REPO SYSTEMS

NONDISCLOSURE AGREEMENT

In consideration for the disclosure by RepoSystems.Com Inc., The RepoSystems Group, LLC and Optical Recognitions Systems, Inc. (collectively referred to as "The Company") the confidential information contained therein (the Proprietary Material), the respective customers whose financial information reporting processes and controls include those of The Company and collectively, the users agree that the Proprietary Material is, and shall at all times, remain the property of The Company and shall be used solely by the users for the purposes described in agreement with The Company.

Use of Proprietary Material for the benefit of parties other than the intended users is prohibited. The users may not copy, reproduce, sell, assign, license, market, transfer, or otherwise dispose of or give the Proprietary Material to any person, firm, corporation, or other entity.

The users shall keep the Proprietary Material confidential and shall not disclose the Proprietary Material to another party without first obtaining written permission from a duly authorized officer of The Company.

The users shall restrict use of Proprietary Material to its employees who are involved in the evaluation of the Proprietary Material.

If you disagree with the above statement you must immediately:

If sent electronically - remove the documentation from your computer, computer networks and any other system that you personally or automatically (mechanically) replicated it to.

If received a printed document – return the document to the discloser without copying or reproducing.

9400 n. macarthur blvd.
suite 124-409
irving, tx 75063

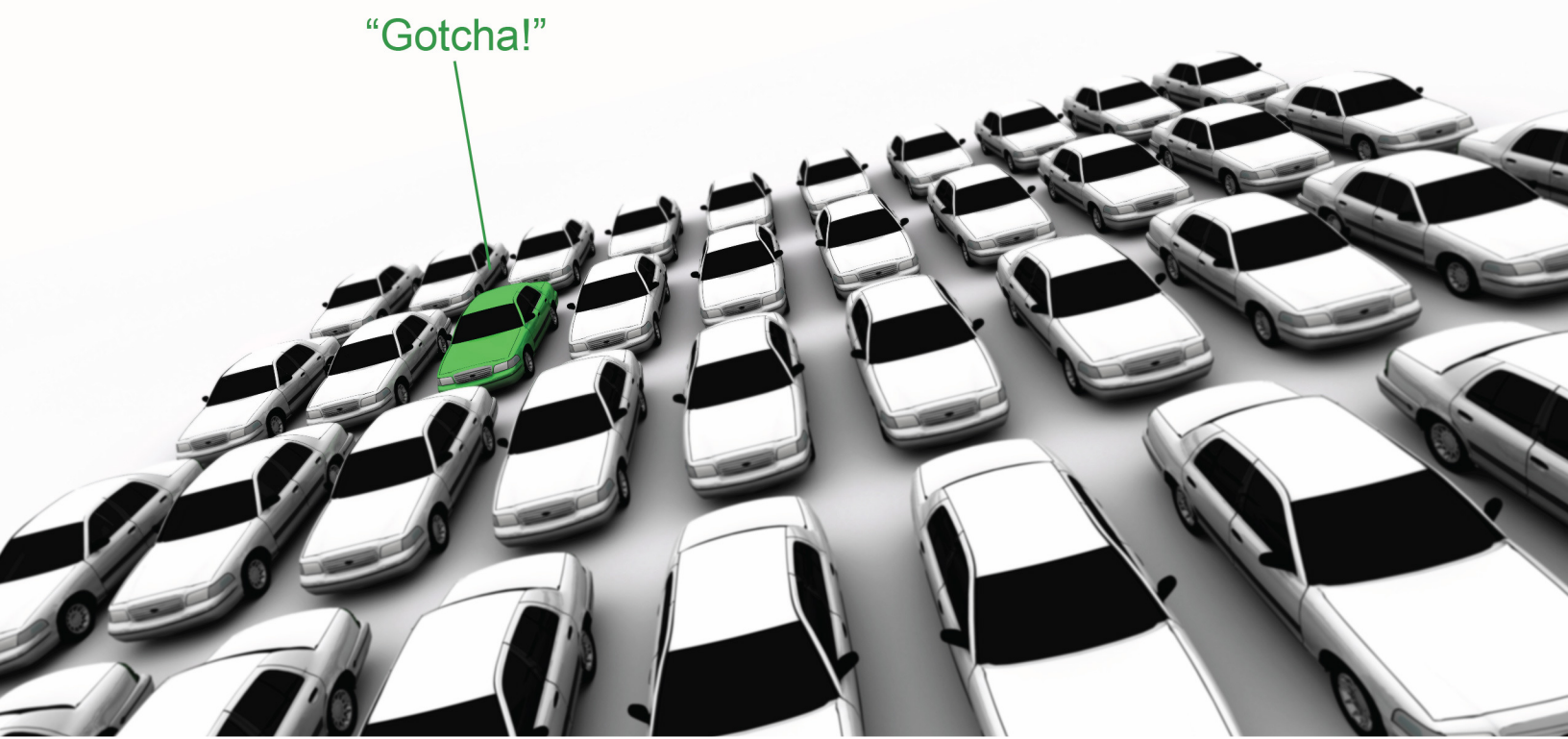
866.906.0573
p. 972.501.0375
f. 214.853.5327

reposystems.com

REPO | SYSTEMS

Facts & Information

For Lenders



REPO SYSTEMS Facts & Information

Our philosophy is extremely simple:

We provide you the tools and Network to help you recover your collateral.

- Web portal to manage your recoveries and assignments
- LPR Solutions to increase the opportunities
- Payment solutions to assure that your agents are paid quickly and accurately
- Skip Trace Technology Solutions so that you can locate collateral much easier. *
- VIN 2 Plate service so that you get the most recent registration of a license plate to a VIN.
- GPS DNA so that you don’t ever have to question if your recovery company agents are actually running your repossession accounts.

* Must be credentialed prior to usage

REPO | SYSTEMS Facts & Information

Who is RepoSystems?

RepoSystems is a management and communications tool for the collateral recovery industry. "Lending Institutions" and "Recovery Agents" can communicate in real-time to enhance productivity, efficiency and accuracy in the recovery of the collateral. Our system provides an end-to-end collateral recovery solution that automates the repossession process from assignment and recovery, to disposition.

RepoSystems key benefits include:

- Overhead substantially reduced
- Redundant data entry eliminated
- File processing costs reduced
- Telephone time greatly reduced
- Processing capacity increased
- Assignments quickly processed and dispatched
- Efficiency gains direct to bottom line

We aren't part of the "good 'ol boy" network. We only provide the best technology to help you with your collateral recovery.

We don't spend money trying to "win" you over…we simply want to provide you the best tools to help you get your recoveries.

REPO | SYSTEMS Facts & Information

Need Tag or License Plate Information from your VIN?

Utilize our VIN2PLATE Service

ANY License Plate Recognition system needs License Plate data. We have the ability to provide you with the data, internally from RepoSystems. Just click on the "Request License Plate" checkbox while entering the repossession order or editing the vehicle information section and you will be provided the data IMMEDIATELY!

THE RESULT IS INSTANTANEOUS!

This service is optional and not required. However, the ability for you to locate your repossession by LPR is IMPOSSIBLE without a License Plate!

For each request you make, you will be charged 75₵ ($0.75) deducted from your RepoSystems Wallet.

If we do not get a positive result on the License Plate search, your RepoSystems Wallet will be refunded the amount automatically.

For more information on our services including RepoSystems Services or our Skip Tracing Tools, please call our sales department at 972.501.0375 x 1005 or email us at sales@reposystems.com

REPO | SYSTEMS Facts & Information

RepoSystems GPS DNA

How would you like it if:

- Your agents were able to provide updates guaranteeing you that they actually visited the location?

- If you didn't have to spend any more time calling your agents for updates and if they ran the addresses?

- If you could reduce your overall costs of verifying updates to your accounts!?!

We have 3 great versions of our patent pending GPS DNA mobile application that you can choose from.

Our iPhone and Android applications are available for download from the Apple Store or the Play Store and will work on most any version of iPhone, iPad, Android Phones and Tablets.

They have the following features:

- Notification of an opportunity from our National Hotlist within an approximate 1 mile radius of a potential repossession

- Notification details of the opportunity when you are within an approximate 250 feet of the opportunity. Will display the unit details so that you can visualize what you are looking for.

- No files are stored on the device for the National Hotlist, everything is in virtual memory and only available while the application is active.

(Continued on Next Page)

REPO | SYSTEMS Facts & Information

RepoSystems GPS DNA (Continued)

- No debtor information is revealed or stored for compliance maintenance.
- Spotter fee are potentially available to the agents or spotters
- Automatic updates of the address visit to assure the agents were there.

Our GPS DNA PC version has the same features as the iPhone and Apps with the following additional features:

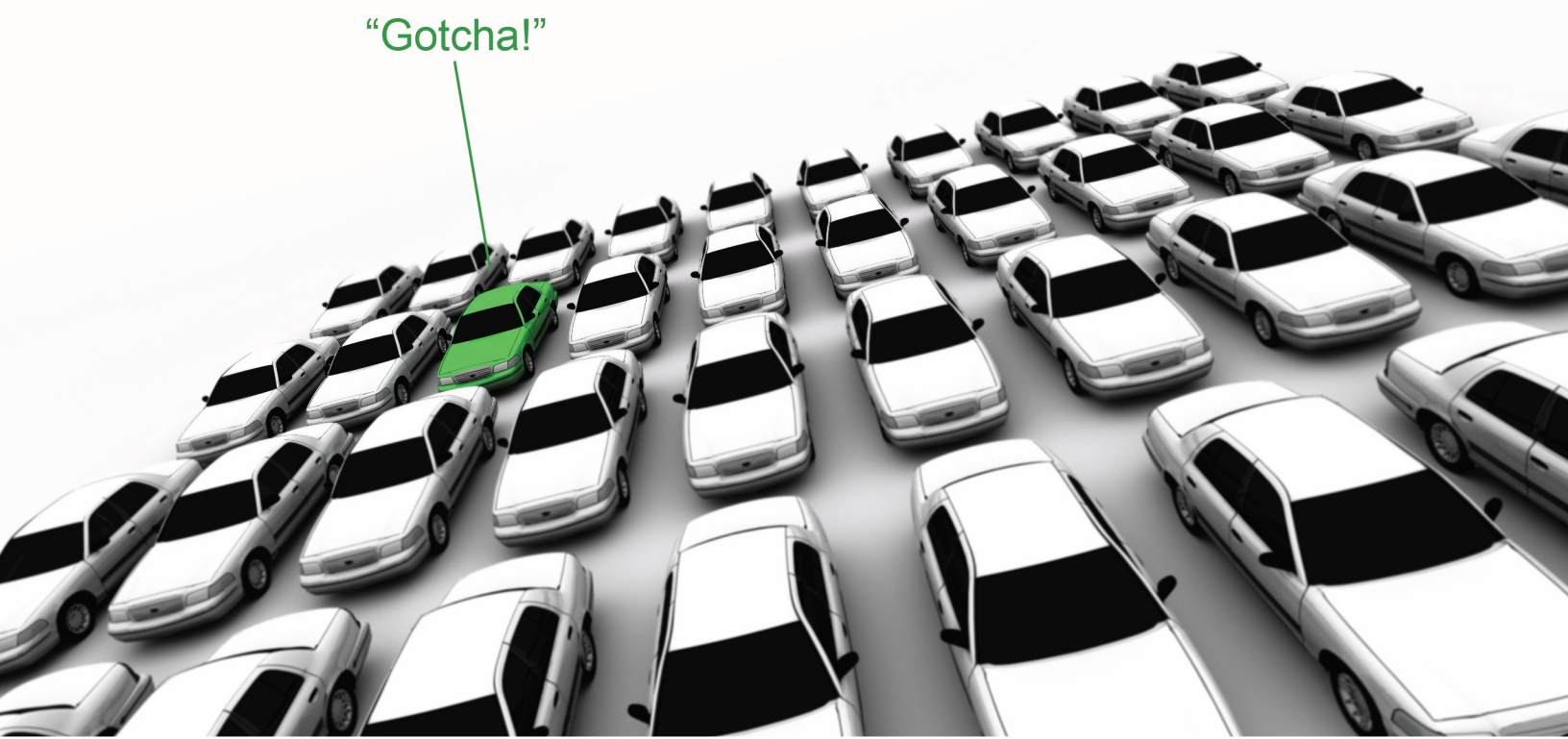
- Is an add-on application to Microsoft Mappoint
- Allows agent to export from within RepoSystems different status files for import into Mappoint
- Route Optimization for agents to conserve fuel

For more information on our GPS DNA services please call our sales department at 972.501.0375 x 1015 or email us at gpsdna@reposystems.com

REPO | SYSTEMS

Facts & Information

Competitor Comparison Report



RSN REPO | SYSTEMS
A Veteran Owned Business

Feature	RSN	RDN	iRepo / REPros
Address Visit Verification through GPS DNA	Yes	No	No
GPS DNA Spotter Network with AVV	Yes	No	No
Has own LPR System	Yes	No	No
Prohibit lenders from using other similar services by contract	No	Yes	?
Provide Export out to other LPR Systems (including DRN, MVTrac, VLS)	Yes	?	?
Compliance Auditing	Yes	?	?
Repossession Company Report Cards	Yes	?	?
Reconciliation Reporting (to see if orders are in the system and their status)	Yes	?	?
Incident Reporting – Case Management (for issues with repo companies)	Yes	?	?
Document Retention Policy	Yes	?	?
Integrated Skip Tracing Technology	Yes	No	No
Able to get License Plate/Tag information from VIN	Yes	Yes	?
Verified Assessments / customized testing (pass/no pass to be able to work accounts)	Yes	No	No
Customizable	Yes	?	?
Lenders Interface	Yes	Yes	Yes
Free Access For Lenders	Yes	No	No
Paperless Capabilities for Lenders and Recovery Companies	Yes	?	?
Integrated Accounting	Yes	Yes	Yes
Flexible Flat Monthly Fee Pricing Structure	Yes	No	No
Unlimited Users	Yes	No	?
Online Chat Technical Support	Yes	?	?
Email Technical Support	Yes	Yes	Yes
Phone Support	Yes	Yes	Yes
Receptive to Customer Technology Change Requests	Yes	?	?
Charge Customers for New Development or Change Request	No	?	?
Integrated Wallet System for Payments Processing	Yes	?	?

? = Information was not available at publication

RSN REPO | SYSTEMS
A Veteran Owned Business

Feature	RSN	DRN	MVTRac
Address Visit Verification through GPS DNA	Yes	No	No
Charge Lenders for locates	No	Yes	Yes
Charge Repo Company to locate own vehicles	No	Yes	?
Charge Repo Company for Locates (if their data)	No	Yes	Yes
Immediate Locate Notification	Yes	?	?
Camera Cost	See Below [1]	See Below [2]	See Below [3]
Financing Options (camera equipment)	Yes	Yes	Yes
Historical Plate Search	Yes	Yes	Yes
Charge for History Searches	Yes & No*	Yes	Yes
Claim ownership of the data	No	Yes	?
Prohibit lenders from using other similar services	No	Yes	?
Prohibit Repo Company from using other similar services	No	Yes	?
Camera Operator can set their own finder/locate fees	Yes	No	No
Can Provide Tag information from VIN	Yes	?	Yes
Integrated with collateral management software tool	with Self/RSN	RDN	RMP
Wide Network Many Users (cameras on the street)	Yes	Yes	Yes
Integrated Wallet System for LPR Locate Purchases	Yes	?	?
Full Reporting and Management Suite of Tools	Yes	?	?

? = Information was not available at publication

[1] RSN has 2 camera Economy = $4390-$5480, 2 Camera Rugged = $5930-$7410, 4 Camera Rugged $7940-$9930

[2] Historically the camera systems have been in excess of $12,000 depending on when and where you purchase

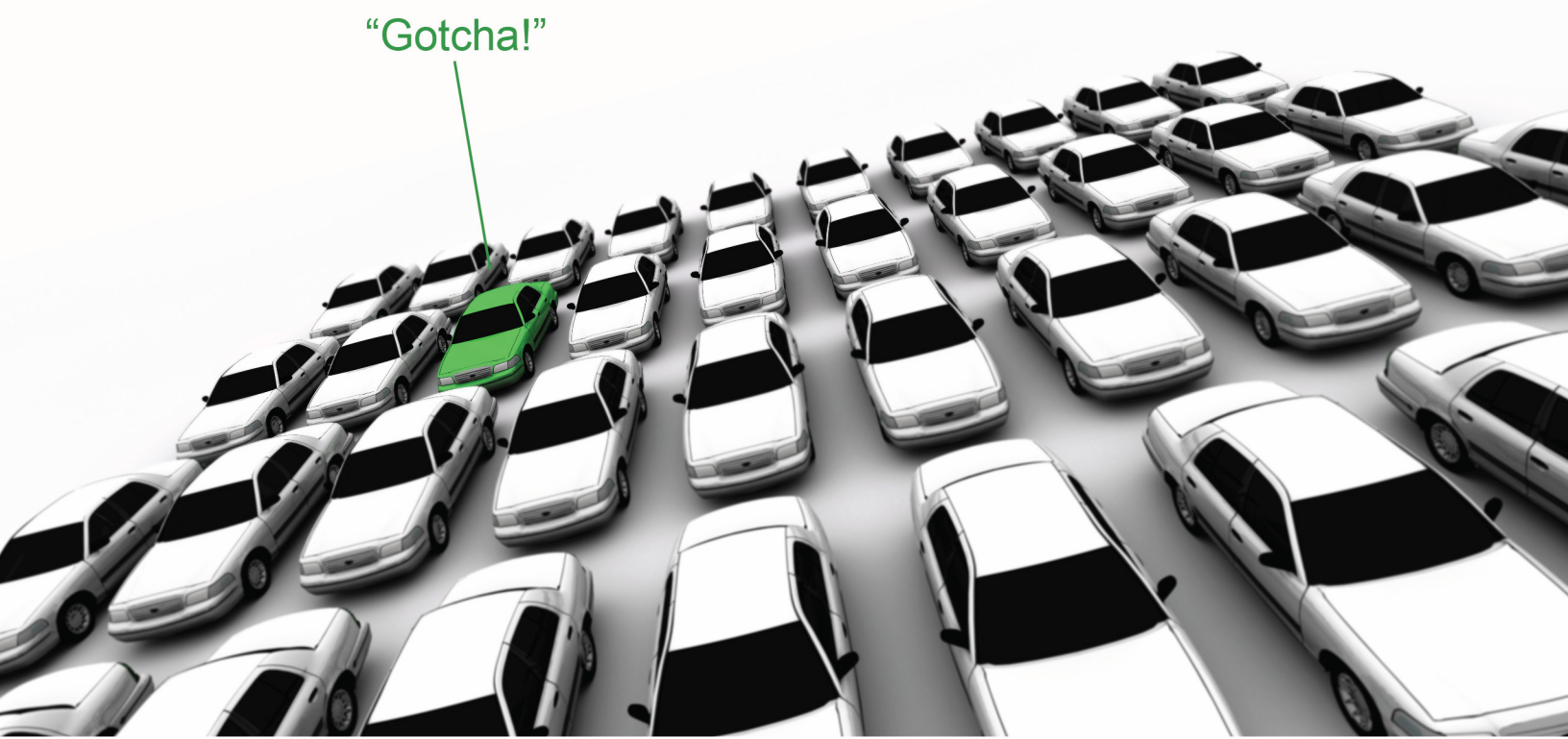
[3] General knowledge indicates this is a lease at $600 per month, with no end in contract, minimum of $3000 down

* RSN doesn't charge for the searches, however, we do allow the agent to set a fee and charge a fee, money is transferred from buyer to seller using the RSN Wallet.

REPO | SYSTEMS

Facts & Information

Document Retention



BUSINESS RECORDS &
DOCUMENT RETENTION POLICY

I. PURPOSE

The purpose of this policy is to define the retention periods RepoSystems.Com Inc, The RepoSystems Group, LLC and Opticial Recognition Systems, Inc, hereinafter known as the "Company", for various types of business records in order to promote efficiency and to minimize the cost and space required to store and maintain business records. The policy identifies business records by category and defines how long such documents should be retained. Once the retention period has expired, such records may be discarded in order to eliminate the accumulation of unnecessary documents. A proper business records retention program also ensures compliance with relevant laws and may help to protect the Company when it is involved in a litigation, government investigation or audit.

II. SCOPE

This policy applies to all domestic Company locations and all functional responsibilities, including corporate offices and all branch facilities located in the United States, its territories and possessions.

III. POLICY

Company business records are to be maintained and discarded (by destruction or otherwise) in accordance with the Record Retention Schedule set forth below and as updated from time to time.

IV. RESPONSIBILITY

The interpretation and administration of this policy shall be the responsibility of the Legal and Human Resources Departments of the Company and any business that each entity is "doing business as", depending on the type of document in question.

BUSINESS RECORDS &
DOCUMENT RETENTION POLICY

V. DEFINITION OF BUSINESS RECORDS

The business records discussed in this policy include any records documenting the domestic business operations of RepoSystems.Com Inc. or The RepoSystems Group, LLC and its affiliates (hereinafter "RepoSystems" or the "Company") which are in a retrievable state. Records may be written, such as agreements, correspondence, memoranda, electronic mail, invoices, sales receipts and summaries, books of account, purchase orders, and tax reports. Records may also be stored electronically on computer hard drives, floppy disks and tapes, or on microfilm, acetate slides, and video cassettes. Business records include not only materials which are distributed or retained in office or central files, but also individually maintained materials, such as appointment books, telephone logs, electronic mail folders, presentations, travel and expense reports and calendars.

VI. LOCATION OF RECORDS

All Company business records approved for retention should be maintained on Company property or in an approved storage location. Employees are generally not permitted to maintain business records in personal, off-site files (at home, in car trunk, etc.). An employees wilfull violation of this policy may be cause for termination.

VII. GENERAL RULE FOR RETENTION PERIODS

A. Hard or Electronic Copies. As a general rule, hard or electronic copies of business records are only to be retained for the current calendar year plus one year ("C+1"). This general policy is to be adhered to uniformly throughout the Company. **However, various exceptions to this general rule apply. Such exceptions are set forth in Section VIII below.**

B. Electronic Mail. As a general rule, all electronic mail residing on individual personal computers are to be deleted by the user as soon as they no longer need to be retained. Messages without attachments that are stored or retained electronically will be deleted automatically by the Company after six months. Electronic messages with standard attachments (e.g., Word documents, Excel spreadsheets, PowerPoint presentations, etc.) will be deleted automatically by the Company after three months. Employees who wish to avoid automatic deletion by the Company are encouraged to print hard copies of such attachments or electronically archive them with the assistance of the Information Services Department. Electronic messages with non-standard attachments are discouraged (e.g., videos, sound files, and large graphics with file extensions such as .AVI, .GIF, .MP3, .EXE, .BMP, .WAV, etc.) and MAY be deleted automatically by the Company on a weekly basis.

BUSINESS RECORDS &
DOCUMENT RETENTION POLICY

VIII. EXCEPTIONS

For a variety of reasons, certain documents must be retained for longer (or shorter) periods than C+1. Drafts of records are to be disposed of as soon as final records are prepared. Other exceptions to the general C+1 policy are described below:

A. TAX AUDITS

(1) Income Tax Audits. All books of original entry and original source documents which support such books of accounts are to be retained until the year's tax returns, both Federal and State, have been examined and settled. For example, records such as travel and expense reports, inter-company invoices, supplier invoices, balance sheets and operating statements are to be retained for a minimum of seven years (C+7). Agreements entered into with governmental authorities may extend this period. Therefore, prior clearance for destruction of tax-related documents must be obtained from The Company Tax Department.

