**Consolidated Client Confidentiality**

**and Security Requirements**

**SECURITY FOLLOW-UP AND NEW TEAM MEMBER CHECKLIST**

Security follow-up: 5/01/12

Agreed-upon Security Parameters:

• Locked War Room (with digital bio lock) for Brand – access only for core Brand team

• Windows in war room tinted so that no one may see in

• NDA’s for all employees (part of everyone’s new hire paperwork)

• NDA’s for all vendors that are used across XXX divisions

• Formalized employee on-boarding and removal process: If and employee is moved on or off account, will make sure the change form is prepared by the Brand Director or Brand Group Director and given to IT in advance of or at time of addition/departure

o Employees to agree to the following terms: must not use thumb drives/firewire drives, must not use drop box accounts, must notify us immediately if they lose their phone or laptop, the allowed FTP is only through the approved services provided by ZZZZ/YYY, all printed materials that contain confidential/sensitive info must be shredded after use, must set personal lock on phone that is made up of a complex passcode (ie, not 1234)

• Mail Server to be tested for intrusion scans and vulnerability scans to confirm that it meets XXX guidelines

• Background checks to be made for all director levels, Accounting and IT hires effective April 1, 2012

• Paper shredder in War room that is designated XXX

• Separate server to be set up with current password protocol for those needing access to ensure better control of those with access and to be able to review log reports for sensitive assets –only IT to have administrator rights

• Upon agency move, the team will be housed in a separate building, which has fewer windows and only two doors (front and back) to reduce risk of outside intrusions

• The team will have all have new Mac’s which allow for encryption software (file vault)to reduce risk of data being compromised in case of theft

• Team to have pass-code locks on their smart phones to reduce risk of data being compromised in case of theft

• IT to Install Mac Antivirus software on all team computers

• All employees to make sure auto logins are off, screen locks on, and firewall is on

• All employees to un-install any cloud based services ig. drop box

**follow-ups:**

• Review project policy for transferring assets including methods based on types of assets (e.g. When is email OK vs. Secure FTP)

• Discuss an interim solution to view videos or larger assets

New Team Member Checklist

As a member of the team, I understand the importance of confidentiality as it pertains to this piece of business and agree to the following security parameters:

• I will not use thumb/firewire drives for anything related to materials

• I will notify the Brand Director/IT immediately if I lose my phone or laptop containing any related materials

• I will not use any FTP services for the transmission of materials with the exception of the approved YYY/ZZZ FTP service

• I will shred all printed materials that contain confidential/sensitive info after they have been used

• I will work with IT to ensure that as it applies to my work computer, all auto logins are off, all screen locks are on and the firewall is on

• I will set and keep my personal lock on my phone that is made up of a complex passcode (ie, not 1234) and keep it as such while I work.

• I will not use any cloud-based services (ie drop box and will uninstall any such services that currently exist on my work computer

Signed:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee’s Name Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee’s Signature Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Brand Director’s Signature Date

**THIRD PARTY SECURITY SURVEY**

XXX | Third-Party Provider

Security Survey

<Company Name>

Legend: <Company Name> Response (BLUE); XXX (RED)

Survey Purpose

This survey is used to understand a Third Party’s security posture in order to identify gaps in security controls, which may need to be remediated in advance of sharing or accessing sensitive data. The results of the survey will also inform the security exhibit portion of the contract governing the scope of work and/or master services agreement between us and the Third-Party.

Required Minimum Security Practices

This section describes minimum required security practices expected from Third-Party providers. Please confirm or describe how your company complies with the following topics and where your security controls do not fully meet the requirements below, please describe the gap and a proposed remediation plan or mitigating control for consideration.

1. Legal Contracts: Legal checkpoint for vendors, contractors and their subcontractors that a Master Services Agreement or Independent Contractor Agreement is in place, and it references their NDA, work for hire, ownership of assets, etc.; subcontractors must be approved and also under NDA.

2. Asset Exposure: Policies in place to limit sharing or access to data beyond the specific resources who require access and only for the period they require access.

3. Asset File Transfer: Use approved file transfer methods and NO alternatives, (e.g., agency FTP site or any cloud services or consumer services such as Dropbox, Google Drive, Amazon Cloud or Rackspace).

4. Asset File Storage: File storage must be logically stored to limited access only to those who have approved access and removed when the access is no longer required; logging must be enabled.

5. Termination/Risk: Disclose if an employee or subcontractor who had access to project data, assets or systems has been terminated or role changed warranting an “appropriateness of access review”.

6. Suspected Leaks: Report without delay any confirmed OR suspected leak or disclosure of Project material.

7. Data Protection and Handling: Comply with global data handling regulations and strong practices in handling sensitive data, e.g., consumer data, employee data, and privacy regulations.

8. Information and Physical Security Policies: Policies in place governing Information and Physical Security controls at your company.

9. Unique Authentication Credentials: No generic logins or shared account permissions permitted for user or administrator accounts; each individual must maintain unique username and password combinations which are not shared; periodic password reset scheduled (e.g. 90 day reset)

10. HR Screening/Background Checks: Background checks must be conducted for employees who may have access to sensitive information or areas.

11. Incident Response: Process must be in place to address information security incidents and reporting which includes disclosure of incidents which effect data.

