Netelligent Hosting Services, Inc.

Service Organization Controls 2 (AT101), Type 2

DESCRIPTION OF SYSTEM, SUITABILITY OF DESIGN AND OPERATING EFFECTIVENESS FOR THE

DATA CENTRE COLOCATION SERVICES SYSTEM
RELEVANT TO SECURITY AND AVAILABILITY

For the Period January 1, 2016 through December 31, 2016

TABLE OF CONTENTS

SECTION 1: INDEPENDENT SERVICE AUDITORS' REPORT

Auditwerx
3000 Bayport Drive
Suite 500
Tampa, FL 33607
866.446.4038 office
727.499.6867 fax
AUDITWERX.COM

INDEPENDENT SERVICE AUDITORS' REPORT

To the Management of Management of Netelligent Hosting Services, Inc.:

We have examined the description in Section 3 titled "Description of Netelligent Hosting Services, Inc.'s Data Centre Colocation Services System" ("description") based on the criteria set forth in paragraph 1.26 of the AICPA Guide, *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (description criteria) and the suitability of the design and operating effectiveness of controls described therein to meet the criteria for the security and availability principles set forth in *TSP Section 100, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* throughout the period January 1, 2016 to December 31, 2016.

As indicated in the description, Netelligent Hosting Services, Inc. ("Netelligent" or the "Company") uses a service organization to perform third-party security-monitoring for denial-of-service-attack (DDoS) network attacks. In addition, Netelligent uses a third party data center service to store offsite backups for disaster recovery procedures. The backup power generator and cold water supply systems used by Netelligent to provide data centre colocation services at the 800 Square Victoria facilities are provided by the building management firm. The description indicates that certain applicable trust services criteria can be met only if certain types of controls that management expects to be implemented at the subservice organization are suitably designed and operating effectively.

The description presents Netelligent's system; its controls relevant to the applicable trust services criteria; and the types of controls that the service organization expects to be implemented, suitably designed, and operating effectively at the subservice organization to meet certain applicable trust services criteria. The description does not include any of the controls expected to be implemented at the subservice organization. Our examination did not extend to the services provided by the subservice organization, and we have not evaluated whether the controls management expects to be implemented at the subservice organization have been implemented or whether such controls were suitability designed and operating effectively throughout the period January 1, 2016 to December 31, 2016.

Netelligent's Responsibilities

In Section 2, Netelligent has provided its assertion titled "Netelligent Hosting Services, Inc. Assertion" about the fairness of the presentation of the description based on the description criteria and suitability of the design and operating effectiveness of the controls described therein to

meet the applicable trust services criteria. Netelligent is 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; identifying the risks that would prevent the applicable trust services criteria from being met; designing, implementing, and documenting the controls to meet the applicable trust services criteria; and specifying the controls that meet the applicable trust services criteria and stating them in the description.

Auditwerx's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria and on the suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included procedures that we considered necessary in the circumstances. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is fairly presented based on the description criteria, and the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period January 1, 2016 to December 31, 2016.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria involves—

- evaluating and performing procedures to obtain evidence about whether the description is fairly presented based on the description criteria, and the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period January 1, 2016 to December 31, 2016.
- assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively.
- testing the operating effectiveness of those controls to provide reasonable assurance that the applicable trust services criteria were met.
- evaluating the overall presentation of the description, the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization in its assertion.

We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.

Opinion

In our opinion, in all material respects, based on the description criteria identified in Netelligent's assertion and the applicable trust services criteria—

a. the description fairly presents the system that was designed and implemented throughout the period January 1, 2016 to December 31, 2016.

b. the controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period January 1, 2016 to December 31, 2016, and the subservice organization applied the types of controls expected to be implemented at the subservice organization throughout the period January 1, 2016 to December 31, 2016.

c. the controls tested operated effectively to provide reasonable assurance that the applicable trust services criteria were met throughout the period January 1, 2016 to December 31, 2016 if the controls expected to be implemented at the subservice organization were also operating effectively throughout the period January 1, 2016 to December 31, 2016.

Restricted Use

This report, including the description of tests of controls and results thereof in Section III, is intended solely for the information and use of Netelligent; user entities of Netelligent's data centre colocation services system during some or all of the period January 1, 2016 to December 31, 2016; and prospective user entities, independent auditors, and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, subservice organizations, and other parties.
- Internal control and its limitations.

- The nature of user entity controls and responsibilities, and their role in the user entities internal control as they relate to, and how they interact with, related controls at the service organization to meet the applicable trust services criteria.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the applicable trust services criteria 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.

