independence from management and exercises oversight of the development and performance of internal control.***
TSC Control Criteria	**Controls Provided by Provdotnet, LLC**
CC1.2.1	The board of directors identifies and accepts its oversight responsibilities in relation to established requirements and expectations.
CC1.2.2	The board of directors defines, maintains, and periodically evaluates the skills and expertise needed among its members to enable them to ask probing questions of senior management and take commensurate action.
CC1.2.3	The board of directors has sufficient members who are independent from management and objective in evaluations and decision making.

CC1.3	***Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.***
TSC Control Criteria	**Controls Provided by Provdotnet, LLC**
CC1.3.1	Provdotnet has an organizational chart and job descriptions in place to ensure that the Company has assigned responsibility, accountability and reporting lines for system Security and Availability. The entity evaluates its organizational structure, reporting lines, authorities, and responsibilities as part of its yearly operational review and as part of its ongoing risk assessment and management process. The entity revises these when necessary to help meet changing commitments and system requirements.
CC1.3.2	Roles and accountability are defined through formal job descriptions. Roles and responsibilities are defined in written job descriptions and communicated to managers and their supervisors.
CC1.3.3	Provdotnet, LLC management and the Board of Directors evaluate its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process and as part of its ongoing risk assessment and management process and revise these when necessary to support the achievement of objectives.
CC1.3.4	Provdotnet, LLC has an appropriate organizational structure based on functional departments, with an executive leader heading each department.

CC1.4	***The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.***
TSC Control Criteria	**Controls Provided by Provdotnet, LLC**
CC1.4.1	Job requirements are documented in the job descriptions, and candidates' abilities to meet these requirements are evaluated as part of the hiring and annual performance review. During its ongoing and periodic business planning and budgeting process, Management evaluates the need for additional tools and resources in order to achieve its business objectives.
CC1.4.2	Management establishes requisite skill sets for personnel and provides continued training about its commitments and requirements for personnel.
CC1.4.3	During its ongoing and periodic business planning and budgeting process, Management evaluates the need for additional tools and resources in order to achieve its business objectives.

CC1.5	***The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.***
TSC Control Criteria	**Controls Provided by Provdotnet, LLC**
CC1.5.1	Roles and responsibilities are defined in written job descriptions. Job descriptions are reviewed on a periodic basis for needed changes and updated if such changes are identified. Candidates' abilities to meet these requirements are evaluated as part of the hiring and annual performance review.

Communication and Information	
CC2.1	***The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.***
TSC Control Criteria	**Controls Provided by Provdotnet, LLC**
CC2.1.1	On a weekly basis, senior management meets to discuss and document operational procedures and their impact on achieving the Security and Availability commitments of Provdotnet.
CC2.1.2	Provdotnet communicates to its staff the policies and procedures regarding the design and operation of the system and its boundaries to permit them to understand their role in the system. These policies and procedures are available to staff via an online document repository for them to access at any time.
CC2.1.3	The boundaries of the systems have been defined and included in the network diagram which is available to all employees (and customers, if requested).
CC2.1.4	The building's environmental conditions (i.e., climate control components) are monitored utilizing APC and Liebert environmental monitoring systems which are configured to automatically notify Provdotnet technicians via email and/or text message should adverse conditions arise.
CC2.1.5	The internal network is monitored using PRTG Monitoring for server health, uptime, performance, resource issues, bandwidth and disk. Alerts generated by the systems are forwarded through the Help Desk to a Provdotnet Help and System Support Desk Associate for review and follow-up.
CC2.1.6	The network firewall incorporates IDS/IPS, Antivirus, Web Filtering and Malware detection utilities to monitor external access attempts to the Provdotnet environment.

CC2.2	***The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.***
TSC Control Criteria	**Controls Provided by Provdotnet, LLC**
CC2.2.1	Provdotnet communicates to its staff the policies and procedures regarding the design and operation of the system and its boundaries to permit them to understand their role in the system. These policies and procedures are available to staff via an online document repository for them to access at any time.
CC2.2.2	Provdotnet has written job descriptions specifying the responsibilities and requirements for key job positions, specifically for personnel responsible for the design, development, implementation, and operation of systems affecting the Security and Availability of services.
CC2.2.3	Security awareness training related to Security and Availability is performed annually for all employees including new hires.
CC2.2.4	Provdotnet communicates policies which address system Security and Availability as well as employee responsibilities during the onboarding process of new employees through the employee Operations Runbook and initial orientation training.
CC2.2.5	Provdotnet communicates to its staff the procedures for identifying and reporting Security and Availability issues, potential breaches and other related incidents in accordance with its Incident Response Policy. The security awareness training and Incident Response Policy includes information concerning the identification of issues and the point of contact in the event of a breach.