12. Secure Enterprise Network: Must include an appropriately configured firewall, intrusion prevention solutions, VPN configuration and routine monitoring of infrastructure.

13. Mobile Device Management: PINs and/or passwords must be enabled on mobile devices that may contain or have access to sensitive information; remote wipe capabilities exist

14. Endpoint Protection: All devices must have current endpoint protection software installed, properly configured and running at all times (never disabled) to detect viruses, malware and malicious software; hard disk encryption in place for laptops and desktops.

15. Patch Management: A patch management process must also be in place.

16. Security Assessment: A security assessment should be periodically performed.

Additional Security Posture Considerations

This section describes additional security practices considerations regarding Third-Party providers. Please confirm or describe how your company policy for the following topics. These responses assist in forming a cumulative risk profile for this project or long-term partnership.

1. Physical office security

• Building access: Do you use keycards, codes, and security personnel to enforce physical security at your site?

• Shared building space: Are you in a large complex with shared common spaces with other companies?

• Visible access: Is there clear line of sight from neighboring buildings or the general public? Can external people easily see sensitive data inside your space?

• Workspace approach: How are individual artists physically arranged? Are they mixed in with other projects in a large open space? Do you have the ability to sequester projects?

• Visitors: When you have visitors (especially other clients) in your building how are they handled? Do they tour the open spaces where they might see our assets in progress?

2. Digital asset storage, protection, backup, management and access

• Storage: How is sensitive data stored (e.g., file server, user laptops, cloud storage)? How do you configure access?

• Data Backup: How is it backed up and who has access to the backups?

• Encryption: Removable data encryption (e.g., laptops, thumb drives)?

• Access Management: What is the process for requesting, granting and removing access – logically and physically?

• IT Support: Is IT Support outsourced, insourced, offshore?

3. Standard Policies and Certifications

• How do you regulate removable storage (e.g., thumb drives, external hard drives), and home/personal/commercial infrastructure use?

• What are your social media and electronic communications use guidelines?

• What is your company's personal guideline for discussing the project?

• Do you or any of your third-party providers perform periodic independent security audits or certifications (e.g. SSAE16, ISO27001)?

**UNILATERAL CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENT**

WHËREAS, prior to its disclosure of Confidential lnformation to Recipient, requires that Recipient enter into this Agreement to preserve the confidentiality and restrict Recipient's use of such Confidential information;

NOW THEREFORE, in consideration of XXX furnishing of confidential information to Recipient, and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, XXX and Recipient agree as follows:

1 . For purposes of this Agreement, "Confidential information" shall mean trade secrets, proprietary information, patents, trademarks, copyrights and other intellectual properly, and any and all other materials, documents and information, regardless of form and regardless of whether such is marked wilh the word "confidential," "proprietary," "trade secret" or a similar legend, (a) from which XXX derives independent economic value, actual or potential (whether or not used in XXX's busíness), due to the fact that such information (i) is not generally known lo the public or other persons in the entertainment software product or computer industries, or (ii) if generally known, is used, implemented, selected, arranged, assembled, grouped together or otherwise exploited by XXX in such a way that is not generally known, and (b) of which XXX exercises reasonable efforts under the circumstances to maintain the secrecy and prohibit the unauthorized use and disclosure, of or to which Recipient has already obtained, or may obtain, knowledge or access through or as a result of viewing XXX documents, observing or examining XXX's physical premises or property, or having meetings or conversations with XXX personnel or authorized agents or representatives. Confidential lnformation includes, but is not limited to,the following types of information and other information of a similar nature (whether tangible or intangible and whether or not reduced to writing): discoveries, ideas, concepts, software programs in various stages of development, prototypes, designs, drawings, patterns, plans, procedures, specifications, techniques, models, data, source code, object code, documentation, diagrams, forecasts, flow charts, research, development, processes, procedures, "know-how" and inventions, applied theories and ideas, management information systems, operations methodologies,policies and procedures, accounting practices, advertising information and concepts, marketing techniques and materials, markeling and development plans, customer names and other information related to cuslomers, price lists,

pricing policies, agreements, identity of and information relating to suppliers, developers, manufacturers, licensors and distributors, and sales, financial and personnel information. Confldential lnformation also includes any written or recorded summary or analysis of Confidential lnformation prepared by Recipient and any information described above that XXX obtains from anolher party and which XXX treals as proprietary or designates as Confidential lnformation, whether or nol owned or developed by XXX.

2. ConfÌdential lnformation shall not include any information that Recipient proves, by clear and convincing evidence, is (a) on or before the date Recipient obtained such information, known to Recipient, as evidenced by Recipient's written records, unless it was obtained from a third party who was under an obligation of confidentiality to XXX; (b) independently developed by Recipient; or (c) received from a third party who was not under an obligation of confidentiality to XXX.

