Hosting.com, Inc.

Service Auditor's Report on Hosting.com, Inc.'s Assertion of the Suitability of the Design and Operating Effectiveness of the System for Datacenter Services Relevant to Security, Availability, and Confidentiality Principles Comprising Trust Services Principles Section 100 ("SOC 3 Report")

For the Period August 1, 2014,
to December 31, 2014

Hosting.com, Inc.
SOC 3 Service Auditor's Report on
Security, Availability, and Confidentiality

Table of Contents Page No.

Independent Service Auditor's Report

To the Board of Directors of Hosting.com, Inc.:

We have examined management's assertion that during the period August 1, 2014, to December 31, 2014, Hosting.com ("the Company," "Hosting.com," or "Service Organization") maintained effective controls over the System for Datacenter Services in Irvine, California; Louisville, Kentucky; Newark, Delaware; San Francisco, California; Dallas, Texas; and Denver, Colorado, to provide reasonable assurance that:

- The hosting system was protected against unauthorized physical and logical access,
- The hosting system was available for operation and use as committed or agreed, and
- Information designated as confidential was protected by the system as committed or agreed

based on the criteria to meet the security, availability, and confidentiality principles set forth in TSP Section 100, *Trust Services Principles, Criteria, and Illustration of Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Technical Practice Aids). The Company's management is responsible for the assertion. Our responsibility is to express an opinion on the assertion based on our examination.

Hosting.com's management is responsible for this assertion. Our responsibility is to express an opinion based on our examination. Management's description of the aspects of the System for Datacenter Services covered by its assertion is attached.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants, and, accordingly, included (1) obtaining an understanding of Hosting.com's relevant controls over security, availability and confidentiality of the System for Datacenter Services; (2) testing and evaluating the operating effectiveness of the controls; and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

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 of 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.

Mountjoy Chilton Medley LLP
P 502.749.1900 | F 502.749.1930
2600 Meidinger Tower | 462 South Fourth Street | Louisville, KY 40202
www.mcmcpa.com | 888.587.1719
An Independent Member of Baker Tilly International

Independent Service Auditor's Report (Continued)

In our opinion, management's assertion referred to above is fairly stated, in all material respects, based on the applicable trust services criteria for security, availability, and confidentiality.

Louisville, Kentucky
February 9, 2015

Section II. Management of Hosting.com's Assertion Regarding Its System for Datacenter Services for the Period August 1, 2014, to December 31, 2014

The management of Hosting.com makes the following assertion pertaining to the System for Datacenter Services:

Hosting.com maintained effective controls over the System for Datacenter Services, during the period August 1, 2014, to December 31, 2014, in Irvine, California; Louisville, Kentucky; Newark, Delaware; San Francisco, California; Dallas, Texas; and Denver, Colorado, to provide reasonable assurance that:

- The system was protected against unauthorized physical and logical access,
- The system was available for operation and use as committed or agreed, and
- Information designated as confidential was protected by the system as committed or agreed

based on the criteria to meet the security, availability, and confidentiality principles set forth in TSP Section 100, *Trust Services Principles, Criteria, and Illustration of Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Technical Practice Aids).

The attached description identifies those aspects of the System for Datacenter Services covered by our assertion.

The Management of Hosting.com

Art Zeile
Chief Executive Officer

Joel Daly
Chief Operating Officer

Section III - Hosting.com, Inc.'s Description of System for Datacenter Services Provided by Hosting.com

A. Overview of the Organization

Hosting.com is a provider of enterprise class cloud computing, dedicated & colocated hosting, managed services, disaster recovery, business continuance services, and infrastructure as a service (IaaS) to a global customer base demanding a high level of security, reliability, and responsiveness. HOSTING monitors, manages, and enhances the Web-based platforms of software as a service (SaaS) providers, content distribution networks (CDN), and medium to large enterprises whose Web presence is crucial and high availability is mandatory.

HOSTING currently operates datacenters in Dallas, TX; Denver, CO; Irvine, CA; Louisville, KY; Newark, DE, and; San Francisco, CA.