(2) Sales Tax Audits. All Company locations must retain documents which are required for local sales tax audits for the current year and seven years prior (C+7). However, agreements entered into with governmental authorities may extend this period. Likewise, this period may be reduced as a result of audits being finalized. Prior clearance for destruction of such documents must be obtained from The Company Tax Department.

(3) Fixed Assets. Fixed asset ledgers and the documentation of acquisitions (vouchers with support, cancelled checks, inter-company advices, etc.) are to be maintained as part of the permanent records.

B. LITIGATION AND INVESTIGATIONS

All records which are relevant to pending or threatened litigation or to a government investigation must be retained until the termination of the litigation or investigation. Records relating to delinquent customer accounts which foreseeably may require litigation for collection are to be retained until payment has been received or the account has been written off. Prior clearance for destruction of such documents must be obtained from the Company Legal Department.

BUSINESS RECORDS & DOCUMENT RETENTION POLICY

C. STATUTORY AND REGULATORY REQUIREMENTS

Certain specific statutes and government regulations require the retention of documents beyond the normal C+ 1 period. For example, certain states may require agreements to be retained for a period of several years following termination or expiration of the agreement. The Department of Labor, the Department of Transportation and the Equal Employment Opportunity Commission impose specific retention periods for designated categories of documents. Certain governmental clients may have special retention rules which must be followed. Some private customers may have contractual requirements for record retention periods as well. Any questions concerning these special retention requirements are to be referred to the custodian of the contracts with the customer in question.

D. CONTRACTS AND LEASES

As a general rule, contracts and leases are to be kept for six years following the expiration or termination of such documents.

E. CRITICAL CUSTOMER AGREEMENTS AND CORRESPONDENCE

Correspondence that records an understanding established with a customer or that is essential to document an on-going relationship are to be retained for longer than the normal C+1 period. Retention for a longer period, however, should be very selectively applied to only the most critical documents. In some instances, customer-related documents must be retained for longer periods as provided in the customer agreement. Letters which are themselves agreements are to be kept for six years following the expiration or termination of such letter agreements.

F. BILLING RECORDS

Billing records for each branch are to be retained for longer than C+1. Such documents, however, should be kept to a minimum and should be retained only to ensure continued access to necessary statistical data. In some instances, billing records must be retained for longer periods as provided in the customer agreement.

BUSINESS RECORDS &
DOCUMENT RETENTION POLICY

G. PERSONNEL FILES

As a general rule, personnel files are to be retained indefinitely following termination of employment.

H. COMPANY ISSUED POLICY MANUALS

Policy manuals, such as conduct of business and summary plan descriptions for benefits plans, are to be retained indefinitely or until they are updated.

BUSINESS RECORDS &
DOCUMENT RETENTION POLICY

RECORDS RETENTION SCHEDULE

CATEGORY OF MATERIAL **RETENTION PERIOD**

- Accounting and Finance

Annual audited financial statements	Permanent
General ledgers	Current + 10
Annual audit workpapers	Current + 7
Monthly financial statements	Current + 7
Bank statements and cancelled checks	Current + 7
Invoices and trade payables	Current + 7
Physical inventory records	Current + 7
Account reconciliation	Current + 7
Bank reconciliation	Current + 7
Fixed asset information	Current + 7
Journal entries	Current + 7
Annual plans and budgets	Current + 2

- Administrative……Current + 1 year
  - Expense accounts
  - Vacation records

- Agreements……Contract term + 6 years

  Customer contracts, leases,
  licenses, purchase orders, bills of sale,
  loan agreements, confidentiality agreements,
  employment agreements, consulting agreements
  and any other commercial agreements, as well as
  related correspondence.

- Branch Records…… Current + 4 years

  Such as Delivery Sheets, Vault Holdover Sheets,
  Vault Delivery Sheets, Messenger Reports,
  Daily Records of Time in Vault, Special Service Orders,
  Driver's Daily Report, Vault Records, Form 132s,
  Coin Transfer Sheets, Messenger's Guide Sheets

-- BUSINESS RECORDS & DOCUMENT RETENTION POLICY of the companies, RepoSystems.Com Inc, The RepoSystems Group, LLC and Optical Recognition Systems, Inc.

-- Last reviewed 4/10/2014

BUSINESS RECORDS &
DOCUMENT RETENTION POLICY

- Customer Materials

  Workplans, research, presentations and the like……..Current + 1 year (unless otherwise required by customer)

- Employment

  Biographical, salary and bonus information, attendance records, evaluation forms, job descriptions, application forms, termination papers, exit interviews, disciplinary records, Direct Access records, etc.……..Indefinitely

  Personnel records relevant to a discrimination charge or action brought by EEOC or Attorney General ……..Until final disposition of action, or 3 years after the personnel action to which the records relate, whichever is later

  EEO-1 Employer Information Report…….Copy of most recent report at each unit

  Affirmative Action Program and Supporting documentation ……Current + 2 years

  Records pertaining to hiring, assignments, promotion, demotion, transfer, layoff or termination, rates of pay, requests for reasonable accommodation, results of physical examinations, job postings, applications, resumes, Speak Out minutes……..Current + 2 years

  Documents related to compliance with Family Medical Leave Act …….Current + 3 years

- Environmental and Hazardous Substances…….Permanent

- General Corporate Records…….Permanent

  SEC-related materials, incorporation documents, By-laws, qualification to do business records, corporate seals, stock certificates and ledgers, stock transfer records, stockholders records, dividend records, minute books, annual reports, resolutions and proxies.

- Historic Records…….Permanent

  Such as pictures, publications, etc.

-- BUSINESS RECORDS & DOCUMENT RETENTION POLICY of the companies, RepoSystems.Com Inc, The RepoSystems Group, LLC and Optical Recognition Systems, Inc.

-- Last reviewed 4/10/2014

BUSINESS RECORDS &
DOCUMENT RETENTION POLICY

- Immigration……Current + 3 years, or one year after
  INS Form I-9, Employment Eligibility Verification Form — termination of employment, whichever is later

- Insurance Records……...Permanent
  Policies of all kinds, including all risk liability, automobile/general bodily injury, property damage liability, workers compensation and group insurance plans.

  Certificates issued by the Company……Current + 3 years
  Certificates issued to the Company…….Permanent

- Letters and Other Routine Correspondence…….…...Current + 1 year
  Such as transmittal letters, notes of appreciation, letters requiring no acknowledgement or follow-up, letters of inquiry and reply and the like.

- Levies & Garnishments…….…….During period of collection + 1 year

- Litigation documents……As determined by Legal Dept. on a case-by-case basis.
  Including discovery, depositions, pleadings, and related correspondence.

-- BUSINESS RECORDS & DOCUMENT RETENTION POLICY of the companies, RepoSystems.Com Inc, The RepoSystems Group, LLC and Optical Recognition Systems, Inc.

-- Last reviewed 4/10/2014

BUSINESS RECORDS &
DOCUMENT RETENTION POLICY

- Payroll
  - Employee earnings records…….Permanent
  - Payroll registers (gross and net)…….Current + 7 years
  - Unclaimed wage records…….Current + 7 years
  - Employee deduction authorizations……Employment period + 4 years
  - Attachments and garnishments……Payment period + 3 years
  - Time cards and time sheets…….Current + 7 years
  - Cancelled checks……..……Current + 7 years
  - Moving expenses…….Current + 7 years
  - Payroll backup…….Current + 7 years
  - Records containing name, address, DOB, ……..Current + 3 years
    Occupation, rate of pay and weekly compensation

- Pension Plan Documents…….Permanent
  Plan documents and amendments,
  IRS determination letters, records of employee
  service and eligibility, required participant and
  beneficiary information and records of pension paid.

- Pension Plan Filings……Filing date + 6 years
  Including reports of pensions and
  pension plans filed with the IRS or
  the Department of Labor.

- Registrations (Copyright and Trademark)……..Permanent
  including related correspondence.

- Safety Compliance…….As determined by Safety Dept.
  on a case-by-case basis

- Tax Records
  Including income and non-income tax returns……..Current +7 years
  (e.g., income, franchise, property), (Subject to adjustment by
  tax bills, receipts and statements, The Company Tax Dept.)
  work papers, payroll tax records,
  sales and use tax records, excise tax
  and charitable contribution records.

-- BUSINESS RECORDS & DOCUMENT RETENTION POLICY of the companies, RepoSystems.Com Inc, The RepoSystems Group, LLC and Optical Recognition Systems, Inc.

-- Last reviewed 4/10/2014

BUSINESS RECORDS &
DOCUMENT RETENTION POLICY

- Welfare Plan Documents

Employee benefit plans (other than……Full period of plan + 1 year qualified plans)

The nature of the Companies function may require the retention of specific documents beyond the retention periods set forth above where advisable to afford appropriate legal protection to the Company customers.

Accepted by:

Rob Lovelace
CEO
RepoSystems.Com Inc.
The RepoSystems Group, LLC
Optical Recognition Systems, Inc.

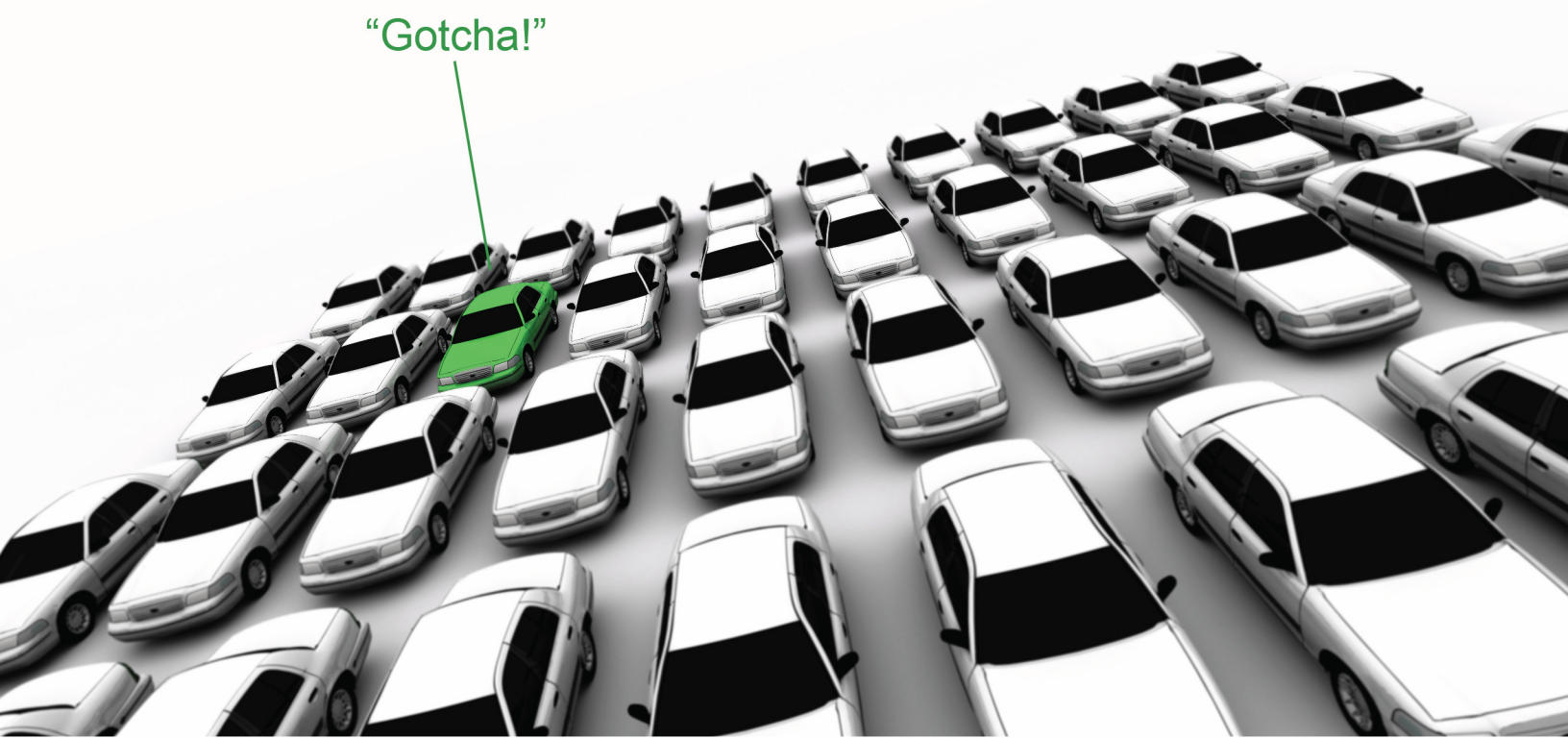
-- BUSINESS RECORDS & DOCUMENT RETENTION POLICY of the companies, RepoSystems.Com Inc, The RepoSystems Group, LLC and Optical Recognition Systems, Inc.

-- Last reviewed 4/10/2014

REPO | SYSTEMS

Facts & Information

Third Party Assessment



Third Party Assessment Questionnaire T2

RepoSystems.Com

4/10/2014

Version control				
Version	**Section(s)**	**Description**	**Date**	**Au.**
1.0		Original Document		

1. Assessment Document

This questionnaire document is used as due diligence of third party vendors. Third parties should complete this and return client.

2. RepoSystems Consumer Contact Information

RepoSystems Customer Business	RepoSystems Com Inc.
Type of Business Relationship	Web application/portal for managing collateral recovery with or without the use of ALPR (Automatic License Plate Recognition)
Type of information to be shared	Company, Customer, Financial
Information share method	RepoSystems.com Website systems, file transfers, email, etc…
Business Unit	Originations, Servicing, etc…

3. Third Party Contact Information

Company Information	
Name of Company	RepoSystems.Com Inc.
Completed by & Title	Rob Lovelace
Primary POC for this document	Rob Lovelace
IT Contact for this business relationship	Rob Lovelace
Date Completed	4/10/2014
Number of employees	10

4. Instructions

Please answer all questions and return to RepoSystems Customer contact listed above. If you have any questions regarding this document please use the contact listed above and they will in-turn have the IT Security Department contact you to clarify.

RepoSystems Customer will follow up with questions if necessary for clarification or further discussion.

5. Questions to be answered by third party

Security Question posed by RepoSystems Customer	Service Provider's Answers
1. Do you have a Safeguard Plan as defined in the Gramm Leach Bliley Act and its applicable regulations?	RepoSystems.com Inc. (RepoSystems.com) Response - Yes
2. Do you perform background screening prior to hiring employees who will have access to NPI? If so, please describe the screening that is performed. Do you hire employees with a criminal record? If so, do they have access to NPI?	RepoSystems.com Inc. Response –Yes. In addition see our hosting providers responses (Peer1 documentation) RepoSystems.com Inc. Response - We do NOT hire employees with a criminal background.

3. Do you have a training program for those who will have access to NPI? If so, please attach or describe the measures that you take to train and manage employees who will have access to NPI (for example, having employees sign a confidentiality agreement, training employees on security practices, limiting access to NPI to employees who have a business reason for seeing it, regularly reminding employees of your securities policies, etc.)	RepoSystems.com Inc. Response – Yes. NDA/confidentiality agreements in place with all employees and contractors. RepoSystems.com Inc. Response -Training is provided in group or individual sessions, generally completed with a G2M (Goto Meeting, or Goto Training) session.
4. Do you share NPI with your affiliates, service providers, vendors or subcontractors? If so, please describe the measures that you take to select and monitor them (for example, checking trade references prior to hiring, having them sign a confidentiality agreement, auditing their security practices and safeguards, etc.)	RepoSystems.com Inc. Response – No information is shared unless requested and approved by clients.
5. Have there been any instances in which your employee or affiliate's employee, your service provider, vendor or subcontractor, or an unauthorized third party has improperly accessed, stolen, altered or destroyed (or attempted to improperly access, steal, alter or destroy) NPI or any other information concerning former or current customers or employees of yours or your other clients? If yes, please describe. If you answered yes to the above question, please describe the measures that you have taken since those instances to prevent such access, theft, alteration or destruction from occurring again.	RepoSystems.com Inc. Response – No theft or breach of any kind.
6. Where do you physically store NPI?	RepoSystems.com Inc. Response – at our hosted facilities through Peer1 Networks.
7. Describe the physical security implemented for access to the building where you retain and/or store NPI? (Proxy card access, Video cameras, Bio-Metrics, etc.)	RepoSystems.com Inc. Response – Physical access to servers is protected by a 2 factor security system. The only individuals allowed into the server room are PEER 1 employees pre-authorized to do work on servers

8. Describe your policy for securing fax transmissions containing NPI (i.e., fax is stored in a secure location, etc.).	RepoSystems.com Inc. Response – Fax Servers are in the secure hosted facility. Only outbound faxing is possible at this time and is encrypted by SSL while on the wire.
9. Describe your policy for disposing of NPI once it is no longer needed for a legitimate business purpose.	RepoSystems.com Inc. Response – this will be dictated by the customer.
10. Describe the password and/or login policy for network, web, database, and email access. Describe how the policies are enforced. How often do these passwords expire? How do you ensure a former employee's password(s) or login is deactivated?	RepoSystems.com Inc. Response – from the application standpoint, we have standard username and password pair. Option, periodical renewal or change of password. Optional 2 Factor Authentication, and Optional IP Address Security. Assurance of an employee's password for a former employee, goes through a 3 step process verification of the removal of the user credentials from our system. From the Peer 1 Hosting Provider perspective: See Marked page 15 of the attached PDF document titled (Peer1_SAS70_Report.pdf)
11. Have any penetration and vulnerability tests been performed for the network? If so, please describe who performs the test, the results of the tests, and the current status of any vulnerability found.	RepoSystems.com Inc. Response – Yes. Peer 1 on our Requests. No Vulnerabilities present.
12. Describe the measures that you take to prevent, detect, and respond to attacks or intrusions upon, or other failures of, your information safeguards (for example, monitoring, or periodically testing the effectiveness of your safeguards, etc.).	RepoSystems.com Inc. Response – Implementing Test procedures from "White Hat" hacker groups and "Penetrating Software" tests, such as Hacker Gaurdian.
13. Provide a schematic or describe the configuration of the organization's DMZ infrastructure. (Firewalls, IDS, IDP, etc)	RepoSystems.com Inc. Response – For the security of RepoSystems.com Inc. PEER 1 and our clients, as outlined by the SAS 70 compliancy regulations, details regarding the PEER 1 internal infrastructure is proprietary and privileged.

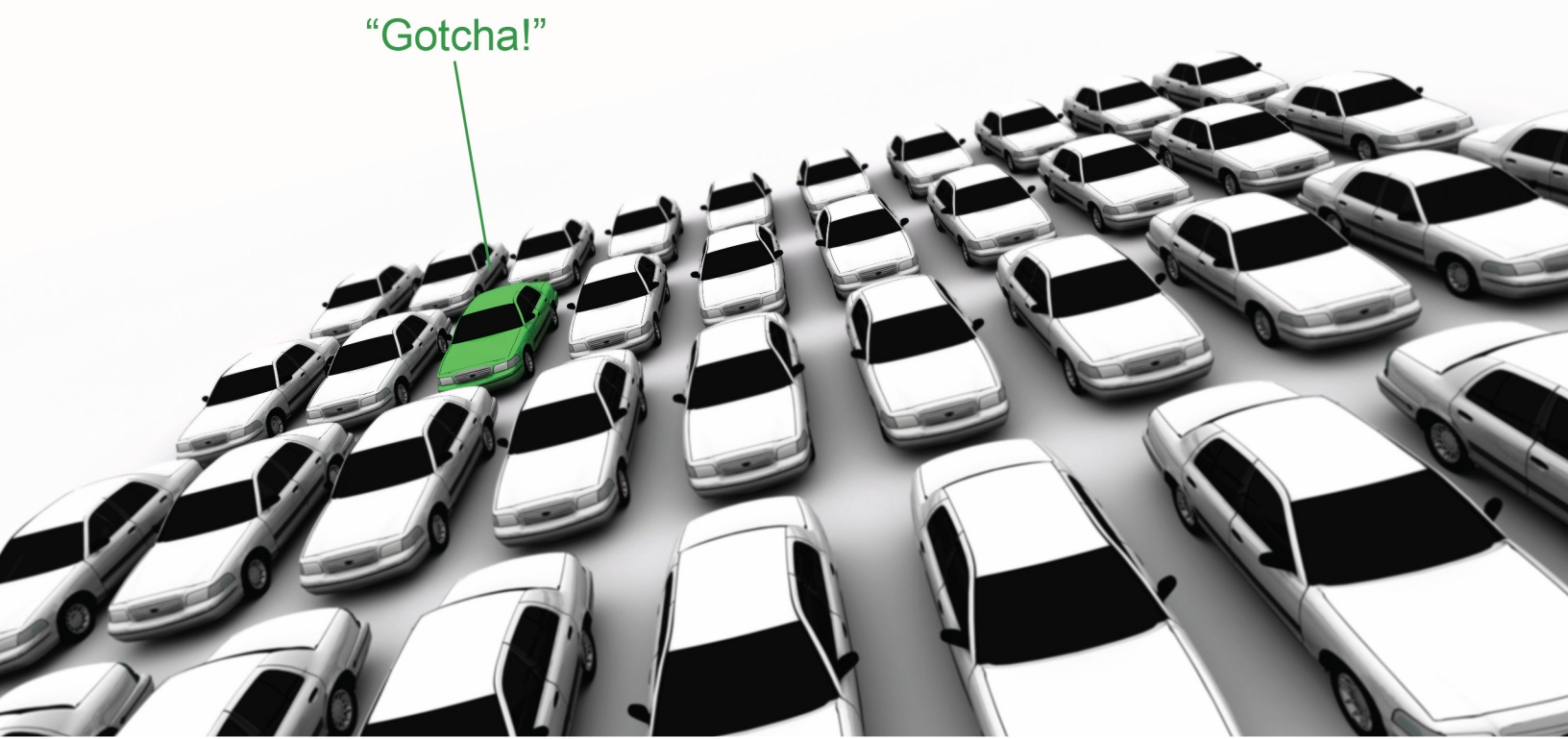
14. Do you have any intrusion prevention or detection systems to monitor network traffic for possible intrusion attacks? If so, please describe the system in place and who monitors the logs.	RepoSystems.com Inc. Response – Yes. Again, For the security of RepoSystems.com Inc. PEER 1 and our clients, as outlined by the SAS 70 compliancy regulations is proprietary and privileged.
15. How is the web application secured? Are the user logins based on individual or groups account access?	RepoSystems.com Inc. Response – Standard SSL 128 bit encryption. All logins are based on an individual profile.
16. How are the databases that contain NPI protected? (Limiting views and access) Is the database monitored for suspicious activity? Is the database utilizing encryption technology?	RepoSystems.com Inc. Response – For the security of RepoSystems.com Inc. PEER 1 and our clients, as outlined by the SAS 70 compliancy regulations is proprietary and privileged. The Database is monitored on 24x7 basis. The application (RepoSystems.Com) provides intrusion algorithms disabling such devices as SQL injection and notifies our support team of any such attempt at intrusion immediately.
17. Do you store NPI on workstations/desktops?	RepoSystems.com Inc. Response – No. None.
18. Describe the physical security built around your server room? (Proxy card access, Video cameras, Bio-Metrics, etc.)	RepoSystems.com Inc. Response – From our Peer1 Hosting providers: All PEER 1 data centers are equipped with government grade proximity badge and biometric scans for entry to secure data center spaces. Mantraps are placed in strategic locations in select data centers. All PEER 1 data centers use 24/7 surveillance cameras on CCTV with a retention cycle of 91 days. Armed guards patrol select PEER 1 data center locations.
19. Are server backup tapes stored on-site or off-site? What are the physical parameters you use to protect the storage of these tapes? Do you utilize tape encrypted?	RepoSystems.com Inc. Response – No offsite storage of any data. All onsite, in house storage, under protected, non Internet accessible computer storage facilities

20. What type of e-mail encryption do you support with outside customers? (Key Exchange, TLS, etc.)	RepoSystems.com Inc. Response – This is Dictated by the customer. Primarily Key Exchange either in conjunction with PGP.
21. Are computer systems protected with anti-virus software? If so, describe the type of anti-virus software used on each system. Describe procedures for updating virus file definitions and type and schedule of scans being performed.	RepoSystems.com Inc. Response – Yes. We use McAfee Viruscan Enterprise on all Windows servers as an optional service. DAT files and software are updated weekly, or more often upon request
22. Are computer systems protected with anti-spam and anti-spy ware software? If so, describe the type of software used on each system. Describe procedures for updating file definitions for the software.	RepoSystems.com Inc. Response – Yes. We use McAfee services on all Windows servers as an optional service Data files and software are updated weekly, or more often upon request
23. Please describe the policy and procedures for keeping the computer systems' operating systems updated with the latest security fixes, patches, and upgrades.	RepoSystems.com Inc. Response – By default, PEER 1 installs OS patches and security Updates on a weekly basis, or as often as requested by the client
24. Do you have any wireless access points for the network? If so, describe the wireless system and what security measures have been implemented for the wireless network (WEP, WPA, 802.11x, etc.).	RepoSystems.com Inc. Response – None at the server level.
25. Do external users connect to the network? If so, are the connections through dial-in or Internet access? Describe procedures that are in place to confirm the identity of external users?	RepoSystems.com Inc. Response – Yes, Access the system through the RepoSystems.com application interface via the Internet.. Standard username password combination. Flags can be set for each user to either be Two Factor and/or IP Security authenticated, through the RepoSystems.com Application.
26. Do you have a disaster recovery plan in place? If so, give a brief description? How often is it tested? When was the last test?	RepoSystems.com Inc. Response – Yes. Once per quarter. Last test 4/10/2014

REPO | SYSTEMS

Facts & Information

Mobile Application Security



REPO SYSTEMS

Our mobile application security for our GPS DNA products is very unique and secure. We do not use the file system on the mobile device therefore any 'hack' or virus cannot attach itself to the file and cause it to be compromised. Essentially there is no "file" to retrieve and or view.