3. Except as may be requíred by court order, subpoena or lawful demand of a governmental agency, Recipient agrees (a) to hold any Confidential lnformation obtained by it in the strictest confìdence, (b) not to directly or indirectly reveal, report, publish, disclose or transfer any Confidential lnformation to any person or entity (other than officers, directors and other employees of Recipient on a "need to know" basis who execute a written agreement to be bound by the terms of this Agreement), (c) make copies of any Confidential lnformation without XXX's prior written approval, or (d) utilize any of the Conlidential lnformation for any purpose whatsoever (other than for the sole purpose of evaluating a proposed business transaction or association with XXX). ln the event Recipient receives notice that it is required to disclose Confìdential lnformation pursuant to a court order, subpoena or lawful demand of a governmental agency, Recipient shall promptly notify XXX of such requirement prior to making any such disclosure and provide reasonable cooperation to XXX so that XXX may contest the required disclosure or 20\_, by and between XXX

intervene to seek appropriate protective orders. lf Recipient shall prepare any written or recorded summary or analysis of any Confidential lnformation, Recipíent shall ensure that such summary or analysis contains a prominent

legend as to the confidential nature of the summary or analysis. Recipient further agrees not to disclose to any person or entity, without XXX's prior written consent, the existence, subject matter or terms, conditions or other facts or circumstances of any discussions or negotiations between Recipient and XXX and will treat this entire matter as strictly confidential.

4. All rights, title and interest, including all intellectual property and proprietary rights, in and to any Confidential lnformation obtained by Recipient pursuant to this Agreement, and all copies thereof, shall be and remain the sole and exclusive property of XXX. Recipient hereby assigns, transfers and conveys, and agrees to assign, transfer and convey, to XXX all rights, title and interest, if any, that Recipient may obtain or have in and to any summary or analysis of Confidential lnformation prepared by Recipient hereunder. All such Confidential lnformation, and any copies, summary or analysis thereof, shall be promptly returned to XXX upon XXX's request.

5. Recipient may disclose Confìdential lnformalion to its lawyers, accountants, investment bankers or other advisors only if such parties also execute a copy of this Agreement and Recipient delivers to XXX a duly executed copy thereof.

6. Recipient must maintain any Confidential lnformation at its principal place of business, unless otherwise agreed to by XXX in writing, and in a secured area with only those authorized officers, directors and employees with a "need to know" having access to such area.

7. Because of the unique nature of the Confidential lnformation, Recipient understands and agrees that XXX will suffer irreparable harm in the event that Recipient fails to comply with the provisions oi this Agreement and that monelary damages will be inadequate to compensate XXX for such breach. Accordíngly, the undersigned agrees that Discloser will, in addition to any other remedies available to it at law or in eqúity, be entifled to injunctive and other equitable relief to enforce the terms of this Agreement and to prevent any actual,'potential or threatened violation of this Agreement by Recipient. Recipient expressly agrees that it shall bear all costs and expenses, including attorneys' fees and costs, incurred by XXX in enforcing the provisions of this Agreement.

Recipient shall indemnify, defend and hold harmless XXX from and against any and all claims, damãges, liabilities, losses and expenses (including attorneys' fees and costs) arising out of or relating to Recipient's breach of

any of the terms or conditions of this Agreement.

8. Recipient's obligations under this Agreement shall continue in perpetuity, subject to the exceptions contained herein.

9. Although XXX has endeavored to ensure its reliability, all Confidential lnformation is provided by XXX to Recipient 'AS lS." XXX makes no representation or warranty, whether express or implied, regarding the accuracy, completeness, quality or results that may be obtained from such Confidential lnformation.

Recipient assumes the entire risk of loss, damage and liability in reliance on such Confidential lnformation.

**CONFIDENTIALITY AND SECURITY – 2 EXAMPLES**

Except as necessary to the performance of its obligations hereunder, Agency shall treat as confidential and proprietary and not disclose to any third party during or subsequent to the term of this Agreement any confidential information, whether verbal or written, supplied to Agency by Client regarding Client’s plans, programs, plants, processes, products, costs, equipment, operations or customers (collectively, “Confidential information”), without securing the consent of Client. Agency agrees that it shall use such information only as is necessary in performing services under this Agreement and not for any other purposes whatsoever.

It is understood that “Confidential Information” shall not include any information: that is or becomes publicly available without breach of this Agreement; that is already in Agency’s possession prior to disclosure by Client; that is learned by Agency from a third party; that is independently developed by Agency; that Client authorizes Agency to disclose; or that is required to be disclosed by law or legal process

Below are a couple examples of security/confidentiality clauses agreed to (more "extensive" then just standard).

Attached are 2 examples are "full blown" privacy/security/confidentiality agreements with 2 of our clients (one a retailer the other is financial).

Examples on next page:

**EXAMPLE #1**

Security.

a.General. Without limiting Vendor’s obligations pursuant to Section 11 (Confidentiality) or elsewhere in the Agreement, Vendor shall: (i) protect the security and integrity of Client’s Confidential Information (including, without limitation, Customer Property) using and maintaining administrative, technical and physical safeguards consistent with the highest industry standards and all applicable laws to protect against anticipated threats or hazards to, or the unauthorized access, disclosure or use of, Client’s Confidential Information, and in no event shall such measures be less restrictive than those Vendor employs to safeguard its most confidential information; (ii) comply with the information security standards and requirements set forth in Exhibit D C [NOTE TO DRAFT. DSG still considering whether it can accept inclusion of the SLA as a part of the Work Order.] attached hereto; and (iii) implement, maintain and update commercially reasonable and current security measures, procedures, policies, controls and practices (collectively, “Security Measures”) regarding the Vendor System designed and tested to prevent unauthorized access to Client Property under Vendor’s control.