HOSTING delivers:

- A National Platform with datacenters in Dallas, Denver, Irvine, Louisville, Newark and San Francisco with 24/7/365 operational support
- Scalable service platforms designed to grow with the customer's availability requirements such as Hosting, Business Continuance-Disaster Recovery, and Burst Capacity
- Highest levels of availability, recovery, security, and responsiveness

B. Datacenter Overview

HOSTING's datacenters are full-service, information management service centers constructed for enterprise business customers. The datacenters are designed to meet the demands of businesses seeking more economical and environmentally responsible ways to achieve optimal secure information technology management and scalable, redundant network connectivity for maximum availability.

In addition to the physical datacenter services, HOSTING provides business customers an integrated suite of information system services including wide area network connectivity via HOSTING's network or other telecommunications providers, managed infrastructure and information technology (IT) systems, colocation services, business continuity services for disaster recovery (BCDR), and unlimited application hosting for cloud, dedicated and colocated customers. HOSTING leverages a Tier 1 Internet backbone, with 2 or more fiber carriers per datacenter site as well as other telecommunications solutions.

A minimum datacenter environmental baseline is in place to provide controls sufficient to maintain the protection of computer equipment from physical security and environmental hazards.

B. Datacenter Overview (Continued)

These key datacenter elements may include: (see Section IV for description of elements and controls contained at each of the HOSTING datacenters):

- Redundant HVAC systems
- Redundant water chillers, condensers and/or air handlers
- Strategically placed water sensors
- Raised flooring
- Separate cooling zones
- Diesel generators sufficient to power entire facility
- A minimum forty-eight hour fuel supply, with vendors waiting on demand if needed
- Redundant UPS, PDU and transfer switches
- Regular testing and preventative maintenance of environment control systems
- Ceiling mounted smoke detectors
- Dry Pipe fire suppression systems
- Chemical fire extinguishers and gas suppression systems
- Global network operations center that monitors environmental systems and customer solutions for availability and performance
- 24/7/365 onsite server engineers who perform regular checks of critical data center facility systems
- Video surveillance equipment that records video footage
- Physical access control systems that operate on the principle of least privilege in order to limit access to secure areas

C. Managed Dedicated Hosting

HOSTING's Managed Dedicated Hosting solutions are custom-built to meet the specific needs of individual clients. These solutions are designed for mission-critical, web-based or back office enterprise application hosting.

As custom solutions, enterprise hosting environments typically include multiple layers of security systems, as well as advanced features such as load-balanced front-end web servers, clustered application and database servers. The objective of every custom configuration is to maximize application performance and availability while providing superior security and data protection in a cost effective manner.

Managed Dedicated Hosting solutions include

- Dedicated server hardware
- Redundant sources of electrical power
- Redundant sources of internet connectivity
- 24/7/365 technical support
- Redundant environmental systems

C. Managed Dedicated Hosting (Continued)

Additional services that can be contracted for Managed Dedicated Hosting solutions include:

- Managed backups
- Enterprise backups
- Scalable monitoring solutions
- Antivirus/Anti-Malware (Windows based servers)
- Operating system security patches (Windows and Linux)
- Firewall
- Virtual Private Networking (VPN)
- Two-Factor authentication
- File integrity monitoring (FIM)
- Centralized Log Management and Retention
- Intrusion detection systems (IDS)
- Vulnerability Scanning and Threat Management
- Critical availability Service (CAS)

D. Colocation Hosting

Colocation Hosting provides secure and redundant services for companies that choose to manage their IT systems but lack the budget or resources to build the necessary infrastructure. HOSTING's high-speed internet connectivity, secure datacenter facilities, redundant power and network systems and technical resources are provided to each colocation customer.

Colocation Hosting Services offer datacenters with:

- 24 hours a day, 7 days a week operations presence
- Receiving processes for customer equipment
- Secure storage and equipment-staging areas
- Secure, continuous environmental systems delivery

Additional services that can be contracted for Colocated Hosting solutions include:

- Scalable Monitoring Solutions
- Firewall
- Virtual Private Networking (VPN)
- Two-Factor Authentication
- File integrity monitoring (FIM)
- Intrusion Detection Systems (IDS)
- Vulnerability Scanning and Threat Management
- Centralized Log Management and Retention

E. Cloud Hosting

HOSTING offers several different cloud hosting options. Customers may choose to use HOSTING's Enterprise cloud offering which provides high availability utilizing advanced features in the virtualized environment on shared hardware infrastructure.