We store the data in virtual memory and is ONLY available to the device while the device is powered on **AND** when the application is in use. When the application "stops" the memory is cleared.

Our encryption process is as follows:

We first reverse the address data then we will take the mode position of that data and divide it into array and store it in virtual memory with an "offset" value. We do not reveal what that "offset" value is.

Once that is done we join the array values taking alternate data from the division and convert the data into baseXX value. Where XX is a value defined within our formula.

We then apply 6 rotations of 128 bit encryption.

For example if the address were 123 AnyStreet, AS 12345 (AS = AnyState), then this is what the encrypted address data looks like if a user attempts to view the virtual memory, "cnJ2LG5tcnAgYWExNmFpdGV0YUFnclAwLzI=".

Viewing virtual memory is extremely difficult or nearly impossible on mobile devices.

The decrypted data is not displayed to the user until they come within the 250 feet of the offset proximity value. The only data displayed is the vehicle information and only a partial VIN.

If the personal information is attempted to be "accessed" by another source OTHER than our application, the memory is completely released, therefore no information is available.

No personal information, i.e. Name, SSN, etc is displayed to the end user, only vehicle information and an "approximate" or "general vicinity" location, for the end user to "locate" or begin looking for the vehicle.

Prior to running through this process all data stored in the RepoSystems environment is secure using methods described in other documentation attached with this documentation.

9400 n. macarthur blvd.
suite 124-409
irving, tx 75063

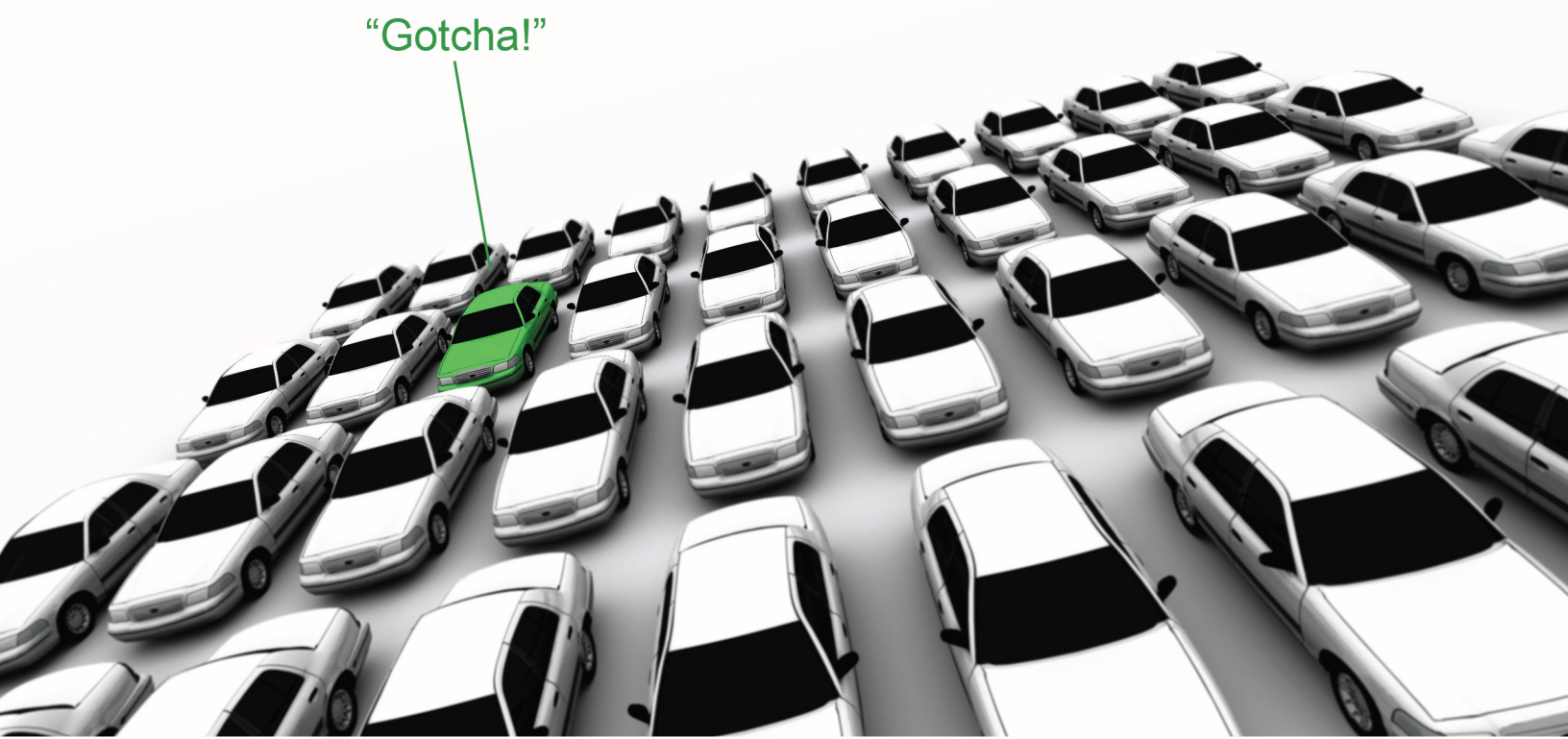
866.906.0573
p. 972.501.0375
f. 214.853.5327

reposystems.com

REPO | SYSTEMS

Facts & Information

System Breach Notification



System Breach Notification Policy

Introduction:

Reposystems.Com Inc, The RepoSystems Group, LLC and Optical Recognition Systems, Inc., hereinafter referred to as the "Company", shall provide timely and appropriate notice to affected individuals or entities when there is reasonable belief that a breach in the security of private information has occurred. A breach in security is defined as an unauthorized acquisition of information, typically maintained in an electronic format by the Company.

Scope:

Attacks on the Company IT resources are infractions of the LICENSE AGREEMENT, TERMS OF USE AND NON-DISCLOSURE AGREEMENT constituting misuse, or they may be vandalism or other criminal behavior. Reporting information security breaches occurring on the system and/or on the network to appropriate authorities is a requirement of all persons affiliated with the Company in any capacity, including employees, contractors, portal users, physical visitors and/or electronic visitors.

Policy Statement:

Suspected or confirmed information security breaches must be reported to the Company authorities. A message may be sent to support@reposystems.com or by calling 972.501.0375 x1004.

The Company will investigate the report, and if a security breach of private and/or highly sensitive information may have occurred, will inform all appropriate parties.

In the event that a public notification of the security breach may be warranted, the Company will consult with the appropriate management and law enforcement officials and make the final determination if a public notification of the event is warranted.

Procedures:

The entity responsible for support of the system or network under attack is expected to:

- Report the attack to the responsible parties
- Block or prevent escalation of the attack, if possible
- Follow instructions communicated from the parties in subsequent investigation of the incident and preservation of evidence
- Implement recommendations from the Company
- Repair the resultant damage to the system

System Breach Notification Policy

Internal Notifications:

The Company IT Security Officer will report serious computer security breaches to the Chief Information Officer (CIO) in a timely manner. The CIO will consult with one or more advisors as appropriate, and decide if a Critical Incident Management Team must be convened to determine a response strategy, or if an alternate group is appropriate for the response. This determination may be made prior to completion of the investigation of the security breach.

The Company affiliates or associates will report the incident to the authorities when, based on preliminary investigation, criminal activity has taken place and/or when the incident originated from a foreign (to the Company) computer or network.

Determination of External Notification:

To determine if unencrypted private or highly sensitive information has been acquired, or is reasonably believed to have been acquired by an unauthorized person, the (likelihood of the) following will be considered:

- Physical possession (lost or stolen device?)
- Credible evidence the information was copied/removed
- Length of time between intrusion and detection
- Purpose of the intrusion was acquisition of information
- Credible evidence the information was in a useable format
- Ability to reach the affected individuals
- Applicable company policy, and/or local, state, or federal laws

External Notification:

If it is determined that an external notification to the affected individuals is warranted, the following procedures will apply:

Written notice will be provided to the affected individuals using US Mail, unless the cost is excessive or insufficient contact information exists. The letter will be developed by the Company responsible for the system experiencing the breach, and approved by the CEO and others as appropriate. The excessiveness of cost consideration will be the decision of the CEO, CIO and General Counsel.

If written notice to the affected individuals is not feasible, the following methods will be considered for providing notice:

- Personal e-mail notices (provided addresses are available), developed by CEO, CIO and General Counsel.
- All expenses associated with external notification will be the responsibility of the entity that experienced the security breach.

-- System Breach Notification Policy of the companies, RepoSystems.Com Inc, The RepoSystems Group, LLC and Optical Recognition Systems, Inc.

-- Last reviewed 4/10/2014

System Breach Notification Policy

Definitions:

Private Information -- If the information acquired includes a name (first and last name or first initial and last name) in combination with any of the following, and the information was not in an encrypted format, a public notification may be warranted:

- Social security number
- Driver's license Number
- Bank Account, Credit, or Debit Card Account number with security, access, PIN, or password that would permit access to the account
- Personal information that is publicly and lawfully available to the general public, such as address, phone number, and email address are not considered private information for the purposes of this policy.

Highly Sensitive Information -- If the information acquired is of a very sensitive, confidential, or proprietary nature, the security breach will be investigated and the CEO, CIO and General Counsel will determine if a public notification is warranted. Examples of highly sensitive information include but are not limited to:

- Name, Address, with Date of Birth
- Records protected by FERPA, HIPAA, GLBA, or other applicable federal laws and regulations
- Research data or results prior to publication or filing of a patent application
- Information subject to contractual confidentiality provisions
- Security codes, combinations, or passwords

Accepted by:

Rob Lovelace
CEO
RepoSystems.Com Inc.
The RepoSystems Group, LLC
Optical Recognition Systems, Inc.

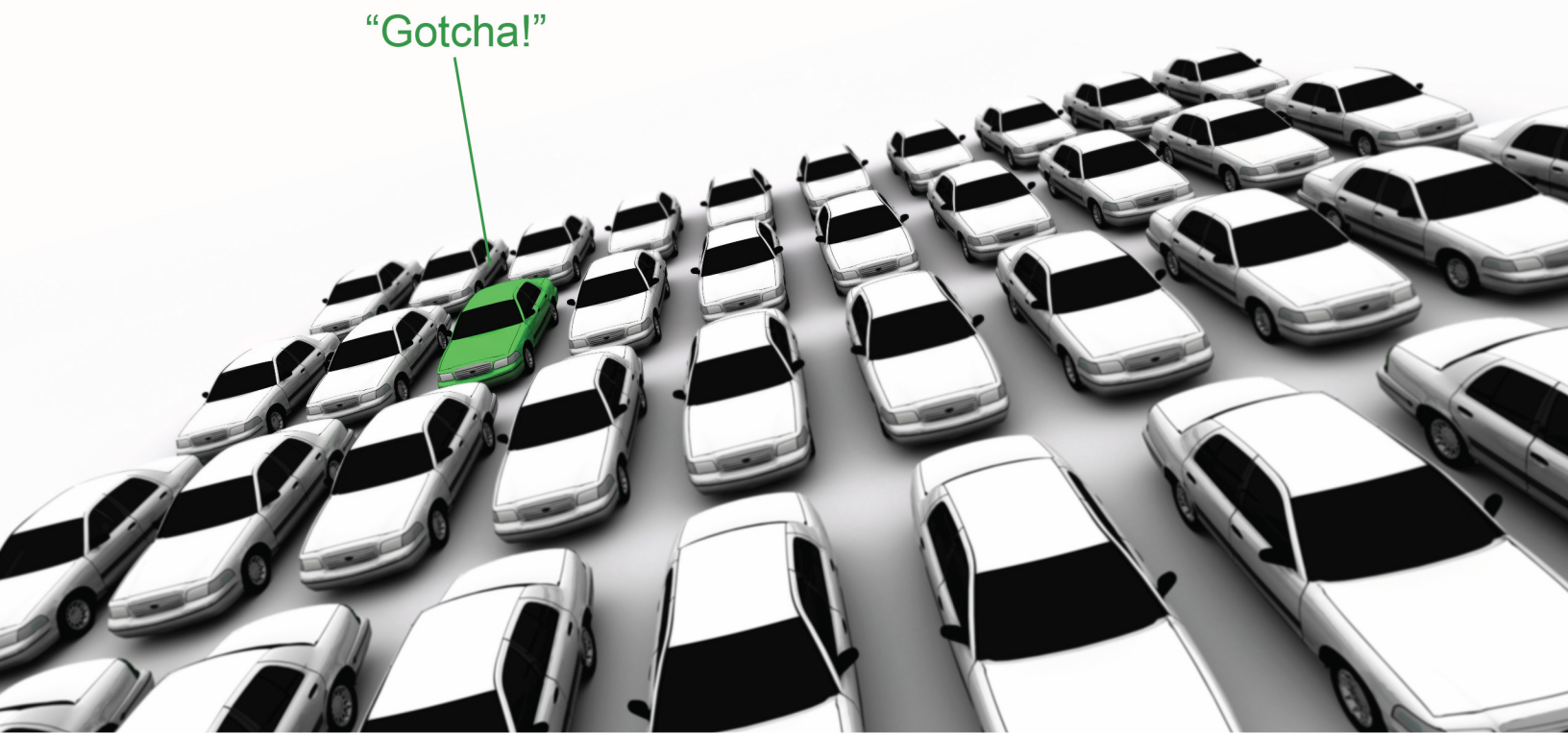
-- System Breach Notification Policy of the companies, RepoSystems.Com Inc, The RepoSystems Group, LLC and Optical Recognition Systems, Inc.

-- Last reviewed 4/10/2014

REPO | SYSTEMS

Facts & Information

Hosting Provider
Security Questionnaire Responses



Physical Security and Facility Info	
Question	PEER 1 Response
Does PEER 1 have any physical security measures in place?	All PEER 1 data centers are equipped with government-grade proximity badge and biometric scans for entry to secure data center spaces. Mantraps are placed in strategic locations in select data centers.
Are any recording devices used at PEER 1?	All PEER 1 data centers use 24/7 surveillance cameras on CCTV with a retention cycle of 91 days.
Are direct modem dial-in or POTS lines permitted?	These services are not provided or allowed in PEER 1 Managed Hosting, but may be available for PEER 1 colocation.
Are PEER 1 facilities patrolled by security guards?	Yes, armed guards patrol select PEER 1 data center locations.
Describe the fire suppression and climate control.	PEER 1 data centers are built on raised floor with redundant climate control systems. All facilities use either FM-200 gas or Energen gas with dry pipes.
What type of power backup is used?	All P1MH facilities are equipped with diesel generators for backup power and N+1 UPS systems. The generator size and redundancy may vary by location, but maintain a minimum 7 days of power without grid assistance.

Network Security	
Question	PEER 1 Response
Does PEER 1 maintain network diagrams that depict the current network security infrastructure and the application infrastructure?	Yes. However, for the security of PEER 1 and our clients, as outlined by the SAS 70 compliancy regulations, details regarding the PEER 1 internal infrastructure is proprietary and privileged.
Does PEER 1 have/provide Internet access?	Yes. All PEER 1 data centers have redundant OC192 fiber connections to multiple Tier 1 internet providers, as well as over 500 peering relationships to other carriers through the PEER 1 SuperNetwork. See also: http://www.peer1.com/infrastructure/network.php
Do you allow remote access to your internal network?	Yes, through multiple proprietary authentication methods via encrypted tunnels.
Does PEER 1 implement wireless (wi-fi) networks?	No. PEER 1 does not provide or utilize WAPs, nor do we scan the perimeter of our data centers for rogue WAP devices.
Can PEER 1 facilitate encryption and two-factor authentication for network access when deemed appropriate?	Yes. IPSec VPN tunnels are permitted on any dedicated firewall device.
Does PEER 1 have a DMZ infrastructure?	Yes. Any PEER 1 facility which allows guests to use an internet connection will have Trust and DMZ policies in place to restrict access to the PEER 1 intranet.
Please describe PEER 1's documented security standards and audit procedures for customer network security to ensure customers cannot compromise PEER 1's network back bone.	Please see our SAS 70 compliancy document for further details regarding network security.
Does PEER 1 implement IDS/IPS?	Yes. However, for the security of PEER 1 and our clients, as outlined by the SAS 70 compliancy regulations, details regarding the PEER 1 internal infrastructure is proprietary and privileged.
Are critical systems (i.e. Network switches and/or Firewalls) located in a secure environment?	Yes. All PEER 1 networking gear is within the physical datacenter environments owned and operated by PEER 1.

General Security and Compliance	
Question	PEER 1 Response
We need the ability to perform our own vulnerability assessments against this system. Is the approval for this written into an SLA or Contract?	As you will have full administrative rights, PEER 1 does not have any issues with you running your own vulnerability assessment against your managed server as long as the scan does not adversely impact other PEER 1 customers.
What kind of reporting is provided for the vulnerability assessments, what tools are utilized and who performs the scanning?	PEER 1 provides a vulnerability scan service powered by Control Scan which runs every two weeks. You will receive email notifications once the report is ready for you to login to the portal and view it. This service is included with your managed host plan.
Does PEER 1 follow the OWASP criteria for application development?	N/A. PEER 1 does not provide application development services.
Does PEER 1 implement proactive processes or measures other than IDS to protect against attacks?	Yes. However, for the security of PEER 1 and our clients, as outlined by the SAS 70 compliancy regulations, details regarding the PEER 1 internal infrastructure is proprietary and privileged.
Does PEER 1 have a business continuity or disaster recovery plan in place?	Yes. However, the PEER 1 disaster recovery plans do not directly coincide with customer-facing servers. Each client is responsible for their own business continuity and disastery recovery for servers housed in PEER 1 data centers.
Does PEER 1 have documented physical security standards and processes?	Yes; please see our SAS 70 compliancy documentation.
Is PEER 1 REQUIRED to comply with Sarbanes-Oxley section 404 and 406?	Yes; please see our SAS 70 compliancy documentation.
Are your security policies based on ISO-17799 /BS7799/ISO-27000 series?	Not in all instances, however ISO and CobiT standards are used when applicable; please see our SAS 70 compliancy documentation.
Describe status of compliance with additional applicable regional customer privacy regulations (international, state, etc.) and standards based compliance assessments or certifications.	SAS 70 Type I audit completed June 30, 2009. SAS 70 Type II audit pending completion mid-2010. Compliant with Canadian Bill 198.
Does PEER 1 protect the network from Trojan horses, malware, and other forms of malicious code?	PEER 1 provides security services, including hardware firewalls, vulnerability scans, and antivirus software. PEER 1 also actively monitors the network 24x7x365 for abnormal traffic patterns that may indicate malicious activity.

Firewalls	
Question	PEER 1 Response
Is there no firewall in place if we choose not to get one? How do you protect servers without firewalls that sit in the data center next to our servers?	Every client has the option of whether or not to be protected by a firewall. Attacks on one client will not be permitted to effect other clients on the PEER 1 network.
What happens when the firewall's session limit is reached?	After the session limit is reached, further connections will be rejected (IE: Connection Unavailable error message).
What does the 70mbps (160mbps, 350mbps) refer to?	Total aggregate throughput allowed for all servers protected by that firewall.
Who is responsible for patching the firewall appliance?	All Juniper dedicated firewalls are fully managed and maintained by PEER 1's support and networking teams.
Do we have access to manage the firewall? What if we need ports opened for our application?	PEER 1 will fully manage the firewall. To have additional ports opened, you may contact support, available 24x7.
Do the firewalls protecting the Third Party network generate logs?	Yes. However, logs from the PEER 1 internal firewalls are considered proprietary and priviliged. Clients will only be granted access to logs from their own dedicated, leased firewalls.
Are all the Firewalls used by the Third Party ICSA Certified?	This is determined by the type of firewall leased by the client. For detailed certification information, please see the Juniper website at http://juniper.net or the ICSA website at http://icsalabs.com
Please list the PEER 1 firewalls and versions currently used.	Juniper Netscreen, Juniper SSG; ScreenOS v6.x
Please provide a generic overview of firewall policies and/or rulesets.	PEER 1 employs a default ruleset which may be customized and modified based on each client's requirements. The default policies restrict access to only the most commonly utilized ports such as SSH, RDP, HTTP, HTTPS, DNS, POP, and SMTP.
Does the Third Party have documented firewall administrative / maintenance procedures?	Yes. All PEER 1 Network Operations and System Administrator personnel have the skills and access required to modify and maintain firewall policies and code.