b.Audits and Reviews. Client shall have the right to review and audit Vendor’s compliance with the security requirements of this Agreement as further detailed in Exhibit D C attached hereto and Vendor shall cooperate with Client in such audit as reasonably requested. In addition, upon Client’s request, Vendor shall provide Client with the results of any audit performed by or on behalf of Vendor that assesses the effectiveness of Vendor’s information security program as relevant to the security and confidentiality of Client Property.

c.Password Protection of Vendor System. The Vendor System may require anyone accessing it to have authorized logon identification and corresponding passwords (“User Credentials”). Client shall promptly notify Vendor following the discovery of any unauthorized disclosure of any User Credentials. Vendor shall as soon as commercially possible (but in no event more than twenty-four (24) hours) terminate access to the Vendor System through the use of such User Credentials of which Client has notified unauthorized disclosure. Provided such liability does not arise as a result of Vendor’s breach of this Agreement or due to Vendor’s negligence or willful misconduct, Vendor shall not be liable for activity occurring under Client’s Users Credentials.

d.Security Breach. Without limiting Vendor’s obligations set forth in Exhibit DC, if there is a suspected, threatened or actual breach of security involving Client Property (each, a “Security Breach”), Vendor will at its own expense: (i) immediately investigate and take all steps to identify, prevent and mitigate the effects of such Security Breach; (ii) promptly notify Client (but in all such circumstances within four (4) hours of becoming aware of such occurrence), which notice shall include a detailed description of the incident, the Client Property accessed or attempted to be accessed, the identity of affected Customers and other individuals, and such other information as Client may reasonably request concerning the Security Breach; and (iii) as soon as possible conduct any recovery necessary to remediate the impact of such Security Breach and comply with applicable law relating to such Security Breach. Vendor shall cooperate with Client prior to sending any notices required under applicable law with respect to a Security Breach. Without limiting Client’s other rights, upon Client’s request during the Term, all Customer Data in the possession of Vendor will be provided to Client in a manner reasonably requested by Client.

**EXAMPLE #2**

Section 6. Confidential Information; Security.

6.1.Protection of Confidential Information. All Confidential Information disclosed by a disclosing party shall be maintained as confidential by the receiving party, subject to Section 6.5. Beginning on the date of first association or communication between CLIENT and CONTRACTOR and continuing through the term of this Agreement and thereafter, neither party to this Agreement will disclose, communicate or divulge or permit disclosure, communication or divulgence to another, or use for its own or a Subcontractor's benefit or the benefit of another, any such Confidential Information belonging to the other, except as necessary to the performance of its obligations hereunder. The parties agree that the disclosing party shall be entitled to seek injunctive and/or other equitable relief in any court of competent jurisdiction to prevent or otherwise restrain a breach of this Agreement by the receiving party or others. This Section 6 shall be binding upon the parties hereto, Subcontractors and all individuals assigned by either CONTRACTOR or a Subcontractor to perform Services for CLIENT.

6.2.Non-Disclosure and Inventions Agreement. In furtherance of CONTRACTOR's obligations under Section 5 and this Section 6, upon request by CLIENT, CONTRACTOR agrees to obtain from each CONTRACTOR Employee a written agreement obligating each such employee to adhere to and be subject to the terms of Section 5 and this Section 6. To the extent that any third-party vendor of materials or software (to be disclosed to CONTRACTOR in connection with performance of Services) requires a specific form of non-disclosure agreement as a condition of access to such materials or software, CONTRACTOR and all Subcontractors will execute (and will cause all respective employees to execute, if required) any such form, subject to good faith negotiation.

6.3.Further Protection of Confidential Information. Each party shall ensure that any and all copies of the Confidential Information made by it or by CONTRACTOR Employees display the respective owner's patent, copyright, trade secret or other proprietary notices in such manner and location as to give reasonable notice of the rights of the respective owner. Any and all copies of the Confidential Information made by either party or a Subcontractor shall remain the sole and exclusive property of the respective owner. Without notice to and the prior written consent of CLIENT, neither CONTRACTOR nor Subcontractors shall use or display on CLIENT's premises any documents or property belonging to any other person or entity to whom CONTRACTOR or a Subcontractor has an obligation of confidentiality, except as necessary to the performance of its obligations hereunder.

6.4.Publicity. During the term of this Agreement and for a period of two (2) years from the date of any expiration or termination of this Agreement, CONTRACTOR shall not disclose the nature of the effort undertaken for CLIENT or an Affiliate or the terms of this Agreement to any other person or entity without the prior written consent of CLIENT. CONTRACTOR is not permitted to use CLIENT's or an Affiliate's name or any trademark, trade name, logo or service mark of CLIENT or an Affiliate in any advertising or publicity without the prior written consent of CLIENT’s legal department, except CONTRACTOR shall not be precluded from verbally identifying CLIENT to third parties as a Client of CONTRACTOR or from taking any action permitted by law. All required consents may be given or withheld at CLIENT's sole discretion.