Auditwerx, LLC, a Division of Carr, Riggs & Ingram Capital, LLC
Tampa, Florida

March 3, 2017

SECTION 2: NETELLIGENT HOSTING SERVICES, INC'S ASSERTION

NETELLIGENT HOSTING SERVICES, INC'S ASSERTION

We have prepared the description titled "Description of Netelligent's Data Centre Colocation Services System" (the "description") throughout the period January 1, 2016 to December 31, 2016, based on the criteria for a description of a service organization's system identified in *paragraphs 1.26 of the AICPA Guide, Reporting on Controls at a Service Organization: Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (description criteria). The description is intended to provide users with information about the data centre colocation services system, particularly system controls intended to meet the criteria for the security and availability principle(s) set forth in *TSP 100, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services principles), throughout the period January 1, 2016 to December 31, 2016. We confirm, to the best of our knowledge and belief, that:

1) The description fairly presents the data centre colocation services system throughout the period January 1, 2016 to December 31, 2016. Our assertion is based on the following description criteria:

    a. The description contains the following information:

        i. The types of services provided.

        ii. The components of the system used to provide the services, which are as follows:

            - *Infrastructure.* The physical structures, IT and other hardware (for example, facilities, computers, equipment, mobile devices, and telecommunications networks).
            - *Software.* The application programs and IT system software that supports application programs (operating systems, middleware, and utilities).
            - *People.* The personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).
            - *Processes.* The automated and manual procedures.
            - *Data.* Transaction streams, files, databases, tables, and output used or processed by a system.

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

        iv. For information provided to, or received from, subservice organizations, and other parties—

            - how the information is provided or received and the role of the subservice organizations and other parties.

- the procedures the service organization performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.

v. The applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, the following:

- Complementary user entity controls contemplated in the design of the service organization's system.
- When the inclusive method is used to present a subservice organization, controls at the subservice organization.

vi. If the service organization presents the subservice organization using the carve-out method—

- the nature of the services provided by the subservice organization.
- each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria.

vii. Any applicable trust services criteria that are not addressed by a control and the reasons.

viii. In the case of a Type 2 report, relevant details of changes to the service organization's system during the period covered by the description.

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

2) The controls stated in the description were suitably designed throughout the period January 1, 2016 to December 31, 2016 to meet the applicable trust services criteria.

3) The controls stated in the description operated effectively throughout the period January 1, 2016 to December 31, 2016 to meet the applicable trust services criteria.

By: /S/ Mohamed Salamé

Mohamed Salamé
President and Co-Founder
March 3, 2017

SECTION 3: DESCRIPTION OF NETELLIGENT HOSTING SERVICES INC.'S DATA CENTRE COLOCATION SERVICES SYSTEM

DESCRIPTION OF NETELLIGENT HOSTING SERVICES, INC.'S DATA CENTRE COLOCATION SERVICES SYSTEM

COMPANY OVERVIEW

Netelligent Hosting Services, Inc. ("Netelligent" or the "Company") is located in Montreal, Quebec, Canada and was incorporated in 2002 in the Province of Quebec, Canada. Netelligent employs approximately 30 employees.

PRODUCTS AND SERVICES OVERVIEW

Netelligent is a data center that offers secure colocation in Montreal QC, Canada. Their services vary from single-server colocation to private-cabinets or full-cage enclosures.

SYSTEM DESCRIPTION

The following system description includes the relevant components that comprise the colocation system relating to infrastructure, software, people, procedures and data.

The "System" refers to all aspects of Netelligent relating to:

- Infrastructure
- Physical premises
- Colocation services
- Power - Main utility feed, backup UPS, and Generators
- Cooling - Chillers, CRACs, Pumps, Precision cooling (XDP/XDV)
- *Prime:* Customer and Infrastructure Database
- *Protégé:* Access card reader software
- *Kayako:* Issue tracking and ticketing software
- *OpenNMS and Cacti:* Network monitoring software

Infrastructure

The colocation data centre space is located within the Netelligent suite at 800 Square Victoria in Montreal's downtown district. All access to the data centre and corporate offices is restricted to only authorized staff and customers through the use of an access card reader system. The entire data centre space and adjoining security areas are monitored by surveillance cameras with image retention. Floor to ceiling perimeter walls prevent the possibility of climb over. Cooling is provided through a combination of multiple cabinet mounted high density modular cooling systems and computer room air conditioning (CRAC) units. The building is connected to a high priority utility power grid. Backup power is provided through the use of uninterruptable power supplies (UPS) and a backup generator. The network core is comprised of a multi-carrier, redundant, and meshed

configuration allowing for no single points of failure. Netelligent is a vendor-neutral data centre served by several fiber uplinks through multiple providers. These uplinks follow diversified physical paths into the facility for added redundancy.