Bandwidth	
Question	PEER 1 Response
What switch speed is the server on? 10/100/1000Mbps?	100Mbps by default, with optional upgrades to 1000Mbps.
What is the cost of exceeding the 1,000GB per month transfer? How is that measured?	All inbound and outbound data packets are monitored at the edge routers which provide your servers public network connection. You may access the bandwidth reports via the customer support portal.
Can we eliminate the transfer limit and go on a dedicated internet connection, all you can eat transfer rate?	PEER 1 does not provide an "a la carte" or 95th percentile bandwidth system for Managed Hosting at this time.
Does PEER 1 have a Privacy Policy that complies with regulatory requirements regarding Personal Identifiable Information? Are PEER 1 employees regulated?	Yes. All PEER 1 employees must submit to background checks and sign a strict confidentiality agreement, including but not limited to client data, passwords, and proprietary information.

Software	
Question	PEER 1 Response
Why is there a monthly charge for Plesk?	This is a requirement set forth by Parallels for Plesk resellers; Plesk has been implemented with a low monthly recurring cost versus a one-time fee.
Do we install our own MySQL/MS SQL or is one provided?	MySQL is provided on all RHEL4 and RHEL5 servers by default. PEER 1 does not provide MySQL support on Windows at this time. Licenses for MS SQL on Windows are charged per processor, or you may install your own.
Do we install our own libraries?	A list of provided libraries is available, and you will have root administrative access to the server to install any 3rd party software.
Does PEER 1 have active anti-virus software running with the current updates?	Yes. PEER 1 provides McAfee Viruscan Enterprise on all Windows servers as an optional service. DAT files and software are updated weekly, or more often upon request.

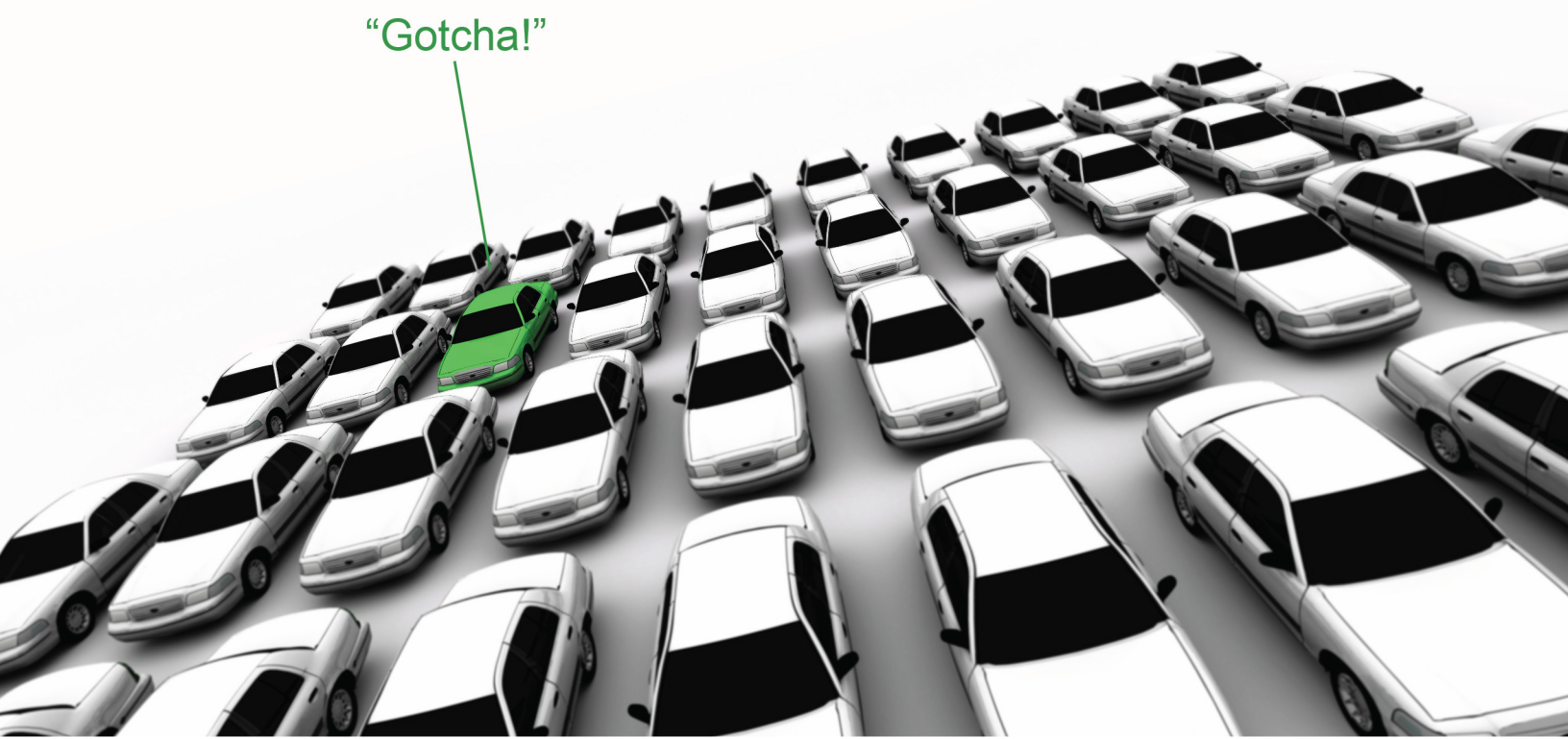
Servers	
Question	PEER 1 Response
What level of access will we have to the Operating System? How do we get access?	You have full Remote Desktop (RDP) access with administrator rights on Windows. You will have full SSH access with root privileges on Linux.
Can we add more RAM? How much is that?	The amount of total RAM allowed is based on the host plan. Several PEER 1 managed hosting plans allow for RAM scaling up to 128gb.
Can we add more hard drive space to the same server? Cost?	1U servers hold only 2 hard drives and therefore can not be expanded upon. 2U servers can hold up to 6 drives. Space can easily be added in a RAID 5 or RAID 10 array; however, the maximum in a RAID 1 is 2 drives.
Does PEER 1 require two-factor authentication for administrative control?	PEER 1 has developed patented technology known as SmartKey, which allows PEER 1 administrators to access managed servers via two-factor authentication. Customers may opt out of this service as necessary.
Has PEER 1 implemented documented security standards regarding server OS hardening?	Yes. PEER 1 does have security standards regarding OS hardening which include but are not limited to: Not using vendor-supplied crentials, disabling unnecessary services, bringing servers to current patch levels, and adding security services such as monitoring and antivirus where applicable.
Where is this server located geographically?	PEER 1 can provide managed hosting in Atlanta, Miami, Fremont, and London. For a list of all available data center, please see http://www.peer1.com/infrastructure/data_centers.php.

Patching and Maintenance	
Question	PEER 1 Response
Who is responsible for configuring and patching the operating system and applicable applications/services that are hosted on the server?	By default, PEER 1 installs OS patches and security updates. You may opt-out of this service at any time.
Is there a documented monitoring process for performance and capacity requirements to identify potential problems/bottlenecks?	PEER 1 can offer advanced monitoring applications to assist in identifying issues related to performance. These services are capable of monitoring over 10,000 metrics related to system and network resources, application availability, and synthetic web transactions. Stress testing services are also available.
Please describe the PEER 1 vulnerability patch management process.	PEER 1 provides managed, automated patching services for all servers regardless of OS. PEER 1 maintains an internal respository of updates from each OS vendor. These updates are tested on an internal environment to ensure hardware driver compatibility. Non-critical updates are enforced once a month during regular maintenance windows; critical updates are pushed out as needed.
What is your scheduled maintenance period?	2:00am - 6:00am Eastern, second Tuesday of each month.

REPO | SYSTEMS

Facts & Information

Hosting Provider
SAS70 Audit Report



PING & PEOPLE

PEER 1 Hosting

Report on Controls Placed in Operation and Tests of Operating Effectiveness
For the period July 1, 2012 - June 30, 2013

July 26, 2013

NONDISCLOSURE AGREEMENT

In consideration for the disclosure by PEER 1 Network Enterprise Inc., PEER 1 Network (USA) Inc., and PEER 1 (UK) Ltd. (collectively referred to as PEER 1 Hosting) of the ISAE 3402, SSAE 16 and CSAE 3416 reports (the Report) as of July 26, 2013 and the confidential information contained therein (the Proprietary Material), the respective customers whose financial information reporting processes and controls include those of PEER1 Hosting and independent auditors of the aforementioned, (collectively, the users) agree that the Proprietary Material is, and shall at all times, remain the property of PEER 1 Hosting and shall be used solely by the users for the purposes described in your agreement with PEER 1 Hosting. Use of Proprietary Material for the benefit of parties other than the intended users is prohibited. The users may not copy, reproduce, sell, assign, license, market, transfer, or otherwise dispose of or give the Proprietary Material to any person, firm, corporation, or other entity. The users shall keep the Proprietary Material confidential and shall not disclose the Proprietary Material to another party without first obtaining written permission from a duly authorized officer of PEER 1 Hosting. The users shall restrict use of Proprietary Material to its employees who are involved in the evaluation of the Proprietary Material.

Table of Contents

Deloitte.

SECTION 1 – INDEPENDENT SERVICE AUDITORS' REPORT (SSAE 16, ISAE 3402 and CSAE 3416)

To the management of PEER 1 Network Enterprise Inc. (including PEER 1 Network (USA) Inc., and PEER 1 (UK) Ltd. and collectively referred to as "PEER 1 Hosting"):

Scope

We have been engaged to report on PEER 1 Hosting description of the system related to managed hosting services, dedicated hosting services and colocation services provided at the Miami, Atlanta, San Antonio, Los Angeles, Virginia, Toronto (Pullman location), Vancouver, and Portsmouth data centers to PEER 1 Hosting's user entities throughout the period July 1, 2012 to June 30, 2013 (the "description"), and the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description. The description indicates certain control objectives specified in the description can be achieved only if complementary user entity controls contemplated in the design of PEER 1 Hosting's controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

PEER 1 Hosting uses various third party service providers ("subservice organizations") to support their operations and activities including the following:

- BackCheck, to conduct background checks for PEER 1 Hosting's employees and contractors in Canada and the United Kingdom throughout the period July 1, 2012 to December 31, 2012.
- ADP, to conduct background checks for PEER 1 Hosting's employees and contractors in the United States throughout the period July 1, 2012 to December 31, 2012.
- Talentwise, to conduct background checks for PEER 1 Hosting's employees and contractors globally throughout the period December 1, 2012 to June 30, 2013.
- eVolve DC Solutions (eVolve), to provide datacenter monitoring and maintenance services to data centers in Miami, Atlanta, Toronto (Pullman location), Virginia, San Antonio and Portsmouth.
- Polaris Realty as the owner of the Vancouver data center facility, whereby Polaris Realty provides datacenter maintenance and environmental monitoring services at that facility.
- Digital Realty Trust, Inc. (Digital Realty) as the owner of the Los Angeles datacenter facility, whereby Digital Realty provides datacenter maintenance and environmental monitoring services at that facility.

PEER 1 Hosting's control objectives and related controls, which are listed in Section 2, include only the control objectives and related controls of PEER 1 Hosting and exclude the control objectives and related controls of these subservice organizations. Our engagement did not extend to controls of the subservice organizations.

Service Organization's Responsibilities

In Section 2 of this report, PEER 1 Hosting has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. PEER 1 Hosting is responsible for preparing the description and for the assertion, including the completeness, accuracy, and method of presentation of the description and the assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria, and designing, implementing, and documenting controls to achieve the related control objectives stated in the description.

Deloitte.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our procedures. We conducted our engagement in accordance with International Standard on Assurance Engagements 3402. "Assurance Reports on Controls at a Service Organization" issued by the International Auditing and Assurance Standards Board, Statement on Standards for Attestation Engagement (SSAE) No. 16. "Reporting on Controls at a Service Organization" and Canadian Standard on Assurance Engagements (CSAE) No. 3416 "Reporting on Controls at a Service Organization".. Those standards require that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period July 1, 2012 to June 30, 2013.

An assurance engagement to report on the description, design and operating effectiveness of controls at a service organization involves performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives stated in the description. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization and described in Section 2. 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, controls at a service organization may not prevent, or detect and correct, all errors or omissions in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives is subject to the risk that controls at a service organization may become inadequate or fail.

Basis for Qualified Opinion

PEER 1 Hosting states in its description that it conducts background checks, which generally consist of an education check, confirming of prior employment and criminal record check (where it is feasible and permitted by the local jurisdictions) prior to granting access to PEER 1 Hosting's corporate network to new hires, including both employees and contractors, (control 2.1). However, as noted in the description of tests of controls and results thereof in Section 3 (control 2.1), background checks were not consistently performed for contractors throughout the period July 1, 2012 to May 12, 2013. As a result, controls were not operating effectively to achieve the control objective: "Controls provide reasonable assurance that policies and procedures are in place to support the hiring and development of personnel." for contractors throughout the period July 1, 2012 to May 12, 2013. PEER 1 Hosting implemented a change to the process of performing background checks for contractors as of May 12, 2013, and our tests noted no exceptions throughout the period May 13, 2013, to June 30, 2013.

PEER 1 Hosting states in its description that it disposes of or removes customer data upon service de-provisioning (control 9.5). However, as noted in the description of tests of controls and results thereof in Section 3 (control 9.5), we noted certain instances where decommissioned hard drives were labeled for de-provisioning and stored in the secured data centers for data erasure at a future date as required by PEER 1Hosting's policies.

Deloitte.

However, those hard drives had not been erased at the time of our testing. As a result, controls were not operating effectively to achieve the control objective, "Controls provide reasonable assurance that data backup and recovery processes are defined and managed consistent with backup and retention plans and schedules".

Opinion

In our opinion, except for the matters described in the preceding paragraphs, and based on the criteria described in the PEER 1 Hosting's assertion in Section 2, in all material respects, based on the criteria described in PEER 1 Hosting's assertion in Section 2 of this report:

a. the description fairly presents the managed hosting services, dedicated hosting services and colocation services provided to PEER 1 Hosting's user entities that were designed and implemented throughout the period July 1, 2012 to June 30, 2013.
b. the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period July 1, 2012 to June 30, 2013, and user entities applied the complementary user entity controls contemplated in the design of PEER 1 Hosting's controls throughout the period July 1, 2012 to June 30, 2013.
c. the controls tested, which together with the complementary user entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period July 1, 2012 to June 30, 2013.

Description of Tests of Controls

The specific controls tested and the nature, timing, and results of those tests are listed in Section 3 of the report.

Restricted Use

This report, including the description of tests of controls, and results thereof in Section 3 of the report are intended solely for the information and use of PEER 1 Hosting, user entities of PEER 1 Hosting's managed hosting, dedicated hosting and colocation services during some or all of the period July 1, 2012 to June 30, 2013, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

Deloitte LLP

DELOITTE LLP
Chartered Accountants
Vancouver, BC, Canada
July 26, 2013

SECTION 2 – DESCRIPTION OF CONTROLS PROVIDED BY PEER 1 HOSTING

MANAGEMENT ASSERTION

We have prepared the description of the system related to managed hosting services, dedicated hosting services and co-location services provided at the Miami, Atlanta, San Antonio, Los Angeles, Virginia, Toronto (Pullman location), Vancouver, and Portsmouth data centers of PEER 1 Hosting for user entities of the system during some or all of the period July 1, 2012 to June 30, 2013 and their user auditors who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when obtaining an understanding of user entities' information and communication systems relevant to financial reporting. We confirm, to the best of our knowledge and belief, that:

1) The description fairly presents the hosting and network system made available to user entities of the managed hosting, dedicated hosting and colocation services during some or all of the period July 1, 2012 to June 30, 2013.The description includes only the controls and related control objectives of PEER 1 Hosting and excludes the control objectives and related controls of sub-service providers. The criteria we used in making this assertion were that the description:
    a) Presents how the system made available to user entities of the system was designed and implemented, including:
        i. The types of hosting and network services provided;
        ii. The procedures, within both automated and manual systems, by which those services are initiated, authorized, documented, processed, corrected as necessary within the company;
        iii. Specified control objectives and controls designed to achieve those objectives;
        iv. Other aspects of our control environment, risk assessment process, information and communication systems, control activities and monitoring controls that are relevant to providing hosting services to user entities of the system.
    b) Does not omit or distort information relevant to the scope of the PEER 1 Hosting services being described, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and the independent auditors of those user entities, and may not, therefore, include every aspect of the PEER 1 Hosting services that each individual user entity of the system and its auditor may consider important in its own particular environment.

2) The description includes relevant details of changes to PEER 1 Hosting's system during the period covered by the description when the description covers a period of time.

3) The controls related to the control objectives stated in the description, (except those noted below) were suitably designed and operated effectively throughout the period July 1, 2012 to June 30, 2013 to achieve those control objectives. The criteria we used in making this assertion were that:
    a) The risks that threatened achievement of the control objectives stated in the description have been identified by the service organization;
    b) The controls identified in the description would, if operated as described, provide reasonable assurance that those risks would not prevent the stated control objectives stated in the description from being achieved; and
    c) The controls were consistently applied as designed, including that manual controls were applied by individuals who have the appropriate competence and authority.

In connection with this audit, Deloitte identified deficiencies with the operation of certain control activities that have resulted in controls not operating effectively to achieve the following two specific control objectives identified in Section 3 of this report.

a) Control objective #2: Controls provide reasonable assurance that policies and procedures are in place to support the hiring and development of personnel.
b) Control objective #9: Controls provide reasonable assurance that data backup and recovery processes are defined and managed consistent with backup and retention plans and schedules.

As reflected in our management responses in Section 3, PEER 1 Hosting is committed to continuously improve our control environment and we have directed the necessary attention and resources to resolving these findings.

Ted Smith
Senior VP, Operation
PEER 1 Hosting
July 26, 2013

GLOSSARY

ACL	Access Control List
ACS	Access Control System
ASHRAE	American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CPU	Central Processing Unit
CSAE	Canadian Standard on Assurance Engagements
CVS	Configuration Version Control
DCO	Data Center Operations
HUB	PEER 1 Hosting's internal website
HVAC	Heating, Ventilation, and Air Conditioning
Hypeerion	PEER 1 Hosting's alert system
IDS	Intrusion Detection Systems
IP	Internet Protocol
IPSEC	Internet Protocol Security
ISAE	The International Standard on Assurance Engagements
ISIS	Intermediate System-to-Intermediate System
IT	Information Technology
JIRA	PEER 1 Hosting's Ticketing System
LAN	Local Area Network
LDP	Label Distribution Protocol
LLDP	Link Layer Discovery Protocol
NDA	Nondisclosure Agreement
NOC	Network Operations Center
Ocean	PEER 1 Hosting's Internal Client Management System
OSPE	Open Shortest Path First
PDU	Power Distribution Unit
P2P	Point to Point
QA	Quality Assurance
QE	Quality Engineering
RANCID	Really Awesome New Cisco Config Differ
RT	PEER 1 Hosting's Ticket Database
RTSP	Real Time Streaming Protocol
SAN	Storage Area Network
SNMPc	Simple Network Management Protocol
SSAE	Statement on Standards for Attestation Engagements
SSL	Secure Socket Layer
TACACS	Terminal Access Controller Access Control System
TSM	Tivoli Storage Manager
UPS	Uninterrupted Power System
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

COMPANY OVERVIEW

PEER 1 Hosting is an Internet infrastructure provider, delivering managed hosting, dedicated hosting, colocation, cloud hosting and network services through 19 data centers and 9 colocation facilities across North America and Europe, all connected together by the company's own Internet Protocol (IP) backbone network. PEER 1 Hosting has established 21 network points-of-presence, with multiple points-of-presence in a single city in some cases. PEER 1 Hosting is a full solution provider and the services are designed to enable customers to focus on their businesses rather than the complexities of maintaining or expanding their Internet infrastructure.

PEER 1 Hosting's principal target market is small and medium-sized businesses whose activities are increasingly dependent upon the Internet. To effectively compete, this target market has become reliant on sophisticated Internet infrastructure that, in the past, has been typically deployed at larger enterprises. However, managing, monitoring, administering, and maintaining a sophisticated Internet infrastructure can rapidly deplete the limited resources of small and medium-sized businesses which need to be directed at core business activities.

Managed hosting is an arrangement with a customer in which PEER 1 Hosting provides the customer with the use of server and related technology and a collection of services designed to ensure the proper management of that technology. These services and technology include the following:

- Data backup and recovery solutions designed to make backups and restorations faster and more flexible with minimal customer impact.
- Firewall technology to protect servers against online exploitation. Firewalls are customized in accordance with customer objectives.
- Dedicated switches and devices that provide a private communication link between servers and assisting the customers in managing their bandwidth consumption.
- Intrusion detection, log monitoring, SSL certificates, and vulnerability scanning services to satisfy customer demands for real-time and periodic server security audits.
- Advance system monitoring services to enable customers to address potential problems.
- Load balancing services that enable customers to better handle high traffic loads.
- Caching system that directs the customers' clients to the nearest caching server or node, allowing for faster delivery of web content that is possible without caching.
- Advanced database administration and clustering services to enable customers to design and maintain highly available database architectures.
- VMware virtualization to enable customers to implement disaster recovery and private clouds.

Dedicated hosting arrangements offered under the ServerBeach brand are substantially similar to managed hosting arrangements except that customers manage and administer their own servers. The services provided to dedicated hosting customers take the form of automated tools to facilitate the provisioning of server solutions. This includes:

- RapidReboot to enable customers to remotely restart their servers, eliminating the need for an on-site technician to manually re-start them.
- RapidRescue to enable servers running the Linux operating system to be rescued by the customers from potentially fatal errors. Customers can recover and repair corrupted file systems, gain immediate access to the server, and boot the server into rescue mode without the assistance of an on-site technician.
- Backup technology to enable customers to back up their critical data on a separate device.
- Control panel technology designed to simplify and automate the management and administration of web sites.

- Various options for port speed and bandwidth allotment that can be tailored to meet the requirements of each customer.
- Private network technology that allows customers to communicate between their website, database and other servers internally without going over the public internet.

Colocation arrangements are substantially similar to dedicated hosting except that colocation customers own the server and technology which they house on PEER 1 Hosting premises in order to access PEER 1 Hosting's high quality infrastructure, large bandwidth capacity, redundant power supply, security and technical support. This type of arrangement also enables customers to easily increase their internet-related aspects of their business with minimal disruption. PEER 1 Hosting's colocation services include the following:

- Customer domain names are hosted on a fully redundant distributed environment providing the customer with fast performance and reliable uptime over the internet.
- Port monitoring services enable customers to define their minimum and maximum thresholds for bandwidth and packets per second usage and receive email alerts once the threshold has been reached. This service enable customers to better manage network costs and alert customers of reductions in traffic to their sites due to server crash, hardware failure or web site configuration issues.
- Convenient, secure browser-based access to servers located on PEER 1 Hosting premises, allowing customers to remotely repair server problems. This device allows the remote installation of operating systems and server troubleshooting.
- Load balancing services that enable customers to better handle high traffic loads by adding more servers to server farms as they are needed and removing them when they are no longer needed.
- Protection of customers' online presence to minimize the impact on operations.

PEER 1 Hosting is divided into departments that promote segregation of duties and responsibility for specific functions within the organization. Departmental oversight is provided by the Executive Management Team (Executive Management) which is comprised of the President and Chief Executive Officer, Chief Financial Officer and Executive Vice President, Senior Vice Presidents and Vice Presidents assigned to each of the functional departments.

PEER 1 Hosting employ staff located in Canada, the United States, and the United Kingdom. The organizational structure represents diverse disciplines in product engineering, product development, network operations, solutions engineers, data center operations, customer care, sales, marketing and communications, finance, legal, compliance, human resources, information technology and business development.