6.5.Exceptions. Notwithstanding anything to the contrary contained herein, the provisions of Sections 6.1 through 6.4 are not intended to cover information which is: (a) in the public domain generally or becomes generally known through no fault of the party receiving the information so disclosed; (b) is rightfully known to the receiving party without obligation of confidence prior to disclosure hereunder; (c) is lawfully obtained without obligation of confidence by the receiving party from a third party whose disclosure does not violate an obligation of confidence; (d) is disclosed by the receiving party to a Subcontractor solely in connection with performance of the Services, provided that such Subcontractor has signed a written agreement with the receiving party containing terms substantially similar to those in this Agreement, including Section 6.1 above; (e) is required by law or regulation to be disclosed, but only to the extent and for the purposes of such required disclosure; (f) is disclosed in response to a valid order of a court or other governmental body of the United States or any political subdivision thereof, but only to the extent and for the purpose of such order; or (g) is independently developed by receiving party as evidenced by written record. If any disclosure is required under (e) or (f) above, the receiving party shall notify the party ordered to disclose as is reasonable under the circumstances to afford the disclosing party a reasonable opportunity to resist the disclosure.

6.6.Security

6.6.1Information Security Guidelines. CONTRACTOR shall have and adhere to commercially reasonable written information security guidelines and shall reasonably discuss with CLIENT such guidelines, which guidelines include without limitation, (a) physical, administrative and technological controls; (b) security training and oversight; (c) written plans to assess and manage system failures and change controls; (d) regular assessments of security risks and measures to prevent and detect unauthorized access; (e) collection, maintenance, transmittal and disposal of CLIENT Confidential Information; and (f) notice and incident response procedures. Any notifications required by this Section 6.6, including its subsections, shall be directed to the CLIENT Technology Assistance Center via telephone at 614-415-7911 or 1-877-415-7911.

6.6.2Access to CLIENT’s Confidential Information. With respect to all employees, agents and subcontractors of CONTRACTOR who at any time have access rights to CLIENT Confidential Information, CONTRACTOR agrees as follows: (a) to limit such access to only those individuals with a need for such access to perform CONTRACTOR’s obligations under this Agreement; (b) to require CONTRACTOR management approval of any system access to CLIENT’s Confidential Information prior to access being granted; and (c) to require CONTRACTOR management to advise individuals of the confidential and sensitive nature of such CLIENT Confidential Information prior to access;. If CONTRACTOR employees, agents or subcontractors connect directly to CLIENT hosted systems or networks then CONTRACTOR agrees, with respect to those individuals, that: (i) individuals will comply with CLIENT’s information Security Policy; (ii) CONTRACTOR management will notify CLIENT within twenty-four (24) hours when any individual with access terminates employment or no longer requires access to perform obligations under this Agreement; and (iii) all CONTRACTOR system access shall be traceable to unique individuals.

6.6.3Retention and Disposal of CLIENT Confidential Information. CONTRACTOR agrees to securely dispose, reliably erase or physically destroy any disk drives or storage devices that store CLIENT Confidential Information when no longer in service. Notwithstanding the foregoing, neither party shall be under an obligation to purge any data archived pursuant to its normal document retention practices or required to be maintained by applicable law if the obligations of confidentiality herein continue to be strictly observed.

6.6.4Notification and Response Obligations. CONTRACTOR shall notify CLIENT promptly under the circumstances, however in no event later than the earlier of: (a) as required by law; or (b) eight (8) hours after discovering or suspecting such event, of any unauthorized access or breach of system security, unauthorized access of CLIENT Confidential Information, or misuse of CLIENT Confidential Information by an employee, agent or subcontractor with access to such information. CONTRACTOR agrees to take all actions reasonable under the circumstances to immediately prevent continued risk of exposure of CLIENT Confidential Information.

6.6.5Security Testing. To detect any material security weaknesses, CLIENT reserves the right to conduct security testing of any of CONTRACTOR's or CONTRACTOR's subcontractor systems or facilities where CLIENT Confidential Information is stored, transmitted or accessed by CONTRACTOR employees, agents or subcontractors. Security testing will be conducted either by CLIENT or a mutually agreed upon third party assessor. Such security testing may include: (a) audit through physical site inspection in accordance with the audit provisions set forth in Section 3.3; (b) executing technical security tests, including, without limitation, vulnerability scans, network, and application or operating system security testing; (c) conducting interviews and reviewing system architecture and procedures documentation with CONTRACTOR information technology and security personnel; and/or (d) completion of information security-related questionnaires. To the extent any such material weakness is found, CONTRACTOR will take appropriate action, prompt under the circumstances, to remedy such weakness at CONTRACTOR’s cost and expense. CONTRACTOR will discuss with CLIENT testing methods, any initial findings, remediation action plans and validation retest results as each pertains to CLIENT Confidential Information. CONTRACTOR will provide security testing or compliance certification evidence no later than thirty (30) days after completion of initial testing.