CC2.3	***The entity communicates with external parties regarding matters affecting the functioning of internal control.***
TSC Control Criteria	**Controls Provided by Provdotnet, LLC**
CC2.3.1	Vendors and third parties with restricted access that engage in business with Provdotnet are subject to confidentiality commitments as part of their agreements with Provdotnet. The agreements communicate information regarding the responsibilities of critical vendors/contractors through Vendor Agreements/Contracts.
CC2.3.2	Provdotnet completes a Vendor Assessment Questionnaire for each of its vendors to assess the internal controls that are in place for each vendor.
CC2.3.3	Provdotnet communicates to its customers its service commitments related to Security and Availability in an executed Service Agreement which includes provisions on both parties' responsibility over the security and confidentiality of information.
CC2.3.4	Provdotnet provides publicly available mechanisms for external parties to contact Provdotnet to report security events and publishes information including a system description and security and compliance information addressing Provdotnet commitments and responsibilities.

Risk Assessment	
CC3.1	***The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.***
TSC Control Criteria	**Controls Provided by Provdotnet, LLC**
CC3.1.1	The Provdotnet Board of Directors regularly meets to review and define company objectives relative to choice of structure, industry trends and the performance of Provdotnet.
CC3.1.2	The Board of Directors establish objectives that reflect the desired level of operations and financial performance.
CC3.1.3	Management establishes objectives consistent with laws and regulations or standards and frameworks consistent with its managed hosting operations.
CC3.1.4	Provdotnet integrates applicable federal, state and local laws into its compliance objectives.
CC3.1.5	Provdotnet maintains a formal risk assessment process to govern its operations and performs a risk assessment continuously.

CC3.2	***The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.***
TSC Control Criteria	**Controls Provided by Provdotnet, LLC**
CC3.2.1	Provdotnet has developed system security measures that help to identify threats that may arise, including threats from vendors and third parties.
CC3.2.2	Provdotnet has defined and implemented a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.
CC3.2.3	During the risk assessment and management process, risk management personnel identify changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives. In response to the identification of such risks, Management updates its policies, procedures, processes and controls, as needed.
CC3.2.4	The Risk and Controls group's recommendations are reviewed and approved by senior management. An owner is assigned for each remediation plan in risk assessments.

CC3.3	***The entity considers the potential for fraud in assessing risks to the achievement of objectives.***
TSC Control Criteria	**Controls Provided by Provdotnet, LLC**
CC3.3.1	Provdotnet has a Vendor Risk Management policy that has developed system security measures that help to identify threats that may arise, including threats from vendors and third parties. Provdotnet completes a Vendor Assessment Questionnaire for each of its vendors to assess the threats that might be present with each vendor.
CC3.3.2	During the risk assessment and management process, risk management personnel identify changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives. In response to the identification of such risks, Management updates its policies, procedures, processes and controls, as needed.
CC3.3.3	The entity has defined and implemented a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.
CC3.3.4	The Risk and Controls group's recommendations are reviewed and approved by senior management. An owner is assigned for each remediation plan in risk assessments.

CC3.4	***The entity identifies and assesses changes that could significantly impact the system of internal control.***
TSC Control Criteria	**Controls Provided by Provdotnet, LLC**
CC3.4.1	Provdotnet's risk management processes considers changes to the regulatory, economic, and physical environment in which it operates.
CC3.4.2	Provdotnet's risk management process considers the potential impacts of new or changes to existing business lines, changes in relationships with vendors and the introduction of new technologies.