Cloud Enterprise solutions include:

- Windows or Linux virtual servers
- High availability utilizing features in VMWare's virtualization technology
  24/7/365 technical support

E. Cloud Hosting (Continued)

Additional services that can be contracted for Cloud Enterprise solutions include:

- Managed backups
- Enterprise backups
- Scalable monitoring solutions
- Antivirus/Anti-Malware (Windows based servers)
- Operating system security patches (Windows and Linux)
- Firewall
- Virtual Private Networking (VPN)
- Two-Factor authentication
- File Integrity Monitoring (FIM)
- Centralized Log Management and Retention
- Intrusion Detection Systems (IDS)
- Vulnerability Scanning and Threat Management
- Critical Availability Service (CAS)

Customers can also choose to have HOSTING create a virtualized environment on hardware that is dedicated specifically to them.

Dedicated cloud solutions include:

- Dedicated server hardware
- Windows or Linux virtual servers
- 24/7/365 technical support

Additional security and availability services that can be contracted for dedicated cloud solutions include:

- Scalable monitoring solutions
- Managed backups
- Enterprise backups
- Antivirus/Anti-Malware (Windows based servers)
- Operating system security patches (Windows and Linux)
- Firewall
- Virtual Private Networking (VPN)
- Two-Factor authentication
- File Integrity Monitoring (FIM)
- Centralized Log Management and Retention
- Intrusion Detection Systems (IDS)
- Vulnerability Scanning and Threat Management
- Critical Availability Service (CAS)

F. Backup of Programs and Data Files

HOSTING offers two levels of optional backup services to customers that provide the following options:

Features common to both backup services:

- Bare Metal/System State Restore of drives and partitions as directed by the customer for
  - Linux OS
  - Windows OS
- Partition level exclusions

F. Backup of Programs and Data Files (Continued)

Features common to both backup services (Continued):

- File by file restore
- Block Level Backup
- MS SQL Server & MySQL Server (Linux only)
- Standard backup retention 7 days
- Encryption configurable upon request.

Additional features of Enterprise backup:

- Adjustable Retention Policy (14 days is default)
- Offsite backup to another HOSTING Data Center
- Customer Premises backups (remote backup only)
- File level exclusions
- Global De-Duplication (Improves backup/restore times)
- Client Side De-Duplication (Improves backup/restore times)
- HOSTING Customer Portal Integration
- Download individual files from the Customer Portal
- Backup Replication
- MS SQL Server & MySQL Server
- NAS Backups
- VMware Hypervisor Layer Backups

G. Control Environment

A company's control environment reflects the overall attitude, awareness, and actions of executive management, and others concerning the importance of controls and the emphasis given to controls in the company's policies, procedures, methods, and organizational structure. The following is a description of the control environment components at HOSTING which focus on Security, Availability, and Confidentiality:

1. Management Controls: Management of HOSTING is responsible for directing and controlling operations and for establishing, communicating, and monitoring control policies and procedures. Importance is placed on maintaining sound internal controls and the integrity and ethical values of all HOSTING personnel. Organizational values and behavioral standards are communicated to all personnel through the Employee Handbook.

2. Organizational Structure: The organizational structure of HOSTING, which provides the overall framework for planning, directing, and controlling operations, uses an approach whereby personnel and business functions are divided into departments according to job responsibilities. This approach allows the organization to clearly define responsibilities, lines of reporting, and communications and allows employees to focus on the specific business issues affecting our customers.

   Up-to-date policy and procedural documentation is in place to instruct personnel on routine activities. Employees are also required to provide a signed acknowledgement of the employee handbook, including a Confidentiality, Non-Competition and Inventions Agreement on their date of hire.

3. Organization and Administration: Corporate structure includes job descriptions, along with organizational charts to ensure that roles and responsibilities are understood and properly assigned. Job descriptions are developed and maintained by the management of each department with the assistance of Human Resources. Job descriptions document the purpose of the position, areas of accountability, education/knowledge/experience/skill requirements and to whom the position reports.

G. Control Environment (Continued)

4. Human Resources: HOSTING has established formal procedures to provide assurance that prospective employees and transfers are qualified and capable of carrying out their job responsibilities. Personnel management policies and practices are consistent throughout HOSTING.

   The Human Resources Department is responsible for verifying that all background and reference checks are obtained and reviewed and that the responses are acceptable. Any discrepancies are highlighted and the information is reviewed with the candidate for follow-up. Negative responses are communicated to the requesting manager, and a decision is made regarding the impact of such responses on the candidate's employment status.