6.6.6 Certification Reporting: SSAE 16, SAS 70 and ISO27000. Upon CLIENT’s written request, on an annual basis, CONTRACTOR shall provide a copy of its most recent Statement on Auditing Standards (SAS) No. 70, Type II auditor’s report (the “SAS 70 Report”) or Standards for Attestation Engagements (SSAE) No. 16 Audit Report (the “SSAE 16 Report”). Additionally, should any of CLIENT’s Confidential Information be retained or transmitted through a third party’s systems/networks, CONTRACTOR shall require such third party to provide CLIENT with a copy of its SAS 70 Report or SSAE 16 Report on an annual basis. Upon CLIENT’s written request, on an annual basis, CONTRACTOR shall provide a copy of its most recent "International Organization for Standardization ISO 27000" report as performed by CONTRACTOR's third party auditor (the "ISO27000 Certification"). In the event any CLIENT Confidential Information is retained in, or transmitted through, a third party's system or network, CONTRACTOR shall cause such third party to provide to CLIENT a copy of its ISO27000 Certification on an annual basis. To the extent any material weakness is found in the SAS 70, SSAE 16 or ISO27000 audit, CONTRACTOR will take appropriate action, prompt under the circumstances, to remedy any such weakness at CONTRACTOR’s cost and expense.

**CONFIDENTIAL INFORMATION – 3 EXAMPLE FORMS**

**Form 1**

Confidential Information.

a. A confidential relationship between Agency and Company exists by reason of which Company has disclosed, and may in the future disclose, commercially valuable confidential information, including ideas, research, marketing, advertising and media methods and strategies, and internal plans and information about Company and its products, any passwords disclosed for use in connection with any Company website or any shadow sites used for development or testing, all Deliverables and documents related to the Deliverables that Company designates as confidential, and any other materials and information of Company that Company designates as confidential, or that Agency should reasonably believe to be confidential. Any unauthorized disclosure of that information to third parties is likely to be damaging to Company. Agency must hold all confidential information in strict confidence and must not disclose that information to any third party without Company's prior written consent, or as required by a government agency or by operation of law.

b. Company acknowledges that Agency may disclose confidential information to Company concerning Agency's financial position and personnel compensation arrangements, as well as Agency Tools, source code, and any other materials and information that Agency designates in writing as confidential. Company must hold that information in strict confidence and must not disclose that information to any third party without Agency's prior written consent.

c. The parties’ respective secrecy obligations do not apply to any information that: (i) has become generally known to the public through no act or omission of the receiving party; (ii) has become available on a non-confidential basis from any source other than the disclosing party, its agents, representatives or employees, and such source is not prohibited from disclosing such information; (iii) was already known to the receiving party at the time of disclosure or is independently developed by the receiving party without use of the disclosing party’s confidential information; or (iv) is required to be disclosed by applicable law or court order. The parties’ secrecy obligations under this Section will remain in effect for a period of 10 years from the effective date of the Agreement.

d. The parties must restrict dissemination of confidential information received from the other party to those of its own personnel who require knowledge of that confidential information in order for Agency to perform Services. This means, at a minimum, that:

i. Agency must keep all files, materials and information regarding Company (e.g., strategic information, brand vision and architectures, briefs, scripts, boards, media plans, proprietary tools and research, insights, etc.) in a secure environment, with access strictly limited to personnel working on Company matters.

ii. Agency must not share any files, materials or information regarding Company with any Affiliate of Agency, and Agency must not make any of that information or those materials accessible to employees not working on Company matters, whether through print, electronic or other means, including web sites, team rooms or internal computer networks.

iii. Agency personnel must not make any presentations, speeches or other remarks concerning Company or Agency’s work for Company (including internally within the Agency), without Company’s prior written approval.

e. As a condition to receiving any payments due under the Agreement, Agency must obtain, and provide copies thereof to Company, the written agreement of each of its employees and contractors engaged in providing Services under the Agreement to be bound by the provisions of this Section.

f. Agency must use its best efforts to prevent its former employees from disclosing confidential information to any third party, and must require all such employees to return to Agency and account for all materials containing confidential information.

**Form 2**

Note: Company has been defined as the ad agency

Confidentiality. Company may, during the course of its engagement hereunder, have access to, and acquire knowledge of or from, materials, data, strategies, systems, or other information relating to the Services or to Client’s business or the business of its parent, related, affiliated, or subsidiary companies, which may not be known to the general public (“Confidential Information”). Any such Confidential Information acquired by Company shall be kept confidential and shall not be used, published, or divulged by Company to any other person, firm, or corporation, or in any advertising or promotion regarding Company or its services, or in any other manner or connection whatsoever without first having obtained the prior written permission of Client, which permission Client may withhold in its sole discretion. In addition: (a) Company only shall disseminate any such Confidential Information strictly on a “need to know” basis within its organization or among its employees, agents or contractors; (b) Company shall specifically apprise in writing any recipient of such Confidential Information of the requirements of this Section; (c) Company shall be responsible for any disclosure of such Confidential Information by any of its employees, agents or contractors; and (d) in the event of any breach of this Section, Client shall be entitled, in addition to any other remedies that it may have at law or in equity, to injunctive relief or an order of specific performance. Upon the termination or expiration of this Agreement or at Client’s request, Company shall immediately return to Client or destroy, all documents, magnetic copies, or other physical evidence of all Confidential Information in Company’s possession or in the possession of any of Company’s directors, officers, employees, agents, or representatives (including, without limitation, all copies, transcriptions, notes, extracts, analyses, compilations, studies, or other documents, records, or data prepared by Company) which contain or otherwise reflect or are generated from the Confidential Information without retaining any copy thereof, all of the foregoing being Confidential Information and the sole property of Client, and an officer of Company shall certify in writing to Client that all of the foregoing has been returned or destroyed as provided in this Section. Company agrees that Client would be irreparably harmed by any violation or threatened violation of this Section and therefore, Client shall be entitled to an injunction prohibiting Company from any violation or threatened violation of this Section. The provisions of this Section shall survive the expiration or sooner termination of this Agreement.