Software

Netelligent utilizes a combination of Windows and Unix based operating systems for the various applications used in support of colocation services. Applications used in the environment include network authentication, Virtual Private Networking (VPN), issue tracking and ticketing, project management, network monitoring, Domain Name Service (DNS), and backup. Netelligent also develops its own proprietary customer relationship, inventory, and invoicing database called Prime. The Prime application also includes a web based portal front-end for internet access by authorized users over an encrypted connection.

People and Responsibilities

The following describes the personnel involved in the operation and use of the Netelligent data centre colocation services system. They are grouped under two main categories, Internal Users and External Users.

Internal Users

Vice President (VP) Technology – The VP Technology is responsible for the day to day management and administration of the information technology (IT) department in support of data centre colocation services.

Director IT – Establishes the provisioning and configuration of key server hardware and software infrastructure often working closely with Support Technicians and Network Administrators.

Facilities Manager – Oversees the Support department, site security, and the Security Council.

Support Manager & Support Technicians – The Support department is responsible for validating authorized users and answering or escalating support requests.

Security Attendants – Responsible for physical site security and security awareness and training.

Security Council – The Security Council consist of the Facilities Manager, VP Technology, Director IT, and Special Projects Manager. The Security Council is responsible for the Company risk assessments, policy administration and the review, planning, implementation and audit of compliancy requirements.

Special Projects Manager – Responsible for monitoring systems and is the Abuse Response Team Lead.

Network Administrators – Responsible for core network administration and support of the infrastructure.

VP Sales – Responsible for the Sales and Marketing Team as well as billing and collections.

VP Finance – Responsible for accounts receivable and bookkeeping.

External Users

Customers – Are considered the end users and have limited site access and limited portal and support access.

Contractors – Provide maintenance and expansion to the facility. They must have an authorized open support ticket or email from management for physical access. They have no portal or support access.

Visitors – No site access unless signed-in and accompanied by an authorized user. Visitors are not granted portal access. Visitors typically consist of customer technicians and their assistants, auditors, and prospective customers.

Procedures

Netelligent has documented procedures for various aspects of data centre colocation services. The automated and manual procedures involved in the operation of the system include:

- Data centre security
- Account Creation and Cancellation
- Access Card Provisioning and Blocking
- Server Removal Authorization
- Access for Visitors and Contractors
- Authenticating Support Requests
- System Monitoring
- Emergency Response Procedures
- Risk Assessment
- Change Management

Data

Limited amounts of customers' personal data are stored on Netelligent corporate servers. Security information is considered the most sensitive information and is stored in the Prime application database.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT, INFORMATION AND COMMUNICATION, CONTROL ACTIVITIES, AND MONITORING

CONTROL ENVIRONMENT

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. The control environment has a pervasive influence on the way business activities are structured, objectives are established, and risks are assessed. It influences control activities, information and communication systems, and monitoring procedures. The control environment is influenced by an entity's history and managerial culture. Effectively controlled entities strive to have competent people, instill an enterprise-wide attitude of integrity and control consciousness, and set a positive corporate direction. These entities establish appropriate controls that foster shared values and teamwork in pursuit of the organization's objectives.

Management's philosophy and operating style affect the way the entity is managed, including the kinds of business risks accepted. Netelligent places a great deal of importance on working to help ensure that the integrity of processing is a primary focus and that controls are maximized to mitigate risk in the daily operations. Management and specific teams are structured to help ensure the highest level of integrity and efficiency.

Netelligent desires to maintain a safe, pleasant, and cooperative working environment and expects employees to have high standards of performance, integrity, productivity, and professionalism. Netelligent has developed professional conduct policies that set forth policies of particular importance to all employees, relating to ethics, values, and conduct. All employees are expected to know and adhere to these standards, as well as to generally accepted norms of conduct and courtesy at all times. While managers are responsible for understanding, communicating, and enforcing Company policies, this does not override or diminish an employee's individual responsibility to be aware of and adhere to these policies.

RISK ASSESSMENT

Team leaders are required to identify significant risks related to their areas of responsibility and implement measures to mitigate those risks. The management team and the Security Council meet regularly to identify any risks and develop corrective steps to minimize the impact of these risks. The Company employs numerous methods to assess and manage risk, including policies, procedures, team structure, recurring meetings, and automated error detection controls. The Company strives to identify and prevent risks at an early stage through policy and procedure adherence in addition to mitigating relevant risks as discovered either through team structure, meetings, or notifications.

