



liquidweb

INDEPENDENT PRACTITIONER'S TRUST SERVICES REPORT

LIQUID WEB, INC.

Web Hosting Services

Trust Services Report on Management's Assertion (SOC 3)

As Of

June 30, 2014

UHY **LLP**
Certified Public Accountants

LIQUID WEB, INC.

Trust Services Report on Management's Assertion (SOC 3)

Table of Contents

I. INDEPENDENT PRACTITIONER'S TRUST SERVICES REPORT.....	1
II. MANAGEMENT'S ASSERTION.....	2
III. DESCRIPTION OF THE LIQUID WEB SYSTEM USED TO MANAGE AND CONTROL WEB HOSTING SERVICES.....	3
Liquid Web Inc. Overview.....	3
Service Offerings Provided.....	3
Components of the Liquid Web, Inc. System.....	3
The Aspects of the System and Description of its Boundaries.....	5
Control Environment Elements.....	6
Management Oversight.....	6
Organizational Structure.....	6
Personnel Policies and Procedures.....	6
Risk Assessment Process.....	7
Monitoring.....	7
Liquid Web Data Centers.....	7
Security On-Site.....	7
Power Systems.....	7
Cooling.....	8
Fire and Smoke.....	8
The Liquid Web Network.....	8
Engineered by Liquid Web™.....	8
Tier-1 Premium Bandwidth Providers.....	8
Network Security.....	9
Logical Security.....	9
Liquid Web Heroic Support® Overview.....	9
<i>Our Support Staff</i>	9
<i>Liquid Web Sonar Monitoring®</i>	9
<i>Comprehensive Statistics</i>	10
<i>Sonar Improves Server Up-Time</i>	10
Dedicated Server Service Level Agreement (SLA).....	10
Network Uptime Service Level Agreement.....	10
Network SLA Exclusions.....	10
User Control Considerations.....	12

I. INDEPENDENT PRACTITIONER'S TRUST SERVICES REPORT

To the Board of Directors of Liquid Web, Inc.:

Scope

We have examined Management's assertion that as of June 30, 2014, Liquid Web, Inc. (Liquid Web) maintained effective controls over the web hosting services and supporting systems based on the AICPA and CICA trust services availability and security criteria to provide reasonable assurance that:

- The systems were available for operation and use, as committed or agreed;
- The systems were protected against unauthorized access (both physical and logical)

Liquid Web'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 hosting services and supporting systems covered by its assertion is attached. We did not examine this description, and accordingly, we do not express an opinion on it.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and included (1) obtaining an understanding of Liquid Web's relevant controls over the availability and security of the web hosting services and supporting systems; (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.

Inherent limitations

Because of their nature and inherent limitations of controls, Liquid Web's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct error or fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. The projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

Opinion

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

UHY **LLP**

Farmington Hills, Michigan
August 26, 2014

II. MANAGEMENT'S ASSERTION

Liquid Web's Assertion:



As of June 30, 2014, Liquid Web, in all material respects maintained effective controls over the web hosting services based on the AICPA and CICA trust services criteria for security and system availability set forth in TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Technical Practice Aids)*. We confirm, to the best of our knowledge and belief, that:

- The system was protected against unauthorized access (both physical and logical)
- The system was available for operation and use, as committed or agreed

Further, Liquid Web confirms that to the best of our knowledge and belief, that

The controls related to the trust services criteria were suitably designed and operated effectively as of June 30, 2014 to achieve those control objectives. The criteria we used in making this assertion were that

- i. The risks that threaten the achievement of the controls related to the trust services criteria have been identified by Liquid Web.
- ii. The controls related to the trust services criteria would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the trust services criteria from being achieved.

III. DESCRIPTION OF THE LIQUID WEB SYSTEM USED TO MANAGE AND CONTROL WEB HOSTING SERVICES

Liquid Web Inc. Overview

Liquid Web Inc. is a privately held managed web hosting company founded in 1997, with four data center facilities located in Lansing, Michigan and Phoenix, Arizona. Liquid Web is a leader in the professional web hosting market with an unwavering dedication to providing the best hosting products available. Liquid Web has over 20,000 clients served in over 120 countries. Liquid Web received the INC.5000 Fastest Growing Companies award in 2007, 2008, 2009, 2010, 2011, and 2012.