   New employees are trained on their security obligations through the use of computer based training modules, employee handbook and security policies maintained in the document management system.

   Employees are required to recertify their understanding of HOSTING security obligations by completing security awareness training and/or re-acknowledging HOSTING security policies annually.

5. Risk Assessment Process: HOSTING has placed into operation a risk assessment process to identify and manage risk that could affect its ability to provide reliable services to its customers. This continuous process allows HOSTING to identify significant risks based on the following:

   - Management's internal knowledge of its operations and the managed hosting industry
   - A quality control function that continuously evaluates the security and architecture of HOSTING's hosting environment

   For any significant risks identified, management is responsible for implementing appropriate measures to monitor and manage these risks (e.g., implementing/revising control procedures, conducting specific audit projects, etc.).

6. Information and Communication: The management team of HOSTING is comprised of business executives who meet periodically to discuss matters pertinent to the Company. The management team is responsible for:

   - Reviewing the effects of regulatory pronouncements on HOSTING
   - Overseeing strategic and operating activities

7. Monitoring: Management and supervisory personnel are responsible for monitoring the quality of internal control performance as a routine part of their activities. To assist them in this monitoring, HOSTING has developed comprehensive and summary management reports (alert monitor system) that monitor the functions of datacenters. Key reports are reviewed by management to help ensure appropriate action is taken as the alerts arise.

   On an on-going basis, datacenter managers discuss quality control measures and operational standards enterprise wide, continually striving to improve performance and efficiency.

H. General System Controls

1. Physical Security and Access Restrictions: The Datacenter Manager is responsible for the design, development and implementation of the datacenter physical and environmental controls in order to comply with corporate standards, objectives and policies. Access control systems are logged and audited.

   Administrative access to the access control system is limited to appropriate individuals based on job responsibilities. Terminated employees are promptly removed from access control systems, disabling the functionality of their physical access credentials until they can be collected.

   In addition to access control systems, the datacenters are monitored onsite and remotely by staff and the security systems such as video surveillance equipment that records video footage that can be reviewed at a later date.

   All visitors must present proper credentials authorized by HOSTING staff to gain admittance to HOSTING facilities. Visitors must obtain approval from HOSTING management before their visit. Any visitors that do not have a colocation contract with HOSTING must sign in and be escorted by authorized datacenter personnel from the time they initially enter the datacenter until they are escorted to the appropriate space. Equipment in the datacenter is secured so that customers onsite are only given access to their solutions. HOSTING internal infrastructure is further secured so that access is limited to only specifically authorized HOSTING employees and third-party vendors approved for maintenance.

   Customer equipment resides in cabinets or cages in the datacenter. The cabinets are constructed of steel/mesh and have locks on the doors, access to which requires physical keys. Electromagnetic card keys are required to reach customer specific areas. Customers are only given keys or access to their own solutions. All persons that do not have a HOSTING issued access badge are escorted while on site.

2. Network Monitoring, Security Incident Response, Problem Escalation, and Support: Escalation Procedures have been developed for addressing issues relating to outages of critical services, security incidents or other issues needing immediate action. These procedures vary based on the severity level of the problem. HOSTING provides 24/7/365 support coverage, including documenting, tracking, troubleshooting, notification and resolving of customer reported issues. This helps ensure system availability and compliance with service levels which vary based on the problem's definition. Service levels focus on the time required to adequately address reported problems. The Event Management team monitors all managed and customer owned equipment within the datacenter for ping and/or other available network services. The specific configuration of monitors depends on what the customer has elected to have monitoring setup on, what network services are made visible for the purposes of monitoring and what services HOSTING has determined monitoring is useful in order to aid in any requested troubleshooting of performance issues. In addition, management has implemented a bandwidth monitoring system that allows customers to view individual utilization reports. Monitoring of bandwidth spikes and traffic anomalies improves the availability of customer solutions and helps to promptly identify and remediate security incidents such as DDoS, protocol abuse and botnet activity.

   Management reviews all identified critical issues on a daily basis to ensure tickets are promptly addressed and appropriate customer communications occur. After resolution, the appropriate technician notifies the customer and communicates the current status and root cause of the problem to the customer. When the problem event has been resolved, the technician will close the online incident tracking ticket and contact the customer, if warranted. For security related incidents which might occur within customer solutions, prompt breach notice takes place to the customer once details about the event are investigated and confirmed. Following or in conjunction with notice, remediation actions are taken or suggested for change management approval as appropriate the nature of the incident.