Monitoring Activities	
CC4.1	***The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.***
TSC Control Criteria	**Controls Provided by Provdotnet, LLC**
CC4.1.1	Provdotnet has a formal Hardware and Infrastructure Monitoring Standards policy that delineates various hardening standards and comprehensive monitoring processes for security of the data centers.
CC4.1.2	Monitoring sensors are configured to automatically notify a third party and Provdotnet technicians via email alerts, and audible and visual alarm, should any adverse temperature and/or humidity conditions occur outside of the configured range.
CC4.1.3	Provdotnet utilizes PRTG as its Data Center Infrastructure Management ("DCIM") tool which continuously monitors all environmental elements and customer traffic in the data centers.
CC4.1.4	Provdotnet personnel perform daily walkthroughs of the colocation facilities during the work week, as well as ongoing monitoring of video surveillance throughout each day and/ or when escorted access is being provided.

CC4.2	***The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the Board of Directors, as appropriate.***
TSC Control Criteria	**Controls Provided by Provdotnet, LLC**
CC4.2.1	Provdotnet has an Incident response program designed to minimize the impact of incidents and protect resources.
CC4.2.2	Data Center Management review weekly events/issues impacting operations and develop corrective actions, as appropriate, to address these items.
CC4.2.3	The Board of Directors evaluates internal control deficiencies in a timely manner as appropriate.
CC4.2.4	Monitoring sensors are configured to automatically notify a third party and Provdotnet technicians via email alerts, and audible and visual alarm, should any adverse temperature and/or humidity conditions occur outside of the configured range.

Control Activities	
CC5.1	***The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.***
TSC Control Criteria	**Controls Provided by Provdotnet, LLC**
CC5.1.1	Provdotnet develops control activities to mitigate risks identified in its Risk Assessment based upon the environment, complexity, nature, and scope of its operations.
CC5.1.2	Control activities are developed to mitigate the risks associated with physical access to the data center and achievement of objectives relative to the service commitments of Provdotnet to its customers.

CC5.2	***The entity also selects and develops general control activities over technology to support the achievement of objectives.***
TSC Control Criteria	**Controls Provided by Provdotnet, LLC**
CC5.2.1	The Provdotnet Hardware and Infrastructure Monitoring Standards policy sets forth control activities relevant to the infrastructure and security monitoring processes over the data center environments.
CC5.2.2	Provdotnet has a formal disaster recovery plan that sets forth operational procedures to implement in the event of a disaster affecting Provdotnet at any or all of Provdotnet's operating locations.

CC5.3	***The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.***
TSC Control Criteria	**Controls Provided by Provdotnet, LLC**
CC5.3.1	Provdotnet management establishes control activities through policies and procedures that establish expectations and relevant day-to-day operational processes. These policies and procedures include: • Change Management • Annual Operations and Control • Incident Response • Hardware and Infrastructure Hardening and Monitoring • Disaster Recovery • Operations Runbook
CC5.3.2	Provdotnet management has assigned responsibility and accountability for control activities with the Director of Financial and Data Center Operations.
CC5.3.3	Provdotnet management annually evaluates the competency of personnel assigned with responsibility and accountability for control activities.
CC5.3.4	Policies and procedures governing control activities are reviewed annually to determine their continued relevance and are updated as business operations warrant.

Logical and Physical Access Controls	
CC6.1	***The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.***
TSC Control Criteria	**Controls Provided by Provdotnet, LLC**
CC6.1.1	Established entity standards exist for infrastructure and software hardening and configuration that include requirements for implementation of access control software, entity process standards and standardized access control lists.
CC6.1.2	System scans are performed for infrastructure elements to identify variance from entity standards. Intrusion detection systems are in place to detect and report unusual activity in the system. Alerts are sent out to Help and System Support Desk associates, issues requiring remediation are logged in the help desk system for follow-up and review.
CC6.1.3	Only internal users can access the system remotely through the use of the VPN, secure sockets layer ("SSL"), or other encrypted communication system.
CC6.1.4	Password complexity standards are established to enforce control over access control software passwords.
CC6.1.5	Administrative accounts are set up, as needed, and the user administration function is segregated for managing privileged accounts**.**

CC6.2	***Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.***
TSC Control Criteria	**Controls Provided by Provdotnet, LLC**
CC6.2.1	Entity standards are established for infrastructure and software hardening and configuration that include requirements for implementation of access control software, entity process standards, and standardized access control lists.
CC6.2.2	Accounts and access controls are delineated by user roles and access to other systems is restricted without management notifications and approval.
CC6.2.3	Only internal users can access the system remotely through the use of the VPN, secure sockets layer (“SSL”), or other encrypted communication system.
CC6.2.4	Password complexity standards are established to enforce control over access control software passwords.
CC6.2.5	Administrative accounts are set up, as needed, and the user administration function is segregated for managing privileged accounts**.**