Service Offerings Provided

Hosting Services

- Dedicated web hosting - Private servers wholly allocated to the customer and fully managed by Liquid Web.
- Shared web hosting – Virtual servers shared with other customers
- Virtual private servers – Dedicated virtual servers

Network Services

- Load Balancing (Dedicated Load Balancers with Active/Active Redundancy)
- Managed File Replication Services
- Redundant Firewalls / Automatic Failover
- Virtual Private Network (VPN)
- Unmetered Bandwidth Solutions
- Content Delivery Network (CDN)

Backup/Storage Solutions

- Guardian Continuous Data Protection
- Storage Area Network (SAN)
- Terabyte Backup

Components of the Liquid Web, Inc. System

Infrastructure

Liquid Web data centers are designed with redundancy installed at every level, ensuring that a failure at any level will not affect customer servers. Liquid Web data center power is conditioned and reliable through the use of centralized UPS solutions backed by state-of-the-art generator technology. Liquid Web's network is robust and reliable. Data centers exclusively utilize premium Tier-1 bandwidth providers, ensuring minimal latency and fast connections to all points of the global internet.

The physical machines that provide hosting services for clients may be either dedicated (private servers wholly allocated to the customer) or virtual (share services between several customers). Each data center is configured to serve as a hot backup recovery site for the other sites. In addition, redundant network firewalls, routers and servers are installed to ensure network equipment failures do not impact customers' availability to their servers.

Software

Security Monitoring Software - Liquid Web maintains a portfolio of network and system security tools and applications to ensure that security threats are actively identified and managed.

Availability Monitoring Software - The Sonar Monitoring team utilizes a robust set of proprietary system level health and service monitoring tools to constantly ensure your server's optimal performance through early detection of problems. Escalation capabilities are built into the core of Sonar technology, ensuring that any complete system or service failures are instantly sent to the Liquid Web Service Restoration team for correction before clients even need be aware.

Backup Software - Liquid Web uses software to back up images of the entire environment at each data center (including infrastructure) to another virtual server located at an alternate Liquid Web datacenter.

People

Executive Management – The Executive Management Team is responsible for monitoring trends in the hosting services industry and identifying risks internally and externally. Executive Management is responsible for implementing appropriate measures to monitor and manage these risks. Appropriate measures may include the addition or revision of control procedures, conducting specific investigations, or any other means necessary to provide adequate control.

Heroic Support Team – Liquid Web has established a world class Heroic Support team that is professionally educated and available on-site at each data center 24 hours per day. Liquid Web currently employs 320+ Heroic Support engineers with specialties in Technical Support, Server Setup, Networking, Security and more.

Network Security Team: The Network Security Team continuously monitors the entire Liquid Web network for possible intrusions and attacks. The team investigates any issues and takes appropriate action. Real-time monitoring activity is presented in dashboards. The network monitoring dashboard graphic displays potential attack signature messages detected by perimeter firewalls and reports the activity back to the Network Security team.

Solar Monitoring Team: The Sonar Monitoring team utilizes a robust set of proprietary system level health and service monitoring tools to constantly ensure your server's optimal performance through early detection of problems. In the event that an issue is identified, our Sonar Monitoring Team responds immediately, reducing downtime and repairing any issues proactively, in many cases before the client is even aware of the problem.

Service Restoration Team: The Service Restoration Team is a highly trained division of Liquid Web specializing in restorations of all levels tasked solely with the purpose of keeping the servers of our clients responsive at all times.

Procedures

The Liquid Web Executive Team is ultimately responsible for the development and maintenance of policies and procedures. Individual department heads are responsible for maintaining and updating policies for their departments. All associates are responsible for suggesting needed updates.

These policies and procedures have been implemented to ensure consistent and effective security and availability over Liquid Web's hosting services, network services, and backup and storage solutions.