**Form 3**

Confidential Information.

(a) The Recipient shall use the Confidential Information only for the purpose of meeting its obligations or exercising its rights under this Agreement, and shall not, without limitation, use the Confidential Information to: (i) compete directly or indirectly with the Discloser; or (ii) interfere with any actual or proposed business of the Discloser.

(b) The Recipient shall not disclose or otherwise make available any of the Confidential Information to anyone, including employees, contractors and representatives, except those employees, contractors and representatives of the Recipient and entities controlled by, controlling or under common control with the Recipient who need to know the Confidential Information for the purpose of meeting Recipient’s obligations under this Agreement or exercising its rights under this Agreement, and who are bound by obligations of non-use and non-disclosure substantially similar to those set forth herein. The Recipient shall be responsible for any use or disclosure of the Confidential Information by such employees, contractors, representatives or commonly controlled entities.

(c) The Recipient shall use its best efforts (but in any event not less than those employed for safeguarding its own proprietary information) to keep the Confidential Information and/or any knowledge which may be imparted through examination thereof or working therewith confidential.

1.1 Compelled Disclosure. The Recipient may disclose the Confidential Information to the extent that such disclosure is required by law or court order, provided that the Recipient shall promptly provide to the Discloser written notice prior to such disclosure and shall provide reasonable assistance in obtaining an order or other remedy protecting the Confidential Information from public disclosure at the Disclosing Party’s sole cost and expense.

1.2 Return of Confidential Information. Each Party shall, upon termination or expiration of this Agreement or applicable SOW, or at any time upon demand by the other Party, promptly return to the other Party any and all Confidential Information together with any copies or reproductions thereof and destroy all related data in its computer and other electronic files. Upon the return, or destruction, of Confidential Information the Recipient will erase all copies of the Discloser’s Confidential Information from all forms of magnetic and electronic media using a method that ensures that it cannot be recovered; provided, however, that each Party may keep one (1) copy of the Confidential Information with its legal counsel for archive purposes.

1.3 Injunctive Relief. Each Party acknowledges that disclosure of the other Party’s Confidential Information by it or breach of the provisions contained herein may give rise to irreparable injury to the other Party and such breach or disclosure may be inadequately compensable in money damages. Accordingly, each Party may seek injunctive relief against the breach or threatened breach of the foregoing undertakings. Such remedy will not be deemed to be the exclusive remedy for any such breach but will be in addition to all other remedies available at law or in equity.

**DATA SECURITY FORM**

Data Security.

(a) Security Policies and Safeguards. Agency shall abide by Client’s information technology and data security policies, and any changes thereto (the “Security Policies”) delivered to Agency in writing. Agency shall also establish and maintain data security procedures and other safeguards against the destruction, loss, unauthorized access or alteration of Client Data and other Client property in the possession or under the control of Agency or to which Agency has access, which are (i) no less rigorous than those maintained by Agency for its own information of a similar nature, (ii) no less rigorous than accepted security standards in the industry, and (iv) adequate to meet the requirements of applicable Laws (the “Agency Data Security Safeguards”).

(b) Breach Notification. In the event Agency discovers or is notified of a breach or potential breach of security relating to Agency’s Systems, Client Data or facilities from which Services are provided, Agency shall notify Client of the following events without undue delay, as soon as practicable after the event:

(i) suspected breaches and compromises of Client Data or Agency’s Systems or networks that directly or indirectly support Client Data, or claims or threats thereof made by any Agency Personnel or external person (notice to be provided telephonically);

(ii) termination of any Agency Personnel for cause, where related to such Agency Personnel’s potential or actual misuse or compromise of Client Data or Agency’s Systems or networks that directly or indirectly support Client Data (notice to be provided telephonically); and

(iii) any law enforcement or administrative investigation or inquiry into suspected misuse or abuse of Agency’s Systems or network (notice to be provided telephonically).

**Security & Privacy Agreement – Sample 1**

Exhibit D

Information Security

At a minimum and as specified herein, in addition to the general requirements set forth in the Agreement, Vendor shall provide security for all data and communication systems in support of the Agreement to which this Exhibit D is attached (“Exhibit”). Capitalized terms used herein, but not defined, have the meaning set forth in the Agreement (or other document) to which this Exhibit is attached.