H. General System Controls (Continued)

3. Customer Solution Development: Each customer solution allows for a high degree of customization. The exact configuration including infrastructure used, software installed and level of managed services are determined solely by the customer based on their need and intended use of the solution.

   HOSTING uses industry best-practices and application vendor recommendations that guide the design of HOSTING's customer solutions. These guiding principles, which pertain to equipment, logical and physical configuration, are designed to help minimize security risks in a consistent environment and maximize availability. The standards permit customization of solutions for customers, within the framework of a known and stable environment. The HOSTING Engineering and Security Teams are responsible for developing, maintaining, and testing these standards.

   There are two general classifications of approved technologies. The first group of standards relate to the use of pre-approved equipment and operating systems. HOSTING has selected a limited number of operating systems and versions (Windows and Linux) to support customer environments. This approach permits HOSTING operations to (1) develop personnel with specialized expertise in the selected platforms, (2) monitor the communications from the platform vendors and others regarding security patches necessary for the systems, and (3) reduce the risk that errors are introduced in configuring systems due to variances in configuration techniques between platforms. HOSTING has developed a process to approve equipment and add new standards as appropriate to better meet customer needs.

   The second group of standards relate to the use of pre-defined configurations of security solutions. These pre-defined configurations are used to provide assurance that implemented security solutions are properly "hardened" to reduce the risk of unauthorized access to customer assets. The Engineering and Security Teams design these configuration standards based on known risks and threats to that particular hardware and operating systems. Senior-level management must approve new configurations and changes to configurations/baselines. All servers deployed as part of customer solutions are configured incorporating industry standard best practices.

   HOSTING uses a development methodology for use in designing and implementing customer solutions. This methodology guides personnel in the design, testing, and implementation of systems to meet individual customer needs and to help ensure all necessary testing is completed before implementation.

H. General System Controls (Continued)

4. Software and Hardware Maintenance: HOSTING uses formal system provisioning documentation to guide personnel in the development/design, maintenance, testing, and implementation of systems. The standards allow for a range of variation when required based on customer's needs, while other components must strictly conform. These standards help ensure sufficient redundancy and capacity exists to provide for contracted availability services to clients. HOSTING has implemented formal change requirements (change request document) to guide personnel through system changes within the datacenter (both systems software and hardware). While the methodologies vary due to the nature of the system(s) maintained, the same general approach is used to help provide assurance that all modifications are properly designed, tested, authorized and implemented. Regardless of the nature of the change, an appropriate member of management must approve the change. To provide assurance that change activities occur in a controlled fashion, production-impacting changes are required to be migrated during predefined timeframes - any exceptions are dealt with on a case-by-case basis with appropriate oversight and approval requirements. Additionally, prior to changes being made in production, testing, back-out plans, risk analysis and risk mitigation activities are reviewed and approved at the appropriate management levels.

   Customers' representatives that are able to provide appropriate authentication information and HOSTING personnel may generate a request for modifications to existing environments. Customer change requests are normally entered into the HOSTING ticket tracking system through direct interface with Customer Service or the Sales Team. Changes that are deemed high risk (i.e. a change that could impact more than one HOSTING customer) are documented and assessed in a formal change management meeting.

5. Logical Access Controls: HOSTING is responsible for establishing standards and protocols for logical security, including: (1) HOSTING systems used to support the datacenter and transport information to customer systems housed at the datacenter, and (2) services provided under HOSTING agreements. Logical security is achieved by operating system-based security controls. Firewalls with VPN and Multifactor Authentication devices are deployed upon customer request and election of services. IDS, Vulnerability Scanning and Central Logging can also be contracted to meet stated security and compliance requirements within the customers hosting solution. Logical access for employees is controlled through Active Directory and RSA security tokens which are disabled upon termination of employment. Employee accounts are removed from the Active Directory environment within 90 days of their last day worked. Active Directory user permissions are reviewed on an annual basis to verify that users still require access.

All sensitive HOSTING and customer authentication information is secured using two factor authentication. Access to core HOSTING network infrastructure is restricted and reviewed on a quarterly basis to correct any potential discrepancies. Password change and complexity controls within systems are used to restrict unauthorized user access to HOSTING support infrastructure.