These services are supported by the Heroic Support Team. The key support services provided by Liquid Web include:

- Security Administration
 - o Physical Security of Liquid Web Facilities
 - o Granting, Revoking, or Modifying Physical Access to Liquid Web Facilities
 - o Logical Security over the System
 - o Granting, Revoking, or Modifying Logical Access to Liquid Web Applications and Systems Supporting Customer Security and Availability
 - o Managing Remote Access
 - o Managing Visitor and Contractor Access
 - o Monitoring Access

- Security Administration (Continued)
 - Network Monitoring, Anti-Virus Protection, and Incident Management
 - Encryption of Information and Customer Data as Agreed Upon in Customer Contracts
 - Management of Environmental Safeguards
 - Redundancy on the Liquid Web System
 - Backups of Customer Data, IT Infrastructure Data, and Backup Storage
 - Data Recovery and Disaster Recovery
 - Management of IT Infrastructure Changes

Data

Client Data – Liquid Web does not manage client data or content.

Audit Logs and System Log Files - Liquid Web system and network user activity, system activity, and system diagnostics are captured in audit logs and system logs that are retained within the system and/or forwarded to monitoring and reporting tools for analysis. The nature of these monitoring and reporting tools are described in Part H of this System Description, Description of General Control Activities and Processes.

The Aspects of the System and Description of its Boundaries

The Liquid Web system used for managing and controlling web hosting services is primarily responsible for the following types of activities:

- Providing physical, logical, and network security safeguards to customers as defined by customer contracts and monitoring those safeguards.
- Ensuring that network and systems are available for use by customers, as defined by service level agreements (SLAs) agreed to in advance with the customer. Availability requirements also include data backup routines, restoring data for clients, and ensuring continuous service during a security or availability incident.
- Resolving customer complaints, issues, and incidents on an as needed basis, or providing administrative services that customers require in order to interface with their hosted environment.

Liquid Web provides the following customer support services, which enhance the security and availability of the system by communicating related issues and requests with the customer:

- Help Desk tickets and other technical support requests
- Requests for changes to equipment configuration
- Requests for new or additional servers and/or services
- Requests for updates or modifications to existing servers and/or services

Through the help desk system and the Liquid Web website, clients may:

- Monitor hardware and services
- Generate and track support requests
- Monitor bandwidth usage and history
- Initiate online chat sessions with support personnel
- Upload and download documents
- View Invoices and Contracted Services
- Add or Remove Services via the website

Customer directed changes to hosted servers and services can also be performed via cPanel, a client control panel interface. cPanel automates and simplifies the administration of customer machines by supplying a client control panel to any domain names customers add to their server, which includes all of the features located under Liquid Web control. cPanel also supplies a webhost manager interface for customer usage to add accounts and perform many of the basic administrative tasks that would normally be very complex without the assistance of cPanel. Liquid Web also receives transactions via email, online chat, and by phone.

The Aspects of the System and Description of its Boundaries (Continued)

Certain monitoring activities are automated and will generate alerts in various formats based on significant events and conditions. Refer to *Environmental Monitoring* and *Threat Management* on subsequent pages.

A variety of web based reporting tools are available to customers. Refer to “Liquid Web Heroic Support” in the section below. Clients have flexibility to customize reporting and alerts based on their preferences. Billing and other financial reports are standardized based on the client’s Statement of Work and the services selected.

Control Environment Elements

Liquid Web’s control environment reflects the position taken by management, its Board of Directors, and others concerning the importance of controls and the emphasis given to controls in its policies, procedures, methods, and organizational structure. The following is a description of the key elements of Liquid Web’s web hosting services:

- Management Oversight
- Organizational Structure
- Personnel Policies and Procedures

Management Oversight

The oversight of the day-to-day operations of the Company is under the direction of the President and the Executive Management Team consisting of the various heads of functional departments. The Management Team meets on a weekly basis to review the results of operations, discuss unusual activity or events, review key metrics and financial results, and discuss other matters important to the operation of the Company.

In addition, the Executive Management Team is responsible for:

- Reviewing the professional services to be provided by Liquid Web’s independent auditors and the independence of such auditors;
- Reviewing the scope and results of all audits - internal and external; and
- Reviewing the system of internal accounting controls and other matters relating to Liquid Web’s web hosting services.