COSO CONTROL COMPONENTS

COSO (Committee of Sponsoring Organizations of the Treadway Commission) defines internal controls as "a process, effected by an entity's Board of Directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following three categories: effectiveness and efficiency of operations, reliability of financial reporting and compliance with applicable laws and regulations." COSO identified five interrelated components of internal control: control environment, risk assessment, information and communication, control activities, and monitoring. PEER 1 Hosting has incorporated these components in the design of their management control framework and the criteria for the service provider audit.

Control Environment

PEER 1 Hosting has a highly experienced management oversight team. Management and the Board of Directors (the Board) are organized to oversee all activities of the Company. Particular attention is focused on customer service and adopting a proactive approach in responding to and addressing customer needs, concerns, and inquiries; to ensure the Company is well positioned to operate and grow to support an increase customer base. PEER 1 Hosting is divided into various departments to ensure appropriate segregation of duties and accountability for specific functions within the Company.

Risk Assessment

PEER 1 Hosting performs an annual risk assessment of potential operational risks which may impede achieving the control objectives covered by this report. In addition, Executive Management meets on a frequent basis with staff to discuss business operations and identify areas which may indicate a problem. Remedial action plans are designed and implemented to mitigate the likelihood of risk occurrence. PEER 1 Hosting's management emphasizes risk awareness in order to effectively identify, monitor and manage risks that could adversely affect the Company's ability to provide reliable hosting solutions to its customers. The primary risks that have been identified through this process pertain to recruitment, corporate and customer system security, data protection and integrity, network backbone infrastructure, and physical and logical access rights. To mitigate these risks, management has established formalized policies and procedures, segregation of duties, performance metrics and multiple levels of monitoring review.

Information and Communication

PEER 1 Hosting has implemented various methods of communication to ensure that employees are aware of and understand their specific roles and responsibilities within the organization and to ensure that significant developments are communicated in a timely and efficient manner. Methods include training for newly hired employees, distribution of corporate policies and employee handbooks, use of communication tools such as electronic mail messages and real-time messenger to communicate time-sensitive and business critical information. Management also conducts periodic staff meetings to address corporate and departmental issues, define and assess achievement of team goals, communicate internal developments, and enhance operational processes.

Staff in Data Center Operations Group (DC Operations, or DCO) and Customer Care Group (Support) provide customer support and ongoing communication with customers. Customers have access to services and support 24 hours a day, 7 days a week, 365 days a year (24x7) via a ticketing system or by phone (*Refer to Control Objective 8 – Manage Problems and Incidents for more details*).

Monitoring

Management has established performance metrics and reports that monitor the activities of the customer facing departments. These reports provide management with the relevant information necessary to assess service level performance and data to make informed management decisions. Reports are generated on a regular basis and sent to management and Executive Management for review. Reports include the following:

- Metrics measurement for each Operations Group (*Refer to Control Objective 5 – Manage Performance and Capacity and Control Objective 8 – Manage Problems and Incidents for more details*).
- Quarterly access rights audits to validate only authorized individuals and groups have access to systems, applications and data center facilities based on their job responsibilities.

These reports are reviewed on a regular basis by management and the Operations Group (Operations) in order to monitor and address service level inquiries and identify opportunities to enhance service levels.

DESCRIPTION OF THE SYSTEM

The objective of this report is to highlight the key internal control activities implemented by PEER 1 Hosting for the period July 1, 2012 to June 30, 2013. Since the prior report (report dated July 20, 2012 for the audit period from July 1, 2011 to June 30, 2012), the scope of the audit has been expanded to incorporate the Vancouver and Portsmouth data center facility and corresponding corporate controls. Selective activities have been updated to more appropriately describe the process in place to validate the effectiveness of the controls in place.

This report is intended to provide PEER 1 Hosting's customer organizations and their auditors with information sufficient to obtain an understanding of those aspects of PEER 1 Hosting's controls that may be relevant to customer organizations internal controls over financial reporting and assist with assessments of control risk for customer organizations. In particular this report, when combined with an understanding of the controls in place at customer organizations, is intended to enhance an understanding of PEER 1 Hosting general control environment for the following areas:

- Management of IT
- Manage Human Resources
- Manage Operations and Monitoring
- Manage Changes
- Manage Performance and Capacity
- Ensure System Security
- Manage Configuration
- Manage Problems and Incidents
- Manage Data and Backups
- Manage Facilities

The scope of this report covers the controls that PEER 1 Hosting employs at the in-scope locations related to the management of technology and related hosting and network services that PEER 1 Hosting provides to its customers. The following locations and related services are included in this report:

Location	Business Platforms	Corporate Network[1]	Linux/Unix[2]	Windows[2]
Miami Data Center	Managed Hosting and Colocation	√	√	√
Atlanta Data Center	Managed Hosting	√	√	√
Toronto Data Center (Pullman location)	Managed Hosting, Dedicated Hosting, and Colocation	√	√	√
Virginia Data Center	Dedicated Hosting	√	√	√
San Antonio Data Center	Dedicated Hosting	√	√	√
Los Angeles Data Center	Dedicated Hosting and Colocation	√	√	√
Vancouver Data Center and Headquarters	Colocation and overall corporate controls that are applied to the in-scope data centers	√	√	√
Portsmouth Data Center and Southampton Headquarters	Managed Hosting, Dedicated Hosting and Colocation, corporate controls that are applied to the UK data centers	√	√	√

The controls relate primarily to services provided to the managed hosting, dedicated hosting and colocation customers for the in-scope data centers and offices as illustrated in the table above. However, corporate controls

[1] The Corporate network will be in-scope to the extent that it manages access to customer systems.
[2] Managed hosting offers RedHat Enterprise Linux, Windows 2003 and Windows 2008. Dedicated hosting offers Linux (RedHat Enterprise Linux, Ubuntu LTS, Fedora, CentOS, and Debian), Windows (2003 and 2008) and Unix FreeBSD. Colocation customers manage their own servers and the installation and maintenance of their operating systems. A combination of these operating systems is also present in the PEER 1 Hosting corporate environment.

within the Management of IT, Manage Human Resources and Manage Changes sections are relevant and apply to PEER 1 Hosting's corporate infrastructure. Selective controls within the Manage Configuration, Manage Performance and Capacity and Ensure System Security sections are relevant and apply across the entire PEER 1 Hosting control environment.

The scope of this report does not include services provided by any sub-service organizations, such as:

- BackCheck, to conduct background checks for PEER 1 Hosting's employees and contractors in Canada and the United Kingdom throughout the period July 1, 2012 to December 31, 2012.
- ADP, to conduct background checks for PEER 1 Hosting's employees and contractors in the United States throughout the period July 1, 2012 to December 31, 2012.
- Talentwise, to conduct background checks for PEER 1 Hosting's employees and contractors globally throughout the period December 1, 2012 to June 30, 2013.
- eVolve DC Solutions (eVolve), to provide datacenter monitoring and maintenance services to data centers in Miami, Atlanta, Toronto (Pullman location), Virginia, San Antonio and Portsmouth.
- Polaris Realty as the owner of the Vancouver data center facility, whereby Polaris Realty provides datacenter maintenance and environmental monitoring services at that facility.
- Digital Realty Trust, Inc. (Digital Realty) as the owner of the Los Angeles datacenter facility, whereby Digital Realty provides datacenter maintenance and environmental monitoring services at that facility.

1. MANAGEMENT OF IT

Control Objective: Controls provide reasonable assurance the management has implemented a planning and governance process within IT.

Management maintains an IT strategic plan that outlines future strategies, initiatives and risks facing the organization.

Strategic Planning and Management Oversight

PEER 1 Hosting's strategic vision is focused on consolidation, standardization, simplification and automation.

Management maintains an organizational strategic plan that outlines the company's future strategic initiatives and an analysis of the obstacles or risks facing the organization. The plan is revisited every year by Management with insights provided by key stakeholders and business units. When reassessing the strategic plan, risks facing the organization are taken into account and initiatives are identified to mitigate risks within the organization or posed by industry.

Management meets on a routine basis to obtain updates on ongoing initiatives and their alignment with the strategic plan. Particular attention is focused on customer service and adopting a proactive approach in responding to and addressing customer needs, concerns, and inquiries. The goal is to ensure the Company is well positioned to operate and grow to support an increasingly sophisticated customer base. PEER 1 Hosting is divided into various departments to ensure appropriate segregation of duties and accountability for specific functions within the Company.

Management has documented and communicated policies, procedures and controls governing the IT organization's activities.

Policies and Procedures

PEER 1 Hosting's control environment reflects the position taken by its Executive Management and the Board concerning the importance of controls and the emphasis given to documented policies and procedures to govern the organizational structure.

PEER 1 Hosting's IT Security Group has developed policies that address its IT operations which provide the basis of the organization's formal control environment. These policies are available on PEER 1 Hosting's intranet and communicated to the organization on an annual basis. Currently, employees are advised of these corporate security policies but are not required to formally sign off and evidence their acknowledgment of these policies (*Refer to Control Objective 6 – Ensure System Security for more details*).

Control Activity Mapping

The following table describes to which business platforms the controls apply or whether it is a corporate control:

Control Activity #	Control Activity	Corporate	Managed Hosting	Dedicated Hosting	Colocation
1.1	Management maintains an IT strategic plan that outlines future strategies, initiatives and risks facing the organization.	√			
1.2	Management has documented and communicated policies, procedures and controls governing the IT organization's activities.	√			

2. MANAGE HUMAN RESOURCES

Control Objective: Controls provide reasonable assurance that policies and procedures are in place to support the hiring and development of personnel.

Management has a standard hiring process, including approval to hire and performing background and reference checks.

Recruitment Procedures

PEER 1 Hosting has formal hiring practices for permanent, contract and third-party agency employees. Each year during the planning process, Executive Management agrees on the new headcount to align with the strategy of the business and budget for the upcoming fiscal year. Once headcount and new positions are approved by the CEO, the hiring process is initiated in accordance with the Recruitment and New Hire policy and procedures.

People Leaders (managers with line management responsibility) regularly discuss upcoming hiring needs with their People Partner (Human Resources Business Partner). If a new hire is required, the People Leader communicates this staffing requirements to the assigned People Partner. The People Partner confirms the requirements and creates a new requisition in the online resume management system ("Jobvite") for approval by the Director of People and Performance or authorized delegate. The Director of People and Performance will coordinate budgetary details in conjunction with the Chief People & Performance Officer and the VP of Finance. The status of open positions is tracked in Jobvite.

The Recruitment Coordinator, a member of the People and Performance team, sources candidates in partnership with the hiring manager – which includes telephone screening candidates to confirm minimal requirements for the role description are met, assessment for cultural fit, and conducting interviews to collectively assess the candidates.

When a candidate is selected for hire by PEER 1 Hosting, the People Partner sends a Request to Extend Offer to the People and Performance email alias for approval by the Director of People or authorized delegate. The consent for background screening, an offer letter and a Non-Disclosure and Confidentiality Agreement (NDA) are drafted and sent to the selected candidate to make a formal offer. The offer is accepted when the candidate returns the completed and signed paperwork.

Background checks generally consist of an education check, confirmation of prior employment and criminal record check (where it's feasible and permitted by the local jurisdictions). These checks are initiated prior to providing an employee or worker with access to confidential corporate, employee, and customer information. Completion of background checks are outsourced to Talentwise from December 1, 2012 (PEER 1 Hosting outsourced background checks to BackCheck for contractors and employees in Canada and the UK and used ADP in the US from July 1, 2012 to December 31, 2012). Once completed, the background check is reviewed and approved by the People & Information Manager as part of the new starter checklist. Any issues revealed through the background check are escalated to the General Counsel and resolved internally with the People & Information Manager.

In some cases, a worker may be hired to work on a specific task or activity that will not require access to confidential corporate, employee or customer information. In these cases, a record will be kept in a corporate register and any changes to the nature of the work must be notified to the People & Information Manager so that the background check can be reviewed.

For selected recruitment needs, the Company may engage the services of a third-party service agency to assist with the process. For these situations, PEER 1 Hosting requires written confirmation of the background screening

performed prior to the individual being given access to systems, applications, or records which has access to corporate or customer information.

For isolated scenarios when the individual starts prior to the completion of the background checks, PEER 1 Hosting has the unconditional right to terminate the employment arrangement if any unfavorable information surfaces from the background check, in accordance with statutory legislation. Termination of the employment arrangement will be a collaborative effort among PEER 1 Hosting's in-house General Counsel, the People and Performance team, the hiring department and/or third-party General Counsel as applicable.

A new hire checklist is followed which tracks all documentation needed to set up each new hire (this includes personal information, background screening, Nondisclosure Agreement (NDA), benefits setup, access rights set up, new hire announcement, and organization chart updates). As part of the hiring process and to ensure safeguarding of confidential information, each employee is required to sign the NDA relating to PEER 1 Hosting and customer information. As part of the onboarding process, the employee is also required to sign an Employee Acknowledgment Form, acknowledging receipt and adherence to the Whistleblower Policy, Code of Business Conduct, Disclosure Policy, and the Employee Handbook.

Confidential employee data is physically secured and maintained by People and Performance in locked facilities or stored on a secure part of the corporate network which is only accessible by authorized personnel.

Workers who are not classed as employees (e.g. third-party consultants, contractors or agency workers) are subject to a similar hiring process*.*

Management provides training and development necessary to fulfill job responsibilities.

Training and Professional Development

PEER 1 Hosting has implemented various training platforms to ensure that employees understand and perform their individual roles and responsibilities, including onboarding, e-learning, and on-the job training. Training and professional development needs are identified ongoing and through the annual review process, which is a collaborative process for individuals and their leaders to discuss performance and development. Training requirements may be met in a variety of ways, including access to internally developed training, vendor-delivered training, or externally offered certifications, degrees, workshops and conferences. The annual review outputs are reviewed by the People Partners to identify roles or functions deemed critical to PEER 1 Hosting that will be included in succession planning and cross-training.

PEER 1 Hosting also provides a sponsored further education program for employees to access and be reimbursed for university courses and degrees. This program is subject to pre-approval by the individual's leader and the Chief People and Performance Officer. There is a procedure and reporting process through Employease for approving further education programs and reimbursement.

Control Activity Mapping

The following table describes to which business platforms the controls apply or whether it is a corporate control:

Control Activity #	Control Activity	Corporate	Managed Hosting	Dedicated Hosting	Colocation
2.1	Management has a standard hiring process, including approval to hire and performing background and reference checks.	√			
2.2	Management provides training and development necessary to fulfill job responsibilities.	√			

3. MANAGE OPERATIONS AND MONITORING

Control Objective: Controls provide reasonable assurance that data center operation tasks are performed and processing issues are monitored.

Management has documented and implemented standard operating procedures to maintain the data center.

Operating Procedures

PEER 1 Hosting has designed and established standard operating procedures that guide the data center operations on a daily basis. Activities such as trouble resolution, system maintenance and provisioning services are governed by a set of documented procedures which meet or exceed industry standards and/or best practices. These procedures are stored on various internal communication platforms such as the Wiki, HUB, Confluence, and/or SharePoint.

Data center management is responsible for maintaining and updating these processes to reflect current business practices. To ensure these documents remain current, data center management has weekly team meetings with data center operational staff to discuss any new procedures or documentation.

Management has defined shift-handover procedures, including handover of tasks, problems and incidents.

Shift-Handover Procedures

Management has defined shift-handover procedures for our 7/24 staffed facilities, which consist of a combination of an end-of-shift report, verbal communication of the handover of tasks, problems and incidents, and documentation of issues using tickets. The end-of-shift report contains details pertaining to handover activities from the previous shift which are outstanding and require resolution. This report may include information related to monitoring of pending trouble tickets, data center tasks to be completed, maintenance issues to be resolved and other material shift handover activities to be addressed.

For the Vancouver Data Center, shift-handover procedures do not occur as they do at the other data centers because there is only one shift at the Vancouver Data Center, Vancouver Data Center staff monitors the data center during normal work hours, and the Network Operations Center (NOC) monitors the data center outside of normal work hours. Issues determined by the NOC are documented using PEER 1 Hosting's ticket system.

Management has defined provisioning procedures to ensure customers subscribed service is provisioned in accordance with the sales order.

Service Provisioning

When customers initially subscribe to managed or dedicated hosted devices, the sales team will have the customers' order recorded in an internal tracking system known as Ocean. Services are provisioned based on this central repository by skilled technicians. Each data center is responsible for provisioning servers and network devices. After provisioning and undergoing the quality assurance (QA) process, a "welcome letter" is sent out to the customer. The customer invoice is created based on the service order recorded in Ocean.

PEER 1 Hosting provides the following selective subscription based security services to its customers:

- **Intrusion Detection Systems (IDS)** – This service is only available for managed hosting customers. PEER 1 Hosting currently offers Intrusion Detection Systems (IDS) services provided by AlertLogic. AlertLogic,

PEER 1 Hosting and PEER 1 Hosting's customers will establish alerts for security incidents. All alerts will be directly reported to PEER 1 Hosting's customers. If customers have questions or need assistance with remediating the alert, they can contact PEER 1 Hosting's Support group to escalate. Depending on the nature of the incident, PEER 1 Hosting support professionals will help the customer to assess the situation and further escalate the issue to AlertLogic, if necessary. AlertLogic acts as an outsourced security operations center (SOC) for PEER 1 Hosting, whereby the AlertLogic SOC services are extended to PEER 1 Hosting customers. PEER 1 Hosting still maintains the customer relationship.

- **Control Scan Service** – This service is only available for managed hosting customers. Bi-weekly vulnerability scans are performed and the result details are provided to customers. Customers have the option to sign up to receive alert notices of completed scans. Customers who subscribe to the managed hosting platform after early 2009 receive complimentary control scan service on their primary IP address.

Control Activity Mapping

The following table describes to which business platforms the controls apply or whether it is a corporate control:

Control Activity #	Control Activity	Corporate	Managed Hosting	Dedicated Hosting	Colocation
3.1	Management has documented and implemented standard operating procedures to maintain the data center.	√	√	√	√
3.2	Management has defined shift-handover procedures, including handover of tasks, problems and incidents.	√	√	√	√
3.3	Management has defined provisioning procedures to ensure customers subscribed service is provisioned in accordance with the sales order.	√	√	√	

4. MANAGE CHANGES

Control Objective: Controls provide reasonable assurance that system changes affecting the customer environment are authorized, tested and implemented in a timely manner.

A documented change management procedure exists to govern programming, system or configuration changes to infrastructure systems, network devices and system software.

Change Management Procedures

PEER 1 Hosting plans, reviews and coordinates proposed changes to production systems for validity, completeness and accuracy in order to minimize the impact on internal and external customers. This is a formalized and documented process which includes changes such as additions, scheduled maintenances, upgrades, or modifications that relate to existing PEER 1 Hosting products, services or corporate infrastructure. The change control management applies to all business platforms, production applications, and data center operations which are customer impacting. Excluded from scope are development, testing, and staging environments which do not affect production, changes already documented within the customer facing ticketing system, and selective network changes which are not customer impacting. Appropriate PEER 1 Hosting personnel supervise the activities completed by external vendors or contractors. The change management process tracks the progress of change requests, including submissions, approvals, modifications, test plans, closures, and post mortems. These processes are described in greater detail below.

Regular changes are documented and approved according to PEER 1 Change Management policies before the changes are implemented.

Regular Changes

Change requests are managed using an in-house developed web-based application, called “Change Control System”, a role based system which is authenticated via the corporate network credentials. This platform documents both regular and emergency changes. A change request consists of a description of the proposed change and a step-by-step scripting of the proposed work. An email is generated with the change request details and sent to the change control email alias. The requestor is responsible for identifying an approving manager or director to review and approve the change. If the change request is declined, the requestor must either modify or cancel the change request. If a change is revised after being approved by a manager or director, the change request will have to be reviewed and re-approved. Upon modification and re-approval, a notice is sent to staff via the change control alias. Following approval, the change will be implemented according to the revised plan. Pre and post implementation test plans are created as part of the change control process with the intention that the change is implemented according to plan.

Each proposed change is defined clearly to provide all evaluating parties with the information required to appropriately evaluate the proposed change. The affected functional groups or departments are responsible for analyzing the impact of the change on their area and notifying the requestor of any concerns. After affected parties are notified of the proposed change, a schedule of change release will be agreed upon with input from the affected parties.

Change requests are primarily initiated by PEER 1 Hosting employees. There may be rare incidents when customers may provide suggestions for functionality or features improvements to production systems or service offerings; in which case PEER 1 Hosting will assess the feasibility of the request, evaluate the cost and benefit associate with the

change, and prioritize it accordingly. Both types of initiated changes follow the change management process identified in this section. Any customer initiated changes related to their existing services at PEER 1 Hosting will be handled via the standard process and tracked in the customer management systems Ocean or Mercury (*Refer to Control Objective 8 – Manage Problems and Incidents for more details*). High level statistics are generated and stored on SharePoint for management's review at their discretion. Individual requests for information by departments can be requested by department heads and submitted to IT Operations for compilation and analysis.

Testing is performed in non-production environments. If a non-production environment does not exist, change control testing is not completed nor required. If the roll-out fails during the execution of a change, PEER 1 Hosting will reverse the change immediately according to the roll-back plan documented within the change request. PEER 1 Hosting will not fix the issue in the production environment as it could lead to inadvertent customer impact. When a roll out failure occurs, the protocol is to identify the cause of the failure, roll back the information and conduct further analysis to resolve the situation.

A post mortem is performed on changes to assess the results. The cause of the failure will be analyzed in order to learn from the mistakes and to put actions in place to prevent them from recurring on a go forward basis.

Emergency changes are documented and authorized (including after-the-fact approval) in a timely manner according to PEER 1 Change Management policies.

Emergency Changes

Emergency changes are defined as immediate action required to resolve a critical situation or an imminent critical situation. Emergency changes follow the same change management process described with the exception that each emergency change must be approved by a director or a more senior individual, with the exception of network and facility related vendor maintenances which can be approved by either the NOC or Data Center managers. For urgent situations where the change was implemented prior to obtaining approval, after-the-fact approval is obtained and documented. Emergency changes do not need to wait for the weekly change control meeting to be executed due to their critical nature. The results of emergency changes are presented in the next available change control meeting. Test plans are also often created retrospectively to confirm that the change was properly implemented.

Control Activity Mapping

The following table describes to which business platforms the controls apply or whether it is a corporate control:

Control Activity #	Control Activity	Corporate	Managed Hosting	Dedicated Hosting	Colocation
4.1	A documented change management procedure exists to govern programming, system or configuration changes to infrastructure systems, network devices and system software.	√			
4.2	Regular changes are documented and approved according to PEER 1 Change Management policies before the changes are implemented.	√			
4.3	Emergency changes are documented and authorized (including after-the-fact approval) in a timely manner according to PEER 1 Change Management policies.	√			

5. MANAGE PERFORMANCE AND CAPACITY

Control Objective: Controls provide reasonable assurance that system performance and capacity levels are monitored and that a process is in place to address suboptimal performance levels.

Management monitors the performance and capacity levels of the internal and customer-facing systems.

Performance and Capacity Management

PEER 1 Hosting's infrastructure is comprised of the corporate network, corporate backbone and the customer production network. PEER 1 Hosting uses network management tools to monitor the backbone, corporate network for each data center, the data center LAN, and customer network connection for all business platforms on a 24x7 basis.