CC6.3	***The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity’s objectives.***
TSC Control Criteria	**Controls Provided by Provdotnet, LLC**
CC6.3.1	When possible, formal role-based access controls to limit access to the system and infrastructure components are created and enforced by the access control system.
CC6.3.2	User access requests for a specific role are approved by the user's manager and submitted for approval to the appropriate operation director/owner according to the change management process. Segregation of duties exists between individuals who request access, authorize access, grant access, and review access.
CC6.3.3	Roles are reviewed and updated by both asset owners and the Risk and Controls group on an annual basis. Access change requests resulting from the review are submitted to the security group via a change request record.

CC6.4	***The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.***
TSC Control Criteria	**Controls Provided by Provdotnet, LLC**
CC6.4.1	An access control system has been implemented within the perimeter of facilities and at the entry and exit points of sensitive areas within these facilities. The access control system includes a combination of fob and fingerprint readers as well as secured cages and cabinets.
CC6.4.2	Guests to the facility are required to sign in and show a form of identification. They are also escorted at all times throughout the facility.
CC6.4.3	Access cards are created during the workforce member orientation period and distributed after all required background investigations are completed. Access cards initially provide access only to areas that fall within one's responsibilities.
CC6.4.4	Access to sensitive areas is controlled through the fob and biometric reader systems. Requests for access must be approved by the owner of the sensitive area. Requests for access and changes to access are made, approved, and communicated through the change management record system.

CC6.5	***The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.***
TSC Control Criteria	**Controls Provided by Provdotnet, LLC**
CC6.5.1	An access control system has been implemented within the perimeter of facilities and at the entry and exit points of sensitive areas within these facilities. The access control system includes a combination of fob and fingerprint readers as well as secured cages and cabinets.
CC6.5.2	Guests to the facility are required to sign in and show a form of identification. They are also escorted at all times throughout the facility.
CC6.5.3	Access cards are created during the workforce member orientation period and distributed after all required background investigations are completed. Access cards initially provide access only to areas that fall within one's responsibilities.
CC6.5.4	Access to sensitive areas is controlled through the fob and biometric reader systems. Requests for access must be approved by the owner of the sensitive area. Requests for access and changes to access are made, approved, and communicated through the change management record system.
CC6.5.5	Logical access to system resources is removed upon an individual's separation from the Company.

CC6.6	***The entity implements logical access security measures to protect against threats from sources outside its system boundaries.***
TSC Control Criteria	**Controls Provided by Provdotnet, LLC**
CC6.6.1	Defined entity standards exist for infrastructure and software hardening and configuration that include requirements for implementation of access control software, entity configuration standards, and standardized access control lists that define which privileges are attributable to each user or system account.
CC6.6.2	External points of connectivity to the entity's internal network are protected by a firewall complex, network segmentation, and several layers of defense to prevent unauthorized external users from gaining access to the organization's internal systems and devices.
CC6.6.3	Firewall hardening standards are based on relevant applicable technical specifications that are compared against product and industry recommended practices and updated as required by business needs.
CC6.6.4	External access to nonpublic sites is restricted through the use of user authentication and message encryption systems such as VPN and SSL.

CC6.7	***The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.***
TSC Control Criteria	**Controls Provided by Provdotnet, LLC**
CC6.7.1	VPN, SSL, secure file transfer program ("SFTP"), or other encryption technologies are used for defined points of connectivity and to protect communications between the processing center and users connecting to the processing center from within or external to the entity's internal networks.
CC6.7.2	Entity policies prohibit the transmission of sensitive information over the Internet or other public communications paths (for example, email) unless it is encrypted.
CC6.7.3	Backup media are encrypted during creation.

CC6.8	***The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.***
TSC Control Criteria	**Controls Provided by Provdotnet, LLC**
CC6.8.1	Intrusion detection systems are in place to detect and report unusual activity on the network.
CC6.8.2	Anti-virus software is installed on workstations, laptops, and servers supporting such software. The anti-virus program covers any piece of hardware that may be accessing the network, both internally and externally.
CC6.8.3	Anti-virus software is configured to receive an updated virus signature.