Organizational Structure

The Organization employs a staff of approximately 300 people. Liquid Web is divided into operating departments, which provide a framework for planning, directing, and controlling its operations. Personnel and business functions are segregated into distinct process units listed here:

- Sales and Marketing – Responsible for all new business development for the company as well as Account Management.
- Finance and Administration – Supports the company in all traditional Finance, Accounting and G&A functions including maintaining the General Ledger, Accounts Payable, Accounts Receivable, Fixed Assets, and Human Resources.
- Operations – Responsible for the data center, network infrastructure, client’s deployments, and managed services. Supports all technologies, including, but not limited to: hardware, software programs, software development, networks, desktops, telecommunications, and security.

Personnel Policies and Procedures

Liquid Web’s controls cover all critical aspects of employment, including hiring, training and development, performance appraisals, and terminations. In addition, all employees have access to an employee handbook, policies, and procedures. Changes to these documents are communicated to existing personnel in writing. The sensitivity of the job determines the level of background checks performed on applicants before his/her employment.

Personnel Policies and Procedures (Continued)

The Human Resources Department is primarily responsible for recruiting and evaluating job applicants. Hiring practices are designed to ensure that new employees are qualified for their job responsibilities. The Human Resources Department and the management of the department hiring the employee must jointly approve each hiring of a new employee. Liquid Web has a structured interview process, which includes application screening, a screening interview, testing, and interviews.

Training of personnel is accomplished through supervised on-the-job training and in-house classes. Certain positions require the completion of special training. Department managers are also responsible for encouraging the training and development of employees so that all personnel continue to improve their skills applicable to their functional responsibilities.

Risk Assessment Process

Liquid Web recognizes that risk management is a critical component of its operation that helps ensure that assets are properly managed and clients are properly served. Through regular and open communication among staff, management, and its client base, Liquid Web identifies risks that could negatively impact the security of the business. For any significant risks that are identified and communicated, the Executive Management Team is responsible for implementing appropriate measures to monitor and manage these risks. Appropriate measures may include the addition or revision of control procedures, conducting specific investigations, or any other means necessary to provide adequate control.

Monitoring

Management and supervisory personnel are responsible for monitoring the quality of internal control performance as a routine part of their daily duties. To assist them, Liquid Web utilizes a series of management reports and other methods to monitor the business. Key reports are reviewed by management to help ensure appropriate action is taken as needed. If issues arise that cannot be readily resolved, issues are escalated to the Executive Management Team.

Liquid Web Data Centers

Liquid Web's data center locations are staffed by highly skilled engineers around the clock. Liquid Web data centers are designed with redundancy installed at every level, ensuring that a failure at any level will not affect your server. Liquid Web data centers power is conditioned and reliable through the use of centralized UPS solutions backed by state-of-the-art generator technology. Liquid Web's network is robust and reliable. We exclusively utilize premium Tier-1 bandwidth providers, ensuring minimal latency and fast connections to all points of the global internet.

Security On-Site

Datacenter access is strictly limited to technical staff. Electronic security systems control data center access and are accompanied by a full complement of motion detecting security cameras which monitor the entire facility. Our Datacenter facility external walls are reinforced poured concrete. We are a fully managed facility, which means we have level 3 technicians on site 24 hours per day, allowing incident response times to be kept to a minimum.

All Datacenter visitors are required to register and wear a visitor badge at all times. All visitors are escorted by a Liquid Web associate at all times while on site.

Power Systems

Our power systems feature extensive fault tolerance and resilience at every layer. Incoming service is routed underground to a dedicated on-site transformer. This system routes to our automatic transfer switch that monitors power quality, and automatically transfers to our emergency generators in the event they are needed. Each facility is also protected by one or more uninterruptible Power Supplies (UPS), featuring redundant battery cabinets, and full maintenance bypass cabinets allowing for service and upgrades without interruption of power to our servers.

Power Systems (Continued)

Power distribution units handle final power transformation and distribution to racks, ensuring clean consistent power to data center equipment.

Each facility has multiple emergency generators waiting on standby, featuring over 24 hours of autonomous runtime before requiring refueling. Each generator is test run at least once a week to ensure they are ready in the event they are needed. Generator fuel is maintained in sub-base storage tanks that are locked.