Each data center has one production and one corporate network. The data centers are inter-connected via the corporate backbone. The NOC in Vancouver monitors production network for each data center – which includes monitoring device availability and uptime, customer connectivity, bandwidth utilization, and central processing unit (CPU) on core routers and switches.

The corporate network is monitored by the NOC for availability and uptime. This includes monitoring the inter-connections that make up the backbone of the corporate network, backbone capacity and response time, packet loss and latency, and devices such as routers, access switches and distribution switches, via Simple Network Management Protocol (SNMPc). The SNMPc screen provides a map of the PEER 1 Hosting network and displays the health of links and key locations. The NOC also utilizes a threshold monitoring system called Mercury to monitor critical ports which have thresholds defined for performance monitoring.

Performance and capacity of internal systems are monitored through Hypeerion (primary) and SNMPc (secondary). Hypeerion monitors infrastructure devices ranging from corporate servers and switches, to HVAC and uninterrupted power system (UPS) units. This monitoring will happen at three levels: activity, availability and polling with some reporting and overlapping between them. Hypeerion is set up and operating in all data centers with two physical servers at each data center, a primary and secondary which are used to poll and aggregate data on the various network segments.

The NOC monitors colocation data center networks. Thresholds are pre-defined for applicable systems and automated alerts are generated and sent to the NOC when thresholds are reached. ***Please note***: It is the responsibility of the customers to contact PEER 1 Hosting if support is required. PEER 1 Hosting is not responsible for active monitoring of individual customer systems for capacity issues. Colocation is a self-serve product and its customers are primarily responsible for monitoring and resolving their own servers' performance and capacity concerns. PEER 1 Hosting, at its sole discretion, may assist colocation customers with performance related inquiries on a case-by-case basis.

PEER 1 Hosting's Support team monitors managed and dedicated hosting customer servers for device availability and uptime using Hypeerion. An offshore monitoring team monitors Hypeerion and addresses alerts as the tool detects performance issues, opens tickets and assigns them to the appropriate team.

Other subscription services such as Smart Monitoring and Port Monitoring are available to selective customers for monitoring system capacity and traffic thresholds respectively. Smart Monitoring is available to managed hosting customers while Port Monitoring is available to colocation customers.

On a monthly basis, PEER 1 management meets to discuss network metrics for the month ended. The network metrics report tracks overall network utilization and specific link / circuit utilization, critical areas and potential problem points, bandwidth usage, and NOC issues tracked though the ticketing system. Areas of concern are identified and remediating activities are carried out to resolve or prevent any issues raised.

Management has a process in place to respond to suboptimal performance and capacity measures in a timely manner.

Performance Issues Resolution

There are processes in place to address suboptimal performance and capacity issues in a timely manner. Depending on the type of service and monitoring tool used, either PEER 1 Hosting or the customer will be notified.

If customer-related performance or capacity issues are detected within Hypeerion, they will display on screens monitored by Support. Support will create a ticket in Ocean to initiate the problem resolution process. During the initial account setup, customers may provide the Support team with preferred issue resolution guidance. Customers also have the option to decline this monitoring service and must notify and advise PEER 1 Hosting of this arrangement. As colocation customers are in charge of their own systems, no monitoring is performed on colocation customers' servers.

Within Mercury, once a threshold is breached, an email alert is sent to the monitoring team, which will then use several other tools (e.g., CACTI, Inmon) to diagnose and resolve the problem. A ticket may be created in the ticketing system (Ocean) at any point during the process.

Smart Monitoring sends out automated alerts directly to the managed hosting customers if a threshold pre-defined in the applicable systems is reached. Customers are able to configure alert settings and it is up to the customer to create a ticket within Ocean if they require further support from PEER 1 Hosting. ***Please note:*** The managed hosting customer is responsible for responding to any issues identified by the Smart Monitoring service.

Port Monitoring allows colocation customers to set up thresholds for traffic to their servers. Once a threshold is breached, an email alert is sent directly to the customer. ***Please note:*** The colocation customer is responsible for responding to any issues identified by the Port Monitoring service.

There are escalation procedures in place for trouble tickets that provides for timely notification and resolution of customer performance and capacity issues. These escalation procedures would apply to all three business platforms (*Refer to Control Objective 8 – Manage Problems and Incidents for more details*).

Control Activity Mapping

The following table describes to which business platforms the controls apply or whether it is a corporate control:

Control Activity #	Control Activity	Corporate	Managed Hosting	Dedicated Hosting	Colocation
5.1	Management monitors the performance and capacity levels of the internal and customer-facing systems.	√			
5.2	Management has a process in place to respond to suboptimal performance and capacity measures in a timely manner.	√	√	√	√

6. ENSURE SYSTEM SECURITY

Control Objective: Controls provide reasonable assurance that systems are secured to prevent unauthorized access, use, modification or loss of data.

Management maintains and communicates security policies that address IT security requirements.

Corporate Security Policies

On an annual basis, the Corporate Security team will advise employees of these corporate security policies. These corporate security policies include:

- Acceptable Use
- Non-Discrimination and Anti-Harassment
- Computer and Network Use
- Clean Desk
- Software Use and Installation
- User Provisioning Process
- Information Classification Security
- User Minimum Access
- Physical Access
- Segregation of Duties
- System Restoration
- Data Destruction
- Acceptable Encryption
- Laptop Use
- Server Anti-virus
- Workstation Anti-virus
- Wireless
- Ethics
- Password
- P2P File Sharing
- Email
- Remote Access
- Internet Usage

Procedures are followed to request, establish, issue, suspend, and close user accounts in a timely manner for new hires, job changes, and job terminations. The process includes approval of access rights based on the role of the user.

Access Rights Administration

PEER 1 Hosting requires management authorization for employee access to critical applications and underlying systems. Access is granted according to a user's functional requirements and position within the organization as determined during the new hire or internal transfer process. Group access rights restrict users to only those systems required to perform the duties as necessitated by the job position. A new user is created in response to a request from People and Performance. This request automatically creates a ticket in JIRA, a ticketing system used to track internally initiated requests. Details of the access granted are retained in the ticket, and the ticket is closed once all access has been provisioned by IT Operations in collaboration with other departments as needed.

Internal staff transfers are also recorded in JIRA. The request of internal transfers is submitted by People and Performance and managed by IT Operations. Any access which is not required for the staff's new role is removed, and new access is added based on the new role.

Changes in title, salary, reporting, department or location are tracked on a Request for Employee Status Change form, which must be authorized by the Chief People and Performance Officer and the reporting manager. This form documents the type of change (i.e. department, title, compensation, location, reporting structure, leave or exit), reason for the change, and the effective date of the change. Access changes are made by IT upon receipt of an email

from People and Performance authorizing the changes. Confidential employee data is physically secured and maintained by People and Performance in locked facilities or stored on a secure part of the corporate network which is only accessible by authorized personnel.

When an employee or contractor is terminated or resigns, a Request for Employee Status Change form is completed to indicate the effective date of termination. A termination checklist is followed to ensure all relevant departments are notified of the impending departure. People and Performance authorizes the IT Operations Group (IT Operations) to either remove access to all systems immediately (for terminations) or on the last day worked (for resignations).

PEER 1 Hosting allows authorized employees remote access to its network using a corporate VPN system. Users must be authenticated against the corporate Active Directory domain, with a second factor required: a user must also authenticate against an internal RADIUS solution requiring that the user provide a one-time token (generated by a Safeword token generator, which can be either a hardware device or a smartphone app) plus a PIN before access is granted to corporate systems. The data traversing the VPN is encrypted using SSL and IPSEC protocols.

Access to customer impacting network devices, domains and system functions is restricted to authorized personnel.

Information Security of Network and Devices

PEER 1 Hosting's production network is directly reachable from Internet sources. PEER 1 Hosting has taken a proactive approach to secure network devices including routers, switches, load balancers, and firewalls that are Internet accessible through the use of hardened security baselines to configure devices. PEER 1 Hosting uses a Terminal Access Controller Access-Control System (TACACS) which provides network devices a centralized authentication platform to determine whether the user has authorized access to the system. Corporate computers and devices are located in physically secure locations within each facility.

Security access for remote login to network devices is controlled by an ACS managed by the networking departments and source access control via access control list (ACL). Access controls is broken down into two security components: user authentication (who can login using what username and password) and command authorization (what a user is allowed to do once logged in). User authentication is performed against the ACS system which maintains its own local copy of user credentials. The management of users and passwords for network device access is handled manually via additions, changes, and removals of users as needed.

Command authorization is managed by mapping user groups (such as departments, sub departments, functional security grouping) to available command lists for each logical group of network devices. ACLs (such as access-lists, admin manager-IPs) are used to limit remote logins on network devices to trusted sources only. ACLs are scanned on a daily basis by RANCID, a configuration version control (CVS) system, for all network devices to identify any unauthorized configuration changes.

An audit process exists and is followed to periodically review and confirm access rights to systems and facilities.

Auditing of Access Rights

Employees' access rights to key systems, customer environments, data centers and facilities are reviewed and evaluated on a quarterly basis by Corporate Security and/or Network Operations to ensure that proper access levels are maintained and consistent with the job requirement and in compliance with existing practices. These include:

- Badge system audits[3] (An audit of access badges designed to ensure that access permissions to PEER 1 Hosting data centers are correct and authorized).
- Safeword user audits (An audit of access rights to the Safeword system (administrative access to a subset of customer servers)).
- Corporate Active Directory user audits (An audit of the Active Directory designed to ensure that PEER 1 Hosting employees are assigned the appropriate individual and group membership rights based on their job responsibilities).
- ADM/user audits (An audit designed to ensure only authorized PEER 1 Hosting employees have access to the ADM domain, which is used for administrative access to a subset of customer servers).
- Bastion server audits (An audit of each bastion server designed to ensure that only authorized PEER 1 Hosting employees have access to the bastion servers, which are used to administer local customer switches and act as a jump box for dedicated hosting production servers).
- Ocean system audits (An audit is performed on the customer management system to ensure that only authorized personnel have access to the system).
- TACACs audits (An audit of access rights to the network devices).

Procedures are in place to require complex passwords, with a minimum of 8 characters that change every 90 days, to access corporate and customer systems.

Password Management

Access to IT resources on the corporate network is authenticated with the Corporate Active Directory before access is granted. PEER 1 Hosting enforces password complexity requirements which are in place for each user and adhere to industry best practices. Valid passwords must be a mixture of upper and lower case alpha-numeric characters, contain a minimum of 8 characters in length, password to be changed a minimum of every 90 calendar days, and cannot be a duplicate password used during the last five times. IT Operations manage all passwords for key business systems. The network departments manage passwords which are specific to network devices (refer to Network Devices below).

Access to network devices is controlled through an Access Control System (ACS) and local password policies managed by the network departments. Passwords directly configured on networking devices for local access are encrypted and only known by the managing network departments. These local passwords are audited periodically and changed immediately upon a privileged employee's departure or revocation of security clearance.

Logical segregation is in place to protect customer systems from the internet for customers that subscribe to the firewall service.

Firewall Management Solutions

PEER 1 Hosting offers firewall management solutions to all its customers who have purchased PEER 1 Hosting's firewall management solution. The baseline configuration and level of firewall management services provided will differ across the business platforms. For managed hosting customers situated behind a dedicated firewall, PEER 1

[3] Please note: The physical access audits performed by IT Security historically did not include access cards issued to colocation customers or other cardholders (such as contractors, visitors, etc) since the customer is responsible for alerting PEER 1 Hosting if changes are required (control 6.4). The customers manage their own access to their system environment (e.g. cages) at PEER 1 Hosting. An exhaustive audit of all badges (including customers) is currently underway, but remediation of customer accounts is in progress and may not be completed by the report date.

Hosting can also perform a security review of the customer's network configuration and provide recommendations for security improvements.

PEER 1 Hosting's security professionals will work with the customer to assess their specific network needs and custom-design the firewall rule set to meet these requirements. For dedicated hosting customers, PEER 1 Hosting sells a firewall product separately from the servers. But it is the customers' responsibility to configure the firewall rule set and perform any necessary security reviews since it is a self-managed environment. Colocation customers who subscribed to the firewall service are situated behind a shared firewall and are fully responsible for configuring and managing their firewall permissions and rule sets.

Logical segregation is in place to protect the corporate network from the internet.

Protection of the Corporate Network

Corporate network is logically segregated from the external network using firewall management solutions. Juniper SSG Firewalls are implemented to prevent unauthorized access from the extranet. Corporate network in different cities are logically inter-connected through private IP address, which is not routable or accessible from the external public Internet.

Daily review of firewall configuration changes is conducted to confirm that changes are authorized. Prescribed critical change triggers are outlined and should configurations differ from the baseline, an appropriate technician will be contacted to conduct further investigations.

Procedures are in place to protect information systems from malware (e.g. viruses, worms).

Monitoring Security

PEER 1 Hosting performs security logging, monitoring and reporting. Systems are constantly monitored for outages. Attention is focused on systems that pose the greatest risk to PEER 1 Hosting in terms of impact on business operations. Specific examples include, but are not limited to:

- Virus scanning software is in place for critical corporate systems. The virus signature files are downloaded and deployed within four hours of release.
- System and applications are monitored for outages and alerts are created based on pre-determined escalation procedures.
- Periodic audits of critical network devices are conducted.
- Key events and issues related to critical systems are analyzed for root cause and remediated.
- Video surveillance within and surrounding the data centers.
- Access badge for customer, employee, and vendor access.

On each Windows system, whether corporate or managed hosting, PEER 1 Hosting has deployed the latest anti-virus software provided by McAfee. By default during provisioning, all managed hosting customers operating on a Windows platform have VirusScan® installed on their servers. Managed hosting customers can opt out of the anti-virus service by notifying PEER 1 Hosting. New DAT files are updated on corporate and managed hosting servers multiple times a day. Dedicated hosting and colocation customers do not receive this service since they operate in a self-managed environment which is entirely within the customers' responsibility.

For managed hosting customers, system scans including memory, running processes, and local drives are run once a week. On-access scanning has also been enabled, and scans accessed files including scripts, and scan logs are maintained. Alerts raised by either the on-access or weekly scans on any system are captured and sent to the two central McAfee ePolicy Orchestrator (ePO) servers. Viruses found during the real-time scans or weekly scans are cleaned automatically by the software. Non-critical definitions are configured to be held one day to confirm compatibility of the definition DAT update before it is released to the managed hosted customers' ePO server.

Management makes tested patches available to customers on a weekly basis.

Patch Management

PEER 1 Hosting performs frequent patch updates on their own systems and infrastructure. PEER 1 Hosting provides managed hosting customers with downloaded, tested patches for installation. Due to customer requirements to administer their own systems, PEER 1 Hosting does not install patches for customers, but rather provides pre-implementation testing services which can be accepted or declined based on the customer's requirement. Managed hosting customers are responsible for installing and validating the patches on their own systems. For managed hosting systems, Microsoft patches are downloaded every *'patch Tuesday'*. For LINUX, with the exception of critical patches, routine patching is scheduled to begin the third Thursday of the month. Critical patches are reviewed for their severity and potential impact on the environment, and may be released earlier. ***Please note:*** Dedicated hosting and colocation customers are responsible for patching their own systems.

Patch testing is performed and applied to both Windows and Linux systems. Product Engineering puts the patch packages together and passes them to the SWAT Group (SWAT) who will promote the patch packages to a staging area. Patches are tested by the Quality Engineering Group (QE) team on test lab servers. Once QA has completed their review on the test servers, the patches are deployed to a test group of customer systems. If there are no issues, SWAT will make the patches available for download for corporate and customer systems. The testing turnaround time is generally one week for routine patch releases. Both corporate and customer systems have to be setup to automatically download and install patches. It is the customers' responsibility to ensure that the latest patches are successfully installed on their systems. ***Please note:*** PEER 1 Hosting does not monitor the patch levels on customer systems other than providing patches to their customers. Before patches can be promoted to production and distributed to managed hosting customers, the patches are approved by management for deployment.

Procedures are in place to apply upgrades and patches to network operating systems as appropriate. Upgrades and patches are evaluated to identify whether they are beneficial to the organization and are tested prior to implementation. PEER 1 Hosting leverages prior QE testing performed for operating system patches (i.e. patch updates for Window and Linux operating systems), which have already been rolled out to customer facing servers during every '*patch Tuesday'*. Network change management follows standards and procedures as outlined in Control Objective 4 "Manage Changes". IT Operations is responsible for installing the downloaded patches on corporate servers. Patches are often included within the images that are used to provision new systems. This process is outlined within Objective 7 "Manage Configurations".

Control Activity Mapping

The following table describes to which business platforms the controls apply or whether it is a corporate control:

Control Activity #	Control Activity	Corporate	Managed Hosting	Dedicated Hosting	Colocation
6.1	Management maintains and communicates security policies that address IT security requirements.	√			
6.2	Procedures are followed to request, establish, issue, suspend, and close user accounts in a timely manner for new hires, job changes, and job terminations. The process includes approval of access rights based on the role of the user.	√			
6.3	Access to customer impacting network devices, domains and system functions is restricted to authorized personnel.	√			
6.4	An audit process exists and is followed to periodically review and confirm access rights to systems and facilities.	√	√	√	
6.5	Procedures are in place to require complex passwords, with a minimum of 8 characters that change every 90 days, to access corporate and customer systems.	√			
6.6	Logical segregation is in place to protect customer systems from the internet for customers that subscribe to the firewall service		√	√	√
6.7	Logical segregation is in place to protect the corporate network from the internet.	√			
6.8	Procedures are in place to protect information systems from malware (e.g. viruses, worms).	√	√		
6.9	Management makes tested patches available to customers on a weekly basis.		√		

7. MANAGE CONFIGURATION

Control Objective: Controls provide reasonable assurance that IT components as they relate to security, processing and availability, are protected, are designed to prevent unauthorized changes, and assist in the verification and recording of the current configuration.

Management has defined a baseline configuration for servers and network elements and new systems are configured according to the baseline.

Baseline Standards

The PEER 1 Hosting Product Engineering Group (Product Engineering) has developed baseline configurations for each of the operating systems supported for managed hosting customers (Redhat Enterprise Linux, Windows 2003 and Windows 2008). Various hardened configurations of each of these operating systems are available to customers. Once a server is built by an automated provisioning system and/or a manual provisioning system for a customer, the server is submitted to Product Engineering for testing and validation before being deployed by Support into the production environment. If the server build fails, Product Engineering works alongside Support to remediate the configuration.

Dedicated hosting customers can select from various hardened baseline configurations for each of the operating systems supported, including Linux (RedHat Enterprise Linux, Ubuntu, Fedora, CentOS, and Debian), Windows (2003 and 2008), Unix and FreeBSD. Provisioning for dedicated hosting customers is automated and does not require human intervention unless manual hardware configuration or building a server which is not available from the shopping chart is required. Since dedicated hosting operates in the self-managed environment, initial testing and validation of specifications requested by the customer is performed on the server before deployment. This involves hardware installation and network connection.

Colocation customers are responsible for the configuration, installation and implementation of their own operating systems. Colocation customers own their servers and rent cabinet space from PEER 1 Hosting in one of its available data centers where colocation services are offered.

Network devices such as firewalls and routers are manually deployed with a predetermined baseline configuration by Network Operations. In cases like firewalls, there is a common rule set that is consistently deployed across the infrastructure for corporate platforms and managed hosting customers. If the baseline needs to be customized, the change will be raised in the weekly departmental meeting and the need to update the baseline will be validated. ***Please note:*** PEER 1 Hosting is only responsible for the initial set up of the network devices and dedicated hosting and colocation customers are responsible for configuring their firewall rule sets in details according to their own needs.

At PEER 1 Hosting, corporate system owners are responsible for determining how their systems should be configured and maintained. These procedures vary depending on the requirements of the application and system. PEER 1 Hosting business owners are responsible for informing IT Operations of new system deployments and code deployments. Deployments must be thoroughly tested and documented before submitting to IT Operations for implementation.

Changes to baseline configurations applied to servers and network elements are authorized and tested prior to implementation.

Baseline Configuration Changes

There is a process in place to govern changes made to baseline configurations for network devices. When it is determined that functionality changes are required to a baseline template, the network team and other Operation Groups will discuss this collectively to determine the best course of action. Recommendations are made and approved during change meetings. The functional changes are made by an authorized network engineer and deployed to current non-customer impacting devices. If the functionality fails to perform as designed, the network engineer will make necessary modifications and re-deploy the configuration changes to the network elements. Network engineers are authorized to make changes which do not affect functionality and are cosmetic in nature, without having to obtain prior approval from the Network manager.

Product baseline requirements are stipulated for each product and determined by Product Management, in collaboration with the applicable departments who manage these assets. Changes to baseline configurations can initiate from various sources – such as an operating system change which is suggested by Support or Data Center Operations, or due to emerging trends in the product group. The nature of the change and the effort required to implement the change will affect the roadmap taken and the approval needed. Security patches, driver updates for newer equipment and/or necessary cosmetic changes will drive changes to the baselines. Generally, requests from baseline configuration changes are tracked via JIRA or internal correspondence, and will be submitted to either the Product Management team, Product Development team, or the Executive team for approval. The approval process will entail reviewing the scope of the change, the business reasons for the change, and the extent of resources required, and any business plan document which was prepared. The configuration will go through Quality Engineering (QE) testing as part of the deployment process. The activities surrounding change management is discussed in Objective 4 “Manage Changes”.

Baseline configuration changes for networking include anything that affects the overall global operations of the network device. Changes to the network device baseline functionality, must follow PEER 1’s existing Change Control process and have management approval before being pushed into production. Changes that have not been previously released into production will be tested on non-production equipment first to ensure performance is as expected.

Some examples of baseline configuration changes are:

- Global modification to a device’s routing protocols such as RTSP, LDP, LLDP, ISIS, OSPF
- Modifications to the management ACLS’s of any network devices (SNMP, Telnet ACLs)
- Implementation of any feature set that affects the global operations of a network device.

Please note: Changes to individual customer configurations, provisioning of new clients and modifying individual interface/VLAN settings are not considered to be changes to baseline configurations and are exempt from the Change Control process.

Periodic testing and assessment is performed to confirm that software and network infrastructure is appropriately configured.

Periodic Testing and Assessment of Network Configurations

RANCID, a configuration version control (CVS) system has been implemented at PEER 1 Hosting to provide a repository of system configurations for network devices. RANCID covers corporate network devices and customer

facing devices for dedicated and managed hosting platforms (such as firewalls, switches, routers, and load balancers). RANCID covers all corporate network devices, managed customer firewalls and managed hosting switches, routers and load balancers. Every night RANCID logs into the network devices and runs several commands to view the configuration, as well as other specific pieces of interest such as current running firmware operating system version. The downloaded configuration file for each device is compared to the most recent configuration stored within the RANCID repository. RANCID retains a history of all changes to every device within the repository; this data is saved as a change log: initial configuration plus all changes. The configuration data for each device in the RANCID repository can be used to restore the device to any point in time. Differences found in device configurations are consolidated into daily emails and sent to the Network Operations Engineers for review.

In addition to the simple comparison to previous configuration files, RANCID is also set to scan changes in each configuration file for a set of security related keywords or critical change triggers. Any changes found which match one of the predefined keywords is consolidated into a daily email, which is sent to every engineer in the networking department. It is a key responsibility of the engineers to investigate any of these changes.