System Operations	
CC7.1	***To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.***
TSC Control Criteria	**Controls Provided by Provdotnet, LLC**
CC7.1.1	Defined entity standards exist for infrastructure and software hardening and configuration that include requirements for implementation of access control software, entity configuration standards, and standardized access control lists that define which privileges are attributable to each user or system account.
CC7.1.2	The entity monitors infrastructure and software for noncompliance with the standards, which could threaten the achievement of the entity's objectives.
CC7.1.3	Procedures are in place to detect the introduction of unknown or unauthorized components.
CC7.1.4	The network firewall incorporates IDS/IPS, Antivirus, Web Filtering and Malware detection utilities to monitor external access attempts to the Provdotnet environment.

CC7.2	***The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.***
TSC Control Criteria	**Controls Provided by Provdotnet, LLC**
CC7.2.1	Monitoring software is used to collect data from system infrastructure components and endpoint systems; to monitor system performance, potential security threats and vulnerabilities, and resource utilization; and to detect unusual system activity or service requests.
CC7.2.2	Requests for support, which may include requests for remote hands or customer access, go through the change management process where either an email or ticket is logged for recording purposes. All personnel follow defined protocols for recording, resolving, and escalating received requests.
CC7.2.3	The network firewall incorporates IDS/IPS, Antivirus, Web Filtering and Malware detection utilities to monitor external access attempts to the Provdotnet environment.
CC7.2.4	Data center operation personnel implement documented counter measures strategies when vulnerabilities are detected.
CC7.2.5	Updates/backups are performed using an automated system on internal systems.

CC7.3	***The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.***
TSC Control Criteria	**Controls Provided by Provdotnet, LLC**
CC7.3.1	Operations personnel follow defined protocols for evaluating reported system events that may indicate a breach or other related incident. Security related events are assigned to an appropriate party for evaluation.
CC7.3.2	Operations and security personnel follow defined protocols for resolving and escalating reported events. This includes root cause analysis that is escalated to Management as required.
CC7.3.3	Internal and external users are informed of incidents in a timely manner and advised of any corrective measures to be taken on their part.
CC7.3.4	Change management requests are opened for events that require permanent fixes.

CC7.4	***The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.***
TSC Control Criteria	**Controls Provided by Provdotnet, LLC**
CC7.4.1	Operations personnel follow defined protocols for evaluating reported system events that may indicate a breach or other related incident. Security related events are assigned to an appropriate party for evaluation.
CC7.4.2	Operations and security personnel follow defined protocols for resolving and escalating reported events. This includes root cause analysis that is escalated to Management as required.
CC7.4.3	Internal and external users are informed of incidents in a timely manner and advised of any corrective measures to be taken on their part.
CC7.4.4	Change management requests are opened for events that require permanent fixes.

CC7.5	***The entity identifies, develops, and implements activities to recover from identified security incidents.***
TSC Control Criteria	**Controls Provided by Provdotnet, LLC**
CC7.5.1	Operations personnel follow defined protocols for evaluating reported system events that may indicate a breach or other related incident. Security related events are assigned to an appropriate party for evaluation.
CC7.5.2	Operations and security personnel follow defined protocols for resolving and escalating reported events. This includes root cause analysis that is escalated to Management as required.
CC7.5.3	Internal and external users are informed of incidents in a timely manner and advised of any corrective measures to be taken on their part.
CC7.5.4	Change management requests are opened for events that require permanent fixes.

Change Management	
CC8.1	***The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.***
TSC Control Criteria	**Controls Provided by Provdotnet, LLC**
CC8.1.1	System changes, other than those classified as minor, require dual approval before implementing.
CC8.1.2	During the ongoing risk assessment process and the periodic planning and budgeting processes, infrastructure, data, software, and procedures are evaluated for needed changes. Change requests are created based on the identified needs.
CC8.1.3	For high severity incidents, a root cause analysis is prepared and reviewed by operations management. Based on the root cause analysis, change requests are prepared and the entity's risk management process and relevant risk management data is updated to reflect the planned incident and problem resolution.
CC8.1.4	A process exists to manage emergency changes.
CC8.1.5	Service related system change requests must be reviewed and approved by both the CEO and a managing partner prior to work commencing on the requested change. Separate personnel are responsible to authorize changes and to implement the changes.
CC8.1.6	Functional and detailed designs are prepared for other than minor changes. Functional and detailed designs must be approved by both the CEO and a managing partner prior to work commencing on the development project.
CC8.1.7	Established entity standards exist for infrastructure and software hardening and configuration that include requirements for implementation of access control software, entity configuration standards, and standardized access control lists.
CC8.1.8	A turnover process that includes verification of operation and back out steps is used for every migration.
CC8.1.9	Post implementation procedures that are designed to verify the operation of system changes are performed for a defined period, as determined during project planning, after the implementation for other than minor changes, and results are shared with internal and external users and customers as required to meet commitments and system requirements.
CC8.1.10	The change management process has defined the following roles and assignments: • Authorization of change requests - owner or business unit manager • Development - application design and support • Testing - quality assurance • Implementation