Liebert Precision power distribution units handle final power transformation and distribution to racks, ensuring clean consistent power to data center equipment.

Generator power is activated automatically in the event of a utility failure by the transfer switch. The data center load is maintained by the UPS units with at least 15 minutes of capacity, however this is not necessary as the generator is active and up to speed within 10 seconds of a power failure.

Cooling

Environmental processing systems include redundant Liebert Precision 22 ton up flow air conditioning units. Temperature and humidity are precisely monitored and regulated year round to ensure optimal equipment reliability. Alerts are sent to Operations personnel any time temperature or humidity is outside an established range. Each unit contains independent compressors and cooling loops to further enhance fault tolerance and reliability. Air filtration systems actively remove foreign particulates from circulation and cycle the entire data center air supply in a matter of minutes.

Fire and Smoke

Each facility is monitored with state of the art smoke and fire detection systems. In the unlikely event of a fire, automated fire suppression systems are also in place.

The Liquid Web Network

The Liquid Web network has been designed to accommodate clients demanding the highest quality network performance. There is a central focus on redundancy allowing our network to rapidly self-heal failures without interruptions to connectivity. Our redundancy is multi-tiered with N+1 internal device elements as well as entirely redundant chassis allowing any routing device to fail without interrupting client data connectivity. All core routing and switching equipment is state of the art Cisco.

Engineered by Liquid Web™

Unlike most providers, Liquid Web owns and operates its entire infrastructure. By engineering and controlling our infrastructure personally, from routers to servers, we are able to immediately respond to any issue directly. This means that the Liquid Web Engineers that you rely on will have direct physical access to the server.

Tier-1 Premium Bandwidth Providers

Providing the highest quality Internet connectivity and performance is our top priority. We have selected premium Tier-1 bandwidth providers, ensuring minimal latency and fast connections to all points of the global internet. Our aggregate connectivity reaches an astounding 8,500+ networks just a single network away from our uplinks.

Network architecture includes a dual feed network fiber ring connected at two diverse points at opposite ends of the physical building. These network feeds take diverse paths to separate telecommunications providers where separate colocation facilities house connections to multiple internet service providers.

Core network devices are maintained within a locked cage facility within the main data center. Only network administration personnel have access to the core network devices.

Network architecture includes four layers of full redundancy. The first three layers are controlled exclusively by network administrators, with the lowest level including limited access by the customer service group in order to facilitate customer access requests.

Network Security

The entire network is constantly monitored using a custom developed real time network monitoring and alerting system. Any unusual or suspicious network activity is highlighted and forwarded to network administrators for investigation and resolution.

Logical Security

Liquid Web maintains a collection of more than 20 corporate policies dedicated to maintaining the security of the equipment and the data in their facilities. Security policies are regularly reviewed and updated to account for changes in risks and technologies. Security policies are available at all times via the corporate intranet. All employees are required to read and acknowledge their understanding of all security policies as part of their initial orientation. Employees are also required to sign a comprehensive non-disclosure agreement to ensure that client privacy and confidentiality is protected.

Security Policies include but are not limited to the following topics:

- Acceptable Use Policy
- E-mail policy
- Password Policy
- Information Sensitivity Policy
- Personal Communication Device policy
- Remote Access Policy
- Malware Protection Policy
- VPN security policy
- Wireless Communication Policy

Liquid Web Heroic Support® Overview

Liquid Web's Heroic Support® provides 24/7/365 access to level 3 engineers by phone or email, state of the art infrastructure engineered for complete reliability, software hardening to protect the integrity of your server, proactive monitoring and service restoration, complete user level tools for monitoring the health of your server, and if anything was to go wrong - a 100% up-time SLA.

Heroic Support® provides our clients confidence and peace of mind through complete reliability, engineer accessibility, and proactive service restoration.

Our average support request phone call is answered within 20 seconds, with an average electronic support response time of 30 minutes.

Our Support Staff

Liquid Web has established a world class Heroic Support team that is professionally educated and available on-site at each data center 24 hours per day. Liquid Web currently employs 320+ Heroic Support engineers with specialties in Technical Support, Server Setup, Networking, Security and more.