To ensure that the RANCID system is correctly identifying security related changes on network devices, in the event that no critical changes have occurred within a quarter, an audit is performed and Network Management will make "dummy changes", or changes that do not directly affect the operation or compromise the security of a device but will be seen as an exception, and verify that an exception report is properly generated and the Networking team takes appropriate corrective and investigative action within 24 hours.

Control Activity Mapping

The following table describes to which business platforms the controls apply or whether it is a corporate control:

Control Activity #	Control Activity	Corporate	Managed Hosting	Dedicated Hosting	Colocation
7.1	Management has defined a baseline configuration for servers and network elements and new systems are configured according to the baseline.	√	√	√	
7.2	Changes to baseline configurations applied to servers and network elements are authorized and tested prior to implementation.	√	√	√	
7.3	Periodic testing and assessment is performed to confirm that software and network infrastructure is appropriately configured.	√	√	√	√

8. MANAGE PROBLEMS AND INCIDENTS

Control Objective: Controls provide reasonable assurance that problems and/or incidents are responded to, recorded, resolved or investigated for resolution.

Management has defined and implemented a service desk function such that customer impacting events that are not part of the standard operation are recorded, analyzed and resolved in a timely manner.

Customer Support

A service desk function is implemented to ensure that customers have access to service and support 24x7 via a MyPEER1 customer web portal or by phone. The customer portal, which is a central contact point, is available to managed hosting and dedicated customers to place service requests, review their orders and invoices, update their contact information, and to obtain any technical support. Managed hosting and dedicated hosting customers can report events by contacting Support. Colocation customers, at the present time, initiate these requests with their customer relations representative or the technical support team (NOC) via email or telephone to resolve support related issues. A PEER 1 Hosting manager or team lead is available 24x7 to monitor customer support operations. The manager or team lead will review operations real-time to ensure the call queue, service request response times, and call load are being efficiently worked on and resolved. To improve upon existing customer service satisfaction, customer surveys are sent out regularly and reported to PEER 1 Hosting's management on a regular basis for analysis and improvement. These various platforms provide resolution of customer related issues in a proactive and timely manner.

Procedures are in place to with the intention that customer incidents which are not part of the standard operations are recorded, analyzed, and resolved in an effective manner. Customer data is handled confidentially with technical support access limited to authorized client relations representatives (Refer to Objective 6 "Ensure System Security"). After verification of the individual's authority to request services, the client relations representative will open a service request (referred to as a "ticket") in the applicable customer management system (Ocean) or ticketing system (JIRA or RT). DC Operations or Support can also create tickets in Ocean for managed hosting customers if they observe alerts or issues through the Hyperion monitoring portal. A ticket pertaining to managed hosting or dedicated hosting problem or incident is tracked and retained in Ocean.

JIRA and RT are internal ticketing systems used by PEER 1 Hosting to record, analyze, and resolve problems and incidents. This system is used by multiple departments to initiate and track incident resolution. The ticket is classified by type and automatically routed to an appropriate representative via established protocols and escalation procedures. Support uses RT to track and retain colocation problems or incidents. Based on established guidelines and procedures, the support personnel act in a triage capacity to resolve the problem or route the ticket to appropriate specialists based on operating system and the criticality of the issue for further investigation and resolution. The Vancouver NOC uses RT to track tickets relating to abuse, issues with the PEER 1 Hosting backbone, escalated tickets from other departments, and also for support relating to colocation customers. IT Operations uses JIRA to track tickets relating to corporate network and systems issues.

On a monthly basis, management of PEER 1 Hosting meets to discuss support metrics of the month. The support metrics report tracks call center activities including the total number of calls, dropped or abandoned calls, the total number of tickets, mean-time to resolve, volumes, re-opened ticket numbers and reasons for churn. Issues such as slow resolution times, dropped calls are identified and remediating activities are implemented to improve the problem resolution performance.

Incident escalation procedures are defined and implemented. Post mortem analysis is performed for critical incidents and the results are communicated to impacted customers in a timely manner.

Incident Procedures

PEER 1 Hosting has established incident escalation procedures to address and resolve incidents in a timely manner. These procedures are reviewed and updated on an as required basis. These procedures govern critical, major or minor incidents which may impact business operations. Upon the internal discovery of a critical, major or minor incident, management is notified immediately and the event is evaluated and assigned an incident level (critical, major, or minor). Once the event level is determined, the appropriate level procedures are followed.

Critical incidents require multi-departmental management team cooperation or impact a large number of customers due to unavailability of critical functions or services. PEER 1 Hosting monitors a critical alias email box for critical incidents reported by employees. Critical incident management procedures including the escalation process are documented and posted on PEER 1 Hosting's intranet. Communication tools such as conference bridges, PEER 1 Hosting forums, and email system are used for incident reporting, problem escalation, resolution documentation and customer notification. Formal post mortem analysis is performed and communicated to impacted customers in a timely manner for critical incidents.

Major incidents result in partial failure of a redundant system or data center/network infrastructure which impacts a moderate number of customers. In addition, a minor incident which is not resolved within 24 hours or escalated by management from a minor incident is also considered major incident. PEER 1 Hosting monitors a centralized email box for major incidents reported by employees. Management may, at its discretion, use conference bridges, forum or Twitter updates, and emails to keep staff and customers updated on the status of the incident. If a service outage occurs at this level, potentially affected customers should be notified by email, ticket, or phone as soon as the incident is identified. If the impact on customers is not readily apparent, all customers who contact a client relations representative will be advised of the event.

Minor incidents are events such as partial failure of redundant system, internal infrastructure failures, or data center/network infrastructure which either does not impact customer performance or where only a minimal number of customers are affected. All internal updates are sent to a minor email alias monitored by PEER 1 Hosting. Customers are not required to be notified of this incident but management may, at its discretion, post updates on PEER 1 Hosting forums and via Twitter. No official post mortem is required for minor incidents.

Management reviews critical incident reports on a monthly basis to identify trends and root causes of the incidents.

Trend and Root Cause Analyses

On a monthly basis, the Director of Network Operations summarizes the critical and major incidents for the prior month in a PowerPoint presentation and distributes the report to the senior management team. The senior management team is comprised of directors and above positions from Operations, Data Center Operations, and Support. During the second Thursday of every month, the results are reviewed at the monthly Operations Execution Meeting with attendees from Operations, Data Center Operations, Support and Client Relations. The discussions are primarily focused on SLA effecting events and customer effecting outages. The meetings will include discussions related to underlying root causes of the incident, resolution plan implemented, any continual maintenance required, and action roadmap for outstanding issues not yet resolved. For recurring issues, the team will also identify and evaluate recommendations to mitigate future occurrences of similar incidents.

Control Activity Mapping

The following table describes to which business platforms the controls apply or whether it is a corporate control:

Control Activity #	Control Activity	Corporate	Managed Hosting	Dedicated Hosting	Colocation
8.1	Management has defined and implemented a service desk function such that customer impacting events that are not part of the standard operation are recorded, analyzed and resolved in a timely manner.	√	√	√	√
8.2	Incident escalation procedures are defined and implemented. Post mortem analysis is performed for critical incidents and the results are communicated to impacted customers in a timely manner.	√	√	√	√
8.3	Management reviews critical incident reports on a monthly basis to identify trends and root causes of the incidents.	√	√	√	√

9. MANAGE DATA AND BACKUPS

Control Objective: Controls provide reasonable assurance that data backup and recovery processes are defined and managed consistent with backup and retention plans and schedules.

Management has implemented procedures for data storage and retention of data.

Backup Policies and Procedures

PEER 1 Hosting maintains backup policies and procedures related to the backup of customer and corporate systems. The policies and procedures address what elements of customer data is subject to backup service, the frequency of backups and for the retention periods. The backup policies and procedures apply to all customers who have subscribed to the backup services.

To ensure new Managed or Dedicated customers who subscribe to the backup services are being provided with the service, the Backup team manually check the exception reports on a daily basis which are automatically updated at 9:00am EST each day. The reports are generated to identify customers who are subscribing to the backup services in our management systems but have not been provisioned with the backup services on a server.

Two primary Tivoli backup services are offered to all business platforms:

- Daily Incremental
- Weekly Incremental

There are notification procedures in place to advise the backup team when customers request a change to their backup service. Such processes include notifying the backups department when the customer adds or cancels backup services, or changes the backup service frequency.

In addition, managed hosting customers can subscribe additional add-on services which are not available to the dedicated hosting and colocation business platforms: Tivoli TDP Daily for MSSQL and Tivoli TDP Weekly for MSSQL. MSSQL backups run every hour (1 full database backup daily or weekly depending on the customer's plan and hourly logs for daily customers or logs every 4 hours for weekly customers). Managed hosting customers also have the option to back up their data locally on the Tivoli systems at each data center or remotely and offsite. For customers who select the remote option, data is backed up to a remote data center (no local data is kept on any local Tivoli system). For customers who select the offsite option, data is backed up to a local Tivoli system at the same data center in which the servers are located and also replicated to a remote location for additional redundancy.

Procedures are defined and implemented to prevent access to backup data stored.

Access Restrictions

Access to sensitive information stored on Tivoli storage devices are restricted to authorized customers and PEER 1 Hosting personnel.

During the backup provisioning process, the customer is provided with a welcome letter which provides details on how to access the information on their Tivoli Storage Manager (TSM) server. Every time a customer logs into the web

graphic user interface to access the data on the TSM database, the customer is required to authenticate login credentials against the information stored in OCEAN. After seven failed attempts, the account will be locked out and can only be unlocked by the backup administrators. The PEER 1 teams (such as Support and Backup) will validate the customer's identity prior to disclosing credential details or other sensitive information related to the customer's backup service.

Corporate access to customer backup servers is also restricted to authorized PEER 1 Hosting personnel. In order to grant access, approval must be obtained before the backup administrators will set up the access rights. Access can be either onsite or via VPN into the corporate domain. Beyond the authentication credentials that are required to access the corporate network, a unique login and password is required to access the TSM servers and databases.

Retention periods and storage terms are defined for managed data and related software, in accordance with contractual requirements.

Retention and Storage

Servers are backed up daily or weekly, respectively, and one copy of active files is retained on the file system, which PEER 1 Hosting retains as long as the customer subscribes to the backup service, and six revisions/changes of individual files, which will expire 30 days after their deletion or modified date. Customers and corporate PEER 1 Hosting's corporate departments can choose between either services, and may specify when they wish to have their system backed up either daily or weekly.

Backups are automatically scheduled defined by PEER 1 Hosting during low traffic times unless a customer specifies otherwise. The daily and weekly backups for customers are run outside of standard business hours. Each customer's first backup is a full backup, all subsequent backups are incremental, regardless of whether it is daily or weekly backups. Automated backup software is used to schedule and manage the backup process. The automated backup software is also configured to back up some customers' data to remote data centers, depending on where the customers are located and if the customer has subscribed for the remote backup option.

Procedures are in place to restore corporate or customer backups when requested.

Restoration Procedures

System restoration is an important element of PEER 1 Hosting's disaster recovery efforts and is managed by IT Operations in collaboration with the Operation Groups. On a semi-annual basis, IT Operations perform two system restores of business critical systems. The three types of restores that are performed are:

- A system of hardware upgrade
- A system restore for a failed or crashed system
- Semi-annual testing and full restoration of two systems to ensure effectiveness of the restoration process

Corporate restores are performed on request and semi-annual restores are done to verify restore procedures and their effectiveness. To place a restoration request, the employee will submit a ticket to IT Support at the assigned email alias. IT Operations and Corporate Security will coordinate with the applicable departments to perform the restore. The application owner is responsible for system restores. IT Operations handles the operating system layer and the database administrators will handle all database restore requests. Restores of data backups are performed for customers on request only. Customers can either perform their own restores without advising PEER 1 Hosting or

they may contact PEER 1 Hosting to request a restore. If PEER 1 Hosting assists with the customer's restoration process, a ticket will be opened to initiate and track the status of the request.

Procedures are in place to dispose or remove customer data upon de-provisioning to prevent unauthorized access to customer data.

Hardware Disposal

When hardware is re-provisioned or disposed of, PEER 1 Hosting has a process in place to clean the equipment of customer information. The process includes decommission of customer servers and erasing customer data, as well as backup servers and SAN storage. The drives are wiped using software. Disposal of SAN storage devices, such as disk drive reformat, overwrite or physical destruction, is processed by EMC Corporation. The results of the server and storage decommission and hard drive data cleansing is recorded in the Ocean ticketing system.

Control Activity Mapping

The following table describes to which business platforms the controls apply or whether it is a corporate control:

Control Activity #	Control Activity	Corporate	Managed Hosting	Dedicated Hosting	Colocation
9.1	Management has implemented procedures for data storage and retention of data.	√	√	√	√
9.2	Procedures are defined and implemented to prevent access to sensitive information stored.	√	√	√	√
9.3	Retention periods and storage terms are defined for managed data and related software, in accordance with contractual requirements.	√	√	√	√
9.4	Procedures are in place to restore corporate or customer backups when requested.	√	√	√	√
9.5	Procedures are in place to dispose or remove customer data upon de-provisioning to prevent unauthorized access to customer data.	√	√	√	

10. MANAGE FACILITIES

Control Objective: Controls provide reasonable assurance that physical access to PEER 1 Hosting data centers and customer systems are limited to authorized personnel and protected against environmental threats.

Access to facilities is restricted to authorized personnel and requires identification and authentication.

Access Controls

Each PEER 1 Hosting data center is physically secured, monitored, and controlled by an access badge system. For each of the facilities, permanent and temporary access badges are granted to authorized PEER 1 Hosting personnel and third-party service providers, respectively. Contractors are provided with a temporary access badge to enter a PEER 1 Hosting facility. The contractor must provide some form of collateral (e.g. driver's license) in order to sign for the badge. This identifies the contractor and encourages them to return their badges to PEER 1 Hosting after the service is completed. Some contractors that are coming by on a daily/weekly basis have their own cards.

Generally, managed and dedicated hosting customers do not have access to the data center facility unless it is by special request. The data center manager or other authorized personnel must escort all visitors, managed hosting customers, and dedicated hosting customers at all times within PEER 1 Hosting data centers. Depending on the nature and duration of the work engagement, vendors and contractors may be escorted by either an authorized personnel or the data center staff will regularly check on the vendors and contractors' status within the facility. For colocation facilities, colocation customers are granted access badges with 24x7 access to the facility section where their server is stored. Customer access rights are cancelled within the access badge system and the badges are returned to PEER 1 Hosting when the service agreement between PEER 1 Hosting and the customer is terminated.

Permissions for these access badges are set up under the principle of least privilege whereby PEER 1 Hosting personnel, third-party service provider, or customer are given the minimum access required to perform the job or access the cabinet where their servers are stored. On a quarterly basis, there is a collective effort among Corporate Security, IT Operations, and DC Operations to audit corporate level access rights to ensure there were no unauthorized access rights granted or deviations from the established guidelines. Colocation customer badge audits are performed semi-annually by IT Security to ensure that access rights are current and former customers' access have been deactivated in a timely manner.. As a consequence of including colocation customers, the audits shall also include cards issued to contractors, vendors, and visitors (as well as any other cardholder – this procedure is being changed from an audit of employee badges to an audit of every badge)

PEER 1 Hosting also controls physical access by authenticating visitors and contractors before authorizing access to the data center facility and hosting servers. Some facilities maintain sign-in sheets to capture information which includes name of person visiting, organization name, purpose and date of visit, time of entry and departure, badge number or visitor pass assigned, signature of visitor or contractor, and DCO technician handling the sign-in. Customers with access badges are not required to fill out the sign-in sheet.

Corporate Security and Data Center Operations are responsible for creating the policies and procedures regarding physical access controls within the facilities. This team works collaboratively to determine and assign appropriate levels of access based on the least privilege concept outlined in the Physical Access Policy. These levels will be

reviewed either quarterly (for corporate access) or annually (for colocation customers) to ensure that there are no unnecessary privileges assigned.

PEER 1 Hosting employs Access Control Systems (ACS) to control computer-networked card reader and alarm systems. The ACS uses proximity card readers to control access into perimeter doors, shipping/receiving areas, storage rooms, and other critical areas. Some PEER 1 Hosting facilities, including the Los Angeles, Miami and Toronto (Pullman location) data centers have Biometric Fingerprint Scanners to protect the most sensitive parts of PEER 1 Hosting data centers and networks. This "two factor authentication" mechanism associates fingerprint geometry (what you are) with an access badge (what you have). The ACS is also used to monitor, notify and log security alarms; monitor perimeter doors, restricted area doors, electrical / UPS room doors, network area doors (where applicable), shipping and receiving doors, and staging area doors. The ACS is equipped and programmed to receive alarms for forced doors, propped doors, unknown card read attempts, and denied card read attempts. Security systems have 24x7 UPS systems and standby emergency power (generator) support.

Physical facilities are equipped with environmental controls to maintain systems and data, such as fire suppression, uninterrupted power service (UPS) power backup, air conditioning and elevated floors.

Environmental Controls

A monitoring system is in place at all facility locations which monitors environmental controls and alert data center staff to potential issues. This system is managed either by PEER 1 Hosting (data center staff or NOC) or the management company who manages the building. The monitoring system has multiple access levels and password to restrict user access as appropriate. The level of monitoring varies across data centers and may include the following:

- Power systems - critical electrical components such generators, transfer switch, main switchgear, power management module and uninterruptible power supply equipment.
- The Heating Ventilation and Air Conditioning (HVAC) system - which controls or monitors space temperature and humidity within the IDC, space pressurization, HVAC equipment run status and performance, and outside air conditions.
- Temperature and water detection monitoring.

For selective data center facilities where remote monitoring and reporting activities are limited, Data Center Operations staff will perform walk-throughs during their shifts to ensure these critical systems are functioning effectively. In addition, external technicians perform regular equipment and maintenance checks to ensure that all fire detection and suppression, power management and HVAC equipment are working properly. Insurance is also in place for all such critical equipment.

Data center facilities are equipped with fire suppression to meet or exceed local building code requirements. This could include dry-pipe pre-action, halotron (or equivalent), with detection types including photo-electric, ionization, and heat sensors above and below raised floor systems, All facilities are equipped with clean agent fire extinguishers.

Facilities are equipped with fire extinguishers throughout the premise. Dry chemical or clean agent extinguishers are installed in the mission critical space, or adjacent areas, where one might reasonably expect a person to carry them into the affected areas during an emergency. The fire suppression system is monitored 24x7. Inside some of the data centers, software is used for fire detection and monitoring, combined with customized floor plan graphics to illustrate detection devices and fire zones to aid data center staff and the fire department in responding to and coordinating all fire control activities.

Each facility is powered by a dedicated utility step-down transformer for each service. The incoming service is connected to an automatic transfer switch, which is also connected to redundant stand-by diesel generators. Electrical loads served by the incoming service and generator sources include mission-critical, life safety, HVAC and general-purpose loads.

The critical mechanical and electrical components in the building of most PEER 1 Hosting data centers are designed with redundancy. The mission critical electrical loads at each location are sourced by a UPS system. Depending on the facility, the UPS in place may be one single source of power (one UPS system), parallel UPS systems which service separate parts of the data center, or redundant UPS systems.

Whenever possible, PEER 1 Hosting makes use of PMMs and/or Power Distribution Units (PDUs) on elevated floors to provide for a physically integrated and electrically redundant system for source selection, isolation, distribution, monitoring and control of power to internal and customer computer loads. PEER 1 Hosting has diesel engine generators in place at each location to provide power to all critical equipment and customer loads. Generators may be located indoors or outdoors depending on site-specific conditions. Separately installed main fuel tanks provide a source of fuel to all engine-generators. These on site fuel storages are sufficient to provide at least 12 hours of design load operation (or as much fuel as local authorities will permit). Each data center also has a short-notice refueling contract for the diesel generators to ensure sufficient generator back-up capabilities.

PEER 1 Hosting maintains multiple HVAC units within each facility to verify correct temperature and humidity settings in critical areas. The average temperature within each zone is maintained to meet ASHRAE server inlet temperature standards, as appropriate for the area. If the temperature or humidity varies outside early-warning, pre-set sensitivity limits, an alarm is generated within the NOC area and facilities personnel are notified. The HVAC units are powered by both normal and emergency electrical systems for redundancy.

Environmental controls are subject to maintenance as per vendor specifications.

Data Center and Environmental Controls Maintenance

Since 2010, PEER 1 Hosting has engaged maintenance service providers, eVolve Data Center Solutions (eVolve) for most of the in-scope data centers, except for the Los Angeles data center. EVolve schedules maintenance for the environmental controls and sends out notifications to the respective data centers when maintenance work is scheduled. EVolve is responsible for coordinating to receive and distribute the maintenance/service reports to respective data centers. A maintenance cost equipment master summary which includes listings of all the equipment and associated maintenance costs/service providers/maintenance frequency is maintained. Digital Realty owns the Los Angeles data center facility and is responsible for maintaining the environmental devices at that facility. Digital Realty is also responsible for monitoring and responding to environmental system alerts and resolving issues relating to the environmental hazard.

Management has a process in place to monitor the facilities and react to alarms related to unauthorized access and environmental threats to the facilities.

Security Surveillance

PEER 1 Hosting operates CCTV monitoring, recording and control equipment within each data center facility. Depending on the data center, this surveillance function may be performed on an ad-hoc basis by data center staff, Network Operations, or Corporate Security. Exterior cameras are positioned to provide views of critical support equipment, perimeter doors, and parking areas (where applicable). Interior cameras are positioned to monitor

perimeter doors, data center main entry/exit, data center raised floor entry/exit, cage aisle ways, shipping and receiving areas, high security vaults, and other areas as appropriate. Cameras record activity on site via digital video recorders 24x7 to provide a visual record of activity at the data center. Recordings are kept for a minimum of 90 days in a secured location.

Facility Capacity

On a monthly basis, PEER 1 Hosting management reviews the facility capacity metrics report, which tracks physical capacity (including total capacity, ready, utilized and available) and protected power capacity (including total kW, current kW, sold kW and power percentage utilized) for all of the data centers. This report is reviewed as part of the monthly operations management meetings, and issues identified are followed up for investigation.

Colocation customer environments are physically segregated from other customer systems at each data center.

Customer Environment Segregation

Colocation customers have access to their servers which are physically secured within locked rooms, cages or cabinets and do not have access to areas housing managed and dedicated hosting customer equipment. Managed and dedicated hosting customers do have not access to the data center facility and the servers unless arrangements are made with and approved by authorized PEER 1 Hosting personnel. Access to these areas is protected by the access badge system described above. Access doors to these areas are under 24x7 video surveillance.

Control Activity Mapping

The following table describes to which business platforms the controls apply or whether it is a corporate control:

Control Activity #	Control Activity	Corporate	Managed Hosting	Dedicated Hosting	Colocation
10.1	Access to facilities is restricted to authorized personnel and requires identification and authentication.		√	√	√
10.2	Physical facilities are equipped with environmental controls to maintain systems and data, such as fire suppression, uninterrupted power service (UPS) power backup, air conditioning and elevated floors.		√	√	√
10.3	Environmental controls are subject to maintenance as per vendor specifications.		√	√	√
10.4	Management has a process in place to monitor the facilities and react to alarms related to unauthorized access and environmental threats to the facilities.		√	√	√
10.5	Colocation customer environments are physically segregated from other customer systems at each data center.				√

COMPLEMENTARY USER ENTITY CONTROLS

PEER 1 Hosting's managed hosting services, dedicated hosting services and co-location services and its related controls were designed with the assumption that certain controls would be placed in operation by user entities. Section 3 describes some of the controls that should be in operation at user entities to complement the controls at PEER 1 Hosting. User auditors should consider whether these controls have been established at user organizations.