Netelligent maintains security policies and communicates them to staff to ensure that all individuals utilizing Company resources understand their responsibility in reducing the risk of compromise and exercise appropriate security measures to protect systems and data.

INFORMATION AND COMMUNICATION

Netelligent uses a variety of methods for communication to ensure that significant events and issues are conveyed in a timely manner and that staff understand their role and responsibility over service and controls. These methods include the following: new hire training, ongoing training, policy and process updates, departmental meetings summarizing events and changes, use of email to communicate time sensitive information, and the documentation and storage of historical data in internal repositories for business and support activities. The Company maintains systems that manage the flow of information and facilitate communication with its customers.

Netelligent has implemented various methods of communication to help ensure that employees understand their individual roles and responsibilities over processing and controls and communicate significant events in a timely manner. Employee manuals are provided upon hire that communicate all relevant policies and procedures concerning employee conduct. Security of the physical premises and logical security of systems is reinforced by training and through awareness programs. The communication system between senior management and operations staff includes the use of the office email system, written memos when appropriate, and weekly meetings. Periodic department meetings between each manager and their staff are held to discuss new Company policies and procedures and other business issues. Periodic staff and training meetings are utilized to inform staff of new policy and technology updates. Communication is encouraged at all levels to promote the operating efficiency of Netelligent.

CONTROL ACTIVITIES

The Company's trust services criteria and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing them here in Section 3 and repeating them in Section 4. Although the trust services criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of Company's description of controls.

MONITORING

Management monitors internal controls as part of normal business operations. Netelligent uses a series of management reports and processes to monitor the results of the various business processes. The management team regularly reviews the reports, and all exceptions to normal processing activities are logged, reported, and resolved.

The Company monitors the colocation environment and components for capacity, performance, and hardware failure. Overall system health and capacity planning are monitored daily to ensure infrastructure system will meet the needs of the Company's clients.

SUBSERVICE ORGANIZATION(S)

From partnership with the building management firm The Petra Group, Netelligent is able to maintain production systems at colocation data centre. The backup power generator and cold water supply systems used by Netelligent to provide data centre colocation services at the 800 Square Victoria facility, are provided by the building management firm The Petra Group.

Netelligent uses Staminus a cloud based DDoS and mitigation security solution vendor located in Newport Beach, California, to monitor for and mitigate the risk of DDoS attacks against the Netelligent network.

Netelligent uses Cologix as a third party data center service to store offsite backups for disaster recovery purposes. Cologix has a current SSAE 16 type 2 report.

TRUST SERVICES CRITERIA AND RELATED CONTROLS

The Company's trust services criteria and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing them here in Section 3 and repeating them in Section 4. Although the trust services criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of Company's description of controls.

USER CONTROL CONSIDERATIONS

The Company's applications are designed with the assumption that certain controls would be implemented by user organizations. In certain situations, the application of specific controls at the user organization is necessary to achieve control objectives included in this report.

This section describes additional controls that should be in operation at user organizations to complement the controls at Netelligent. User auditors should consider whether or not the following controls are implemented at user organizations:

- Controls to provide reasonable assurance that user organizations' ensure compliance with contractual requirements.
- Controls to provide reasonable assurance of the adherence to all published data centre security policies.
- Controls to provide reasonable assurance that user organizations adopt strong operating system and application password management procedures, including using passwords that cannot be easily compromised and are required to change on a regular basis.

- Controls to provide reasonable assurance that access to the Netelligent support websites is restricted to only authorized personnel and that user names and passwords are kept confidential.
- Controls to provide reasonable assurance that access lists to the Netelligent facility and support websites is periodically reviewed and maintained.
- Controls to provide reasonable assurance that the customer has procedures in place for developing, maintaining, and testing their own business continuity plans (BCP).

The list of user organization control considerations presented above and those presented with certain specified control objectives do not represent a comprehensive set of all the controls that should be employed by user organizations. Other controls may be required at user organizations. Providing colocation services for customers by the Company covers only a portion of the overall internal control structure of each customer. The Company services were not designed to be the only control component in the internal control environment. Additional control procedures are required to be implemented at the customer level. It is not feasible for all of the control objectives relating to colocation services to be completely achieved by the Company. Therefore, each customer's system of internal controls must be evaluated in conjunction with the internal control structure described in this report.