Liquid Web Sonar Monitoring®

Sonar Monitoring is a dedicated division of Liquid Web solely focused on providing service reliability and immediate incident resolution. The Sonar Monitoring team utilizes a robust set of proprietary system level health and service monitoring tools to constantly ensure your server's optimal performance through early detection of problems. In the event that an issue is identified, our Sonar Monitoring Team responds immediately, reducing downtime and repairing any issues proactively, in many cases before the client is even aware of the problem.

The Sonar Monitoring team focuses on prevention of, as well as immediate response to, service interruptions, whether they be software, hardware or network-related. With the bulk of service failures being prevented before occurrence, and nearly all remaining service failures being corrected within minutes, the team operates as a persistent proactive manager of client service consistency. The Liquid Web Sonar Monitoring Team has enabled us to provide the industry's leading 30-minute hardware replacement SLA.

Comprehensive Statistics

System statistics are presented to customers in an overview and drill down format, allowing clients to view all of their server statistics on a single page, including multiple server accounts. Drill down capabilities include the ability to view details on any individual metric and view the status graphically over a period of hours, days, or weeks.

Trending is both easy and convenient and offers peace of mind that would otherwise be impossible with random sampling. Without a tool such as Sonar, off-hour periods of service degradation are nearly impossible to identify.

Sonar Improves Server Up-Time

Without Liquid Web Sonar, failures of services or severe service degradations are more single hit scenarios where an incident occurs and a restore is initiated with no clear vector for repair of the base cause.

With Sonar in place, the failure of a service will be detected and restoration will be initiated by technical staff, however with Liquid Web Sonar both client and technician are able to evaluate the forensic data of all critical statistics leading to that failure and correct the root of the issue. This powerful tool allows Liquid Web to solve problems that could live for many months even with the most vigilant competing managed providers.

Escalation capabilities are built into the core of Sonar technology, ensuring that any complete system or service failures are instantly sent to the Liquid Web Service Restoration team for correction before clients even need be aware. Liquid Web's Service Restoration Team corrects a huge majority of failures long before the client is even aware. The Service Restoration Team is a highly trained division of Liquid Web specializing in restorations of all levels tasked solely with the purpose of keeping the servers of our clients responsive at all times.

Dedicated Server Service Level Agreement (SLA)

Hardware Replacement Service Level Agreement

Liquid Web guarantees that in the event of a dedicated server hardware failure, the faulty hardware will be replaced within **30 Minutes** of identifying the problem. In the event that this guarantee is not met, Liquid Web will issue a credit for ten times the actual amount of additional downtime. The amount of compensation may not exceed the customer's monthly recurring charge. This guarantee does not include the time it requires to perform additional software related maintenance, including rebuilding web accounts from backups, cloning hard drives, reloading the operating system, reloading and configuring applications, or rebuilding raid arrays.

Network Uptime Service Level Agreement

Liquid Web guarantees network uptime to be **100%**. This guarantee assures that all major routing devices within our network are reachable from the global internet 100% of the time.

Network SLA Exclusions

Many possible situations are completely beyond the control of Liquid Web, and therefore are not in the scope of this SLA. These situations include:

- **Scheduled Network Maintenance** - occasionally network maintenance will be required. Liquid Web will do everything possible to minimize and avoid downtime during this maintenance. You will receive prior notification of upcoming maintenance at the email address we have on file. Scheduled maintenance periods are not eligible for SLA credits.
- **Hardware Maintenance** - on rare occasions, the hardware in your Dedicated Server may need maintenance or replacement. Liquid Web will do everything possible to minimize any downtime in these situations per our hardware replacement SLA. Any downtime incurred as a result of this maintenance will not be counted towards our network SLA.