Risk Mitigation	
CC9.1	***The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.***
TSC Control Criteria	**Controls Provided by Provdotnet, LLC**
CC9.1.1	Provdotnet has formal Disaster Recovery and Incident Response Plans developed to respond to, mitigate, and recover from security events that disrupt business operations.
CC9.1.2	The Risk Management Team meets regularly to review the Cumulative Risk Register and to discuss other items that may impact Provdotnet's risk management objectives.

CC9.2	***The entity assesses and manages risks associated with vendors and business partners.***
TSC Control Criteria	**Controls Provided by Provdotnet, LLC**
CC9.2.1	Provdotnet establishes specific requirements for a vendor and business partner engagement that includes (1) scope of services and product specifications, (2) roles and responsibilities, (3) compliance requirements, and (4) service levels.
CC9.2.2	Provdotnet assesses, on a periodic basis, the risks that vendors and business partners (and those entities' vendors and business partners) represent to the achievement of the entity's objectives.
CC9.2.3	Provdotnet has assigned responsibility and accountability for the management of risks associated with vendors and business partners to the Director of Operations and Finance.

C. APPLICABLE TRUST SERVICES CRITERIA RELEVANT TO AVAILABILITY

Additional Criteria for Availability	
A1.1	***The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.***
TSC Control Criteria	**Controls Provided by Provdotnet, LLC**
A1.1.1	Processing capacity is monitored on an ongoing basis in accordance with SLAs, key performance indicators ("KPI"s), and other performance related parameters.
A1.1.2	Critical infrastructure components have been reviewed for criticality classification and assignment of a minimum level of redundancy.
A1.1.3	Future processing demand is forecasted and compared to scheduled capacity on an ongoing basis. Forecasts are reviewed and approved by Senior Operations Management. Change requests are initiated as needed based on approved forecasts.
A1.1.4	Environmental protections receive testing/maintenance on at least an annual basis.
A1.1.5	Weekly/bi-weekly tests are performed on necessary systems using an automated system to ensure reliability.
A1.1.6	Business continuity and disaster recovery plans have been developed, updated, and tested annually.

A1.2	***The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.***
TSC Control Criteria	**Controls Provided by Provdotnet, LLC**
A1.2.1	As part of the risk assessment process, Provdotnet identifies environmental threats that could impair the availability of the system, including threats resulting from adverse weather, failure of environmental control systems, electrical discharge, fire, and water.
A1.2.2	Detection measures are implemented to identify anomalies that could result from environmental threat events.
A1.2.3	Provdotnet has implemented environmental protection mechanisms including fire and water suppression systems, temperature and humidity controls, uninterruptable power system and generator backup and video security systems to prevent and mitigate against environmental events.
A1.2.4	Data Center monitoring occurs continuously with alerts generated to Provdotnet operations personnel when environmental conditions register events outside of normal operations thresholds.
A1.2.5	Procedures are in place for responding to environmental threat events which includes automatic mitigation systems (uninterruptable power systems and generator back-up subsystem).
A1.2.6	The Provdotnet Disaster Recovery plan sets forth measures for migrating processing to an alternate infrastructure in the event normal processing infrastructure becomes unavailable.

A1.3	***The entity tests recovery plan procedures supporting system recovery to meet its objectives.***
TSC Control Criteria	**Controls Provided by Provdotnet, LLC**
A1.3.1	Provdotnet has a formal disaster recovery plan that sets forth operational procedures to implement in the event of a disaster affecting Provdotnet at any or all of Provdotnet's operating locations.
A1.3.2	Business continuity and disaster recovery plans, including restoration of backups, and emergency notification systems are tested annually.
A1.3.3	Test results are reviewed and the contingency plan is adjusted, as necessary.