SECTION 3 – INFORMATION PROVIDED BY SERVICE AUDITOR

INTRODUCTION

This report on the internal controls placed in operation and tests of operating effectiveness is intended to provide interested parties with information sufficient to obtain an understanding of those aspects of PEER 1 Hosting's controls that may be relevant to a user organization's internal control structure. This report is also intended to provide information sufficient to reduce the assessed level of control risk below the maximum for certain financial statement assertions. This report, when coupled with an understanding of internal controls in place at user organizations, is intended to assist in the assessment of internal controls surrounding transactions processed by PEER 1 Hosting.

Our examination included inquiry of the appropriate management, supervisory and staff personnel; inspection of documents and records; observation of activities and operations; and tests of controls implemented by PEER 1 Hosting. Our tests of controls were performed on internal controls as they existed during the period July 1, 2012 to June 30, 2013 and were applied to those controls relating to control objectives specified by PEER 1 Hosting. Our report is dated July 26 2013, the last day of our testing activities.

The description of controls and control objectives are the responsibility of PEER 1 Hosting. Our responsibility is to express an opinion that the controls were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified by PEER 1 Hosting were achieved during the period covered by our report.

TESTS OF OPERATING EFFECTIVENESS

Our tests of the control environment included the following procedures, to the extent we considered necessary:

Ref	Evaluation procedure	Description
1	Corroborative Inquiry	Made inquiries of appropriate personnel and corroborated responses with tests 2, 3 or 4 below to ascertain compliance with the control activity.
2	Observation	Observed application of the control activity.
3	Inspection of Evidential Material or Examination of Documentation	Inspected documents and reports indicating performance of the control activity.
4	Reperformance	Reperformed operation of the control activity.

The combined results of these procedures provided the basis for our understanding of the design of the system as of June 30, 2013 and the rendering of our opinion in accordance with the requirements set forth in the audit standards. Our test of the operating effectiveness of controls included such tests as we considered necessary in the circumstances to evaluate whether the controls and the extent of compliance with them, is sufficient to provide reasonable, but not absolute, assurance that the specified control objectives were achieved during the period July 1, 2012 to June 30, 2013.

In designing our test of controls strategy, we considered the (a) nature of the items being tested, (b) the types and adequacy of available evidential matter, (c) the nature of the audit objectives to be achieved, (d) the assessed level of control risk and (e) the expected efficiency and effectiveness of the test.

In cases where the key controls were standardized, test samples were selected across locations. Testing samples were selected in accordance with accepted auditing standards.

Deloitte examined evidence supporting the effective operation of control activities performed by PEER 1 Hosting. It is each user auditor's responsibility to evaluate this information in relation to the controls in place at each user organization. If certain complementary controls are not in place at user organizations, PEER 1 Hosting's controls may not compensate for such weaknesses.

The results of our tests of the operating effectiveness of controls are described in the following table. Where relevant exceptions were noted, PEER 1 Hosting has included a management response. Unless otherwise indicated, the management response has not been subject to audit procedures.

In addition to the tests listed below for each control specified by PEER1 Hosting, Deloitte ascertained through inquiry with management and the control owner that each control activity listed below operated as described throughout the period.

1. MANAGEMENT OF IT

Control Objective: Controls provide reasonable assurance the management has implemented a planning and governance process within IT.		
PEER 1 Hosting Control Activity	**Deloitte Test of Control**	**Results**
1.1 Management maintains an IT strategic plan that outlines future strategies, initiatives and risks facing the organization.	a) Inspected the PEER 1 Hosting IT Strategic Plan for future strategies, initiatives and risks facing the organization. b) Inspected the annual IT plan and ascertained that it is linked to the IT Strategic Plan.	No exceptions noted.
1.2 Management has documented and communicated policies, procedures and controls governing the IT organization's activities.	a) Inspected the Corporate Security Policies and confirmed that policies for key areas of IT activities have been documented. b) Inspected evidence of communications of the policies and procedures to PEER 1 Hosting employees.	No exceptions noted.
Complementary User Entity Control Considerations: The customer is responsible for their own strategic and operational planning process. The customer policies and procedures have not been assessed by Deloitte.		

2. MANAGE HUMAN RESOURCES

Control Objective: Controls provide reasonable assurance that policies and procedures are in place to support the hiring and development of personnel.		
PEER 1 Hosting Control Activity	**Deloitte Test of Control**	**Results**
2.1 Management has a standard hiring process, including approval to hire and performing background and reference checks.	a) Inspected evidence of the recruiting process and confirmed that a formal process is in place. b) Selected a sample of newly hired PEER 1 Hosting personnel and ascertained that management confirmed their qualifications and skills prior to hiring. c) For the sample selected in b), confirmed that background and reference checks were performed.	For 7 out of 15 selected new hires, including both employees and contractors, background checks (including criminal, education and working experience checks) were not performed. These exceptions related to contractors only. No exceptions were noted for employees. Additional testing was performed on June 25, subsequent to the management remediation on May 12, and no exceptions noted. **Management response:** PEER 1 Hosting remediated this process as of May 12, 2013. PEER 1 Hosting conducted background checks for all existing contractors who had access privileges to PEER 1 Hosting's corporate network and no unfavorable screening results were found.
2.2 Management provides training and development necessary to fulfill job responsibilities.	a) Ascertained through inquiry that management provides training and development necessary to fulfill job responsibilities. b) Obtained and inspected documentation to ascertain that management has assessed skills to identify development areas, and has provided training to fulfill those needs. c) Obtained and inspected documentation to ascertain that a tuition reimbursement program is in place allowing staff to obtain necessary skills to fulfill job responsibilities.	No exceptions noted.
Complementary User Entity Control Considerations: The customer is responsible for ensuring the appropriate human resource management processes are in place to support their own personnel.		

3. MANAGE OPERATIONS AND MONITORING

Control Objective: Controls provide reasonable assurance that data center operation tasks are performed and processing issues are monitored.		
PEER 1 Hosting Control Activity	**Deloitte Test of Control**	**Results**
3.1 Management has documented and implemented standard operating procedures to maintain the data center.	a) Inspected the standard operating procedures used by the data center staff and confirmed that the procedures include guidelines for staff daily duties and standards for regular equipment maintenance.	No exceptions noted.
3.2 Management has defined shift-handover procedures, including handover of tasks, problems and incidents.	a) Confirmed that there are shift handover procedures in place at each data enter. b) Selected a sample of shift handover reports and confirmed that the reports include open problem tickets, operational tasks that need to be completed, and out of the ordinary items that may affect the next shift.	No exceptions noted.
3.3 Management has defined provisioning procedures to ensure customers subscribed service is provisioned in accordance with the sales order.	a) Confirmed that a process is in place to review the provisioning services. b) Selected a sample of services provisioned and inspected documentation to ascertain that provisioned services have been reviewed.	No exceptions noted.
Complementary User Entity Control Considerations: The customer is responsible for monitoring operations at the application or database layer. The customer is responsible for validating the services it subscribed to. Customers are responsible for reviewing and indicating action on reports received from vendors relating to Intrusion Detection Systems (IDS) or vulnerability scans.		

4. MANAGE CHANGES

Control Objective: Controls provide reasonable assurance that system changes affecting the customer environment are authorized, tested and implemented in a timely manner.		
PEER 1 Hosting Control Activity	**Deloitte Test of Control**	**Results**
4.1 A documented change management procedure exists to govern programming, system or configuration changes to infrastructure systems, network devices and system software.	a) Inspected the change procedures for existence. b) Selected a sample of change control meetings and inspected evidence to confirm that meetings took place and were attended.	No exceptions noted.
4.2 Regular changes are documented and approved according to PEER 1 Change Management policies before the changes are implemented.	a) Selected a sample of regular changes and inspected change documentation to ascertain that test plans and backout plans exist, and approval was obtained according to PEER1 Regular Change Management Policies	No exceptions noted.
4.3 Emergency changes are documented and authorized (including after-the-fact approval) in a timely manner according to PEER 1 Change Management policies.	a) Selected a sample of emergency changes and inspected change documentation to ascertain that test plans and backout plans exist, and approval was obtained according to PEER1 Emergency Change Management Policies	No exceptions noted.
Complementary User Entity Control Considerations: Customers can have administrator rights to their own systems and can therefore make changes that may not follow the PEER 1 Hosting change management process. Customers are responsible for changes to the application and database layers. Authorization of customer requested changes and end-user acceptance testing is the responsibility of the customer. Customer change management procedures have not been assessed by Deloitte.		

5. MANAGE PERFORMANCE AND CAPACITY

Control Objective: Controls provide reasonable assurance that system performance and capacity levels are monitored and that a process is in place to address suboptimal performance levels.		
PEER 1 Hosting Control Activity	**Deloitte Test of Control**	**Results**
5.1 Management monitors the performance and capacity levels of the internal and customer-facing systems.	a) Inspected the performance and capacity monitoring activities, and confirmed that the network capacity and uptime is subject monitoring through automated tools. b) Inspected the performance and capacity monitoring activities, and confirmed that internal and customer facing system capacity and uptime are subject to monitoring through automated tools. c) Confirmed that once capacity thresholds are reached, alerts are sent to the support team and problem tickets are created in the problem management system. d) Inspected online tracking reports, and confirmed that performance and capacity monitoring is reported to management on a regular basis.	No exceptions noted.
5.2 Management has a process in place to respond to suboptimal performance and capacity measures in a timely manner.	a) Inspected incident management procedures and confirmed a process in place to respond to suboptimal performance and capacity measures in a timely manner. b) Selected a sample of problem tickets, initiated by customers or identified by the Support Team or Network Team through the performance or capacity monitoring tools; and obtained evidence of actions taken to resolve the issue.	No exceptions noted.
Complementary User Entity Control Considerations: PEER 1 Hosting offers performance and capacity monitoring tools to customers who subscribe to these services. It is at PEER 1 Hosting's customers' discretion to resolve performance and capacity problems themselves or through creating a ticket for PEER 1 Hosting's support. PEER1 Hosting is not responsible for responding to alerts unless the customer notifies them through the ticketing process. PEER 1 Hosting is only responsible for ensuring that the service has been provisioned appropriately.		

6. ENSURE SYSTEM SECURITY

Control Objective: Controls provide reasonable assurance that systems are secured to prevent unauthorized access, use, modification or loss of data.		
PEER 1 Hosting Control Activity	**Deloitte Test of Control**	**Results**
6.1 Management maintains and communicates security policies that address IT security requirements.	a) Inspected the IT Security Policy for existence. b) Inspected evidence of communications of the policies and procedures to the employees. c) Confirmed that management periodically reviews and updates the IT Security Policy.	No exceptions noted.
6.2 Procedures are followed to request, establish, issue, suspend, and close user accounts in a timely manner for new hires, job changes, and job terminations. The process includes approval of access rights based on the role of the user.	a) Confirmed that there is a process in place for establishing, issuing, suspending and closing user accounts. b) Selected a sample of new hires and confirmed that approval was obtained and their access to corporate network and customer systems was granted based on job role. c) Selected a sample of transfers and confirmed access for previous role was removed, and access for new role was granted based on the job position. d) Selected a sample of terminations and confirmed their access to corporate network and custom systems was removed in a timely manner.	No exceptions noted.
6.3 Access to customer impacting network devices, domains and system functions is restricted to authorized personnel.	a) Selected a sample of employees and verified that they were in the correct organizational units (OUs) according to their position in the organization. b) Confirmed network devices are protected by TACACS service.	No exceptions noted.
6.4 An audit process exists and is followed to periodically review and confirm access rights to systems and facilities.	a) Inspected the quarterly review for evidence the logical and physical access audits were performed. b) Selected a sample of quarterly audit tickets and confirmed audit procedures were followed and that exceptions were followed up.	No exceptions noted.
6.5 Procedures are in place to require complex passwords, with a minimum of 8 characters that change every 90 days, to access corporate and customer systems.	a) Inspected password policies and account lockout policies in the corporate network domain and confirmed they were properly configured to prevent unauthorized access. b) Confirmed that access to customer impacting network devices, domains and system functions is restricted to authorized personnel.	No exceptions noted.

Control Objective: Controls provide reasonable assurance that systems are secured to prevent unauthorized access, use, modification or loss of data.		
PEER 1 Hosting Control Activity	**Deloitte Test of Control**	**Results**
6.6 Logical segregation is in place to protect customer systems from the internet for customers that subscribe to the firewall service.	a) Confirmed that default configurations have been created for firewalls. b) Selected a sample of managed, dedicated, and colocation hosting customers who subscribed to the firewall services and confirmed through firewall logging activity that a firewall service is in place.	No exceptions noted.
6.7 Logical segregation is in place to protect the corporate network from the internet.	a) Confirmed that logical segregation is in place to protect the corporate network from the internet. b) Obtained list of trusted IPs from corporate firewall to verify that access to firewall is restricted.	No exceptions noted.
6.8 Procedures are in place to protect information systems from infection by malware (e.g. viruses, worms).	a) Inspected corporate and managed hosting McAfee ePo server configurations. Confirmed that the servers were configured to detect malware and perform scans on a periodic basis. b) Inspected summary reports of DAT versions installed on managed systems and confirmed systems were up-to-date.	No exceptions noted.
6.9 Management makes tested patches available to customers on a weekly basis.	a) Inspected patch management procedures for existence. b) Selected a sample of patches and confirmed patches were tested and approved prior to release. c) Selected a sample of patches and confirmed that they are made available to customers to install on servers.	No exceptions noted.
Complementary User Entity Control Considerations: Customers are responsible for the management and monitoring of administrator and user accounts (including passwords), and other access privileges to their systems. Customers are responsible for subscribing to the firewall service for their systems to be logically segregated from other customer systems. Customers are also responsible for subscribing to and monitoring the Control Scan reports that available to them and remediating vulnerabilities identified in these bi-weekly reports. In addition, customers are responsible for contacting PEER 1 Hosting for support when security intrusion threats have been identified by either themselves or Alert Logic. PEER 1 Hosting provides patches to their customers, but it is the customers' responsibility to ensure that patches are successfully installed on their systems. Certain customers have administrator rights to their servers, thus customers may update or change their system configuration settings and implement their own patches and fixes.		

7. MANAGE CONFIGURATION

Control Objective: Controls provide reasonable assurance that IT components as they relate to security, processing and availability, are protected, are designed to prevent unauthorized changes, and assist in the verification and recording of the current configuration.		
PEER 1 Hosting Control Activity	**Deloitte Test of Control**	**Results**
7.1 Management has defined a baseline configuration for servers and network elements and new systems are configured according to the baseline.	a) Inspected baseline configuration procedures for existence. b) Confirmed baseline configurations have been defined for operating system images. c) Confirmed baseline configurations have been defined for network elements.	No exceptions noted.
7.2 Changes to baseline configurations applied to servers and network elements are authorized and tested prior to implementation.	a) Confirmed that changes to baseline configuration have been defined, tested and rolled out into production as per change management documentation requirement.	No exceptions noted.
7.3 Periodic testing and assessment is performed to confirm that software and network infrastructure is appropriately configured.	a) Inspected Network Security Auditing procedures for existence. b) Selected a sample of dates and confirmed that RANCID had performed a scan of all network devices for changes. c) For the sample selected in b), confirmed that device configuration changes were scanned for a set of security related keywords and results were emailed to the engineering team for review. d) Selected a sample of corporate servers and validated that the systems were recently patched.	No exceptions noted.
Complementary User Entity Control Considerations: Customers are solely responsible for the configuration of the application and database layer. In addition, PEER 1 Hosting is only responsible for the initial set up of the network devices and the customers are responsible for their firewall rule sets in details according to the customers' own needs. Colocation customers are responsible for configurations of devices within the Colocation allocated space.		

8. MANAGE PROBLEMS AND INCIDENTS

Control Objective: Controls provide reasonable assurance that problems and/or incidents are responded to, recorded, resolved or investigated for resolution.		
PEER 1 Hosting Control Activity	**Deloitte Test of Control**	**Results**
8.1 Management has defined and implemented a service desk function such that customer impacting events that are not part of the standard operation are recorded, analyzed and resolved in a timely manner.	a) Confirmed that a problem and incident management process exists that addresses the recording and resolution of incidents, problems and errors in a timely manner. b) Selected a sample of incidents from the incident log. Confirmed that the incident detail was recorded and that the incidents were resolved in a timely manner. c) Obtained and inspected a sample of monthly support metric reports to ascertain that management reviews the performance of the support team on a monthly basis.	No exceptions noted.
8.2 Incident escalation procedures are defined and implemented. Post mortem analysis is performed for critical incidents and the results are communicated to impacted customers in a timely manner.	a) Inspected incident escalation procedures for existence. b) Selected a sample of incidents and the corresponding resolution logs. Confirmed incidents were escalated and closed in a timely manner and corresponding resolutions and notification to customers were recorded in the tickets.	No exceptions noted.
8.3 Management reviews critical incident reports on a monthly basis to identify trends and root causes of the incidents.	a) Confirmed that critical incident reports are reviewed on a monthly basis to identify trends and root causes of incidents. b) Selected a sample of meeting minutes to ascertain that management reviews critical incidents report on a monthly basis.	No exceptions noted.
Complementary User Entity Control Considerations: Customers are responsible for ensuring a process exists to facilitate the timely escalation of any problems impacting the customers' systems environment from PEER 1 Hosting to their customers, and for ensuring the subsequent resolution is appropriate. Customers are responsible for identifying and resolving application and data-related issues.		

9. MANAGE DATA AND BACKUPS

Control Objective: Controls provide reasonable assurance that data backup and recovery processes are defined and managed consistent with backup and retention plans and schedules.		
PEER 1 Hosting Control Activity	**Deloitte Test of Control**	**Results**
9.1 Management has implemented procedures for data storage and retention of data.	a) Inspected data backup policies and procedures for existence and confirm that the documents address PEER 1 Hosting and customer data backup and retention.	No exceptions noted.
9.2 Procedures are defined and implemented to prevent access to backup data stored.	a) Confirmed there are adequate controls to protect access to sensitive information (logically and physically). b) Inspected list of SAN users and confirmed that only authorized members of the backup and storage group have access.	No exceptions noted.
9.3 Retention periods and storage terms are defined for managed data and related software, in accordance with contractual requirements.	a) Inspected data backup policies and procedures for existence and confirm that the documents address PEER 1 Hosting and customer data backup and retention. b) Selected a sample of archived data, and obtain evidence that retention periods are being followed in conformance with the requirements. c) Selected a sample of customers that subscribe to the backup service and confirmed backups are being performed in accordance to the backup service the customer is subscribed to.	No exceptions noted.
9.4 Procedures are in place to restore corporate or customer backups when requested.	a) Inspected system restoration procedures for existence. b) Selected a sample of corporate restore tests and confirmed tests were completed successfully. c) Inspected that there was a recovery process in place to restore customer backups upon request.	No exceptions noted.

Control Objective: Controls provide reasonable assurance that data backup and recovery processes are defined and managed consistent with backup and retention plans and schedules.		
PEER 1 Hosting Control Activity	**Deloitte Test of Control**	**Results**
9.5 Procedures are in place to dispose or remove customer data upon de-provisioning to prevent unauthorized access to customer data.	a) Inspected de-provisioning and disposal procedures for existence. b) Selected a sample of decommissioned media and confirmed de-provisioning was documented, and in conformance with de-provisioning and disposal procedures.	For 5 out of 25 servers selected for de-provisioning testing, we were unable to obtain evidence noting the completion of customer data removal procedures upon service de-provisioning. These exceptions related to dedicated hosting customers only. No exceptions were noted for managed hosting customers. **Management response:** For these hard drives the automated process failed and the manual process followed by the DCO technicians did not include an audit trail. PEER 1 Hosting will educate all DCO technicians to fully document the de-provisioning processes. For another 3 out of the same 25 de-provisioned servers selected for testing, we observed that the decommissioned hard drives were labeled for de-provisioning and stored in the secured data centers for data erasure at a future date as outlined by PEER 1 Hosting's policies. However, those hard drives had not been erased at the time of our testing. These exceptions related to both dedicated and managed hosting customers. **Management response**: PEER 1 Hosting's policies do not currently specify an explicit timeline for completion of the de-provisioning process, including the erasure of related storage media. However, PEER 1 Hosting will review its de-provisioning procedure to consider making erasure time sensitive.
Complementary User Entity Control Considerations: Customers are responsible for subscribing to the backup service for their systems to be backed up on a regular basis. By default, all files on customer systems are automatically backed-up. Customers are responsible for requesting exclusions for any files they do not wish to have backed up. Customers are responsible for validating the results of their restoration requests, with PEER 1 Hosting's help, if required.		

10. MANAGE FACILITIES

Control Objective: Controls provide reasonable assurance that physical access to PEER 1 Hosting data centers and customer systems are limited to authorized personnel and protected against environmental threats.		
PEER 1 Hosting Control Activity	**Deloitte Test of Control**	**Results**
10.1 Access to facilities is restricted to authorized personnel and requires identification and authentication.	a) Through observation confirmed the operation of the physical access proximity card systems. Confirmed that access is only granted if an authorized proximity card is used. b) Selected a sample of individuals per location with access to the respective facilities. Confirmed that their access appears reasonable based on their job description. c) Obtained and inspected sample of quarterly user access audits to ascertain that user access rights are reviewed on a quarterly basis. d) Obtained and inspected sample of colocation customer access audits to ascertain that colocation customer rights are reviewed on an annual basis.	No exceptions noted.
10.2 Physical facilities are equipped with environmental controls to maintain systems and data, such as fire suppression, uninterrupted power service (UPS) power backup, air conditioning and elevated floors.	a) Observed the presence of the fire suppression, uninterruptible power supply (UPS) and smoke detector, Ventilation and Air-Conditioning (HVAC) systems in each location. b) Observed the existence of elevated floors within the data center server rooms.	No exceptions noted.
10.3 Environmental controls are subject to maintenance as per vendor specifications.	a) Selected a sample of maintenance logs for environmental control systems (such as Generators, UPS, PDU, HVAC, Fire Systems) and confirmed that regular maintenance was being performed and any issues were noted and remediated.	No exceptions noted.

Control Objective: Controls provide reasonable assurance that physical access to PEER 1 Hosting data centers and customer systems are limited to authorized personnel and protected against environmental threats.		
PEER 1 Hosting Control Activity	**Deloitte Test of Control**	**Results**
10.4 Management has a process in place to monitor the facilities and react to alarms related to unauthorized access and environmental threats to the facilities.	a) Confirmed a process is in place to monitor facilities and react to alarms related to unauthorized access and environmental threats. b) Inspected email alerts to ascertain that automated alerts are generated by the security and environmental monitoring systems c) Obtained and inspected a sample of monthly facility capacity reports to ascertain that management reviews facility capacity on a monthly basis.	No exceptions noted.
10.5 Customer environments are physically segregated from other customer systems at each data center.	a) Through physical inspection of each datacenter, ascertained that customer environments are physically segregated from other customer systems.	No exceptions noted.
Complementary User Entity Control Considerations: PEER 1 Hosting provides or removes card access to data centers based on the instructions received from authorized customer personnel. Customers are responsible for managing physical access rights for non-PEER 1 Hosting personnel to the customers' physical systems environment (e.g. cages).		