Network SLA Exclusions (Continued)

- **Software Maintenance** - an important part of managing a dedicated server is keeping the software up to date. If you choose to have Liquid Web manage your server, occasional software updates will be required to address security or performance issues. Usually you will experience little or no downtime in these situations, but we cannot guarantee a specific amount of time in all situations.
- **Malicious Attacks** - if a third party not associated with Liquid Web initiates a "Denial of Service" or other form of disabling attack against your Dedicated Server or major portions of our network, Liquid Web will do everything in its power to stop the attack, but cannot guarantee a resolution time.
- **Legal Actions** - In the case that a legal action is taken against a customer of Liquid Web and Liquid Web is required to act in accordance with the order, Liquid Web shall not be responsible for any SLA damages.
- **cPanel Issues** - if you choose to run cPanel and Web Host Manager on your Dedicated Server, the default install will be configured for automatic updates of cPanel related software. On occasion, one of these automatic updates could adversely affect all or part of the cPanel related software on you server. Liquid Web will do whatever is necessary to fix any cPanel related problems, but cannot guarantee a resolution time.

Network SLA Remedy

In the event that Liquid Web does not meet this SLA, Dedicated Hosting clients will become eligible to request compensation for downtime. If Liquid Web is or is not directly responsible for causing the downtime, the customer will receive a credit for **10 times (1,000%) the actual amount of downtime**. This means that if your server is unreachable for 1 hour (*beyond the 0.0% allowed*), you will receive 10 hours of credit.

All requests for compensation must be received within 5 business days of the incident in question. The amount of compensation may not exceed the customer's monthly recurring charge. This SLA does not apply for any month that the customer has been in breach of Liquid Web Terms of Service or if the account is in default of payment.

Response Time SLA

Liquid Web's managed customers are covered by our thirty-minute initial response time guarantee. That means that when you submit a trouble ticket via our help desk system you are guaranteed a response from a Heroic Support® technician within thirty minutes. If Liquid Web fails to respond within thirty minutes, you will be credited 10 times the amount of time exceeding our SLA commitment. That means that if your ticket goes 1 hour past our stated initial response time guarantee, your account will receive a 10 hour hosting credit. All requests for compensation must be received within 5 business days of the incident in question. The amount of compensation may not exceed the customer's monthly recurring charge. This SLA does not apply for any month that the customer has been in breach of Liquid Web Terms of Service or if the account is in default of payment.

User Control Considerations

Liquid Web controls are only a portion of the overall control of each client. Clients of Liquid Web also need to implement and maintain effective internal controls. This section highlights those controls that Liquid Web believes should be present for each client. Liquid Web has considered the following controls in developing the controls which are described in Section IV of this report. Each client must evaluate its own internal controls to determine if the following controls and procedures are in place.

Liquid Web's systems were designed with the assumption that certain controls would be implemented by user organizations. In certain situations, the application of specific controls at user organizations is necessary to achieve certain control objectives included in this report.

This section describes other internal control structure policies and procedures that should be in operation at user organizations to complement the control structure policies and procedures at Liquid Web. User auditors should consider whether the following policies and procedures have been placed in operation at user organizations:

- Each customer must acknowledge receipt and understanding of the Terms of Service and Service Level Agreement for the particular services they sign up for.
- For customers that select optional backup of their data, a monitoring and backup system ensures successful data backup. Verification of backup data and restoration of systems and data is solely the responsibility of the customer.
- Customer data backup is an optional service which is provided by maintaining backups of customer data. Procedures for maintaining customer data backups are available on the company intranet.
- Certain security functions may require additional authentication by customer service reps either online or by telephone.
- Liquid Web does not provide for data classification for customer data. Customers are responsible for classification of their own data.
- If Liquid Web's default backup schedule is not selected, client is responsible for determining the backup schedule that is appropriate for their business needs.
- Client is responsible for maintaining accurate contact information with Liquid Web personnel.
- Client is solely responsible for software and database maintenance.
- For all layers of technology that are not specified in a client contract as Liquid Web's responsibility (including, but not limited to, networking, operating system, database, and application layers), the client is responsible for properly administering and securing relevant layers of technology (e.g., determining appropriate access, segregation of duties, audit trails, etc.). Client is fully responsible for controlling access to supervisor id and passwords that would allow control over customer processing and data.
- Clients are responsible for the review of metrics and statistics and for communicating any issues with service levels to Liquid Web.
- Liquid Web Terms of Service specify prohibited content, prohibited services and processes. It is each client's responsibility to agree to and abide by the Terms of Service.