Security Measures. Vendor’s Security Measures shall in no event be less stringent than: (i) those used to safeguard Vendor’s own confidential property; (ii), those used by other companies providing services similar to the Services (i.e., industry standard measures); and (iii) those required by applicable laws, rules and regulations (including those relating to Customer Data). Such security measures shall include, where appropriate, use of updated firewalls, virus screening software, encryption, intrusion detection systems, logging of incidents, periodic reporting, and prompt application of current security patches, virus definitions and other updates. Vendor shall promptly notify Client if, during the Term of a Work Order, Vendor modifies the Vendor System or its security measures in a manner that causes Vendor not to comply with the terms of this Agreement or otherwise provides a diminution in security to Client Property. In no event shall Vendor make a change to its security measures regarding the Vendor System that result in such security measures being less stringent than those currently in effect and disclosed to Client. Vendor shall document all such security measures and shall keep them current in light of changes in relevant technology. Vendor shall provide Client with such information concerning its compliance with the foregoing as Client may reasonably request. Without limiting the foregoing, Client may terminate this Agreement and/or any Work Order upon its determination, in its sole discretion, that Vendor’s security measures fail to conform to the reasonable policies effectuated by Client from time to time with respect to the security of Client Property.

Reports. Within ten (10) days after the Effective Date and thereafter on an annual basis, Vendor shall provide Client with a copy of Vendor’s (and all applicable subcontractor’s) most recently completed Service Organization Control (“SOC”) one or two, as applicable, Type 2 audit reports, or industry-standard successor reports, which must have been completed within the twelve (12) month period prior to the Effective Date and which shall be updated by Vendor on an annual basis. The most recently completed, as of the Effective Date, SOC audit reports are referred to as the “Current Audit Reports.” Vendor will use commercially reasonable efforts to maintain its ISO 27001 certification or industry-standard successor certification (“ISO Certification”) during the Term or, at a minimum, continue to meet the standards set out in ISO 27001 to the extent such standards are covered by controls within the scope of the ISO Certification obtained by Vendor (“ISO Control”). In no event shall Vendor’s security program use controls materially less protective than the ISO Controls set forth in the Current Audit Reports.

In order for Client to confirm Vendor’s compliance with the Agreement and this Exhibit, as well as any applicable law, regulations and/or industry standard, upon Client’s request, Vendor grants Client or, upon Client’s election, a third party on Client’s behalf, permission to perform an assessment, audit, examination or review of Vendor’s compliance with the security requirements of the Agreement and this Exhibit including, without limitation, an assessment, review or audit of all controls in Vendor’s physical and/or technical environment in relation to all Client Property handled and/or Services being provided to Client pursuant to the Agreement. Vendor shall fully cooperate with such assessment by providing access to knowledgeable personnel, physical premises, documentation, infrastructure and application software that processes, stores or transports such property. In addition, Vendor shall reasonably cooperate with Client in connection with any regulatory or other governmental investigation regarding Client’s or Vendor’s security measures or in connection with any Security Breach and will provide such governmental authority such access and information as is reasonably requested to verify compliance with the terms of this Agreement.

Vendor’s security efforts will include, without limitation:

Logical Access Controls: Vendor agrees to employ effective logical access control measures over all systems used to create, transmit, or process CLIENT Confidential Information, including but not limited to:

1. User authentication must use unique identifiers (“User ID’s”) consistent with individual accountability; shared User ID’s do not provide the level of accountability required by CLIENT.

2. A complex password policy, including the prohibition of clear-text credentials must be enforced.

3. User access rights/privileges to information resources containing CLIENT Confidential Information must be granted on a need-to-know basis consistent with role-based authorization.

4. User access to CLIENT Confidential Information must be removed immediately upon user separation or role transfer eliminating valid business need for continued access.

5. Default passwords and security parameters must be changed in third-party products/applications used to support CLIENT Confidential Information.

6. Two-factor authentication such as token devices, smart cards, biometrics, or public keys shall be used to secure all remote access to CLIENT Confidential Information.

Network Security Architecture: Vendor agrees to employ effective network security control measures over all systems used to create, transmit, or process CLIENT Confidential Information including but not limited to:

1. Firewalls shall be operational at all times and shall be installed at the network perimeter between Vendor’s internal (private) and public (Internet) networks.

2. Properly configured and monitored IDS/IPS (Intrusion Detection/Prevention Systems) must be used on Vendor’s network.

3. Databases must be logically or physically separated from the web server, and the database may not reside on the same host as the web server, where applicable.

4. The database and other information systems used for the purposes of processing CLIENT Confidential Information must have only those services/processes and ports enabled to perform routine business. All other services/processes on the host must be disabled.

5. All information systems, repositories, etc. used for CLIENT by Vendor, or its business partners, must be physically located in a controlled data center environment used for the purpose of protecting information systems.

6. Secure channels (e.g., SSL, SFTP, SSH, IPSEC, etc.) must be used at all times.

Physical Access Controls: Vendor agrees to maintain servers, databases, and other hardware and/or software components that store information related to CLIENT’s business activities in an access controlled and consistently monitored Data Center secured by appropriate alarm systems, which will not be commingled with another unrelated party’s hardware, software or information.

Risk Assessment: At no additional cost, Vendor agrees to provide true, correct and complete responses to a risk assessment questionnaire (if provided by CLIENT), participate in vulnerability scans of their network and/or application (upon notification).

1. Vendor agrees to perform regular security vulnerability assessments and shall provide CLIENT with results of a current security assessment by an accredited third-party (e.g., penetration test results of internet-facing devices, SAS 70-Type II reports, ISO 27001 certification, etc.) as well as action plans describing how Vendor will address all identified security vulnerabilities affecting systems used to store, process or otherwise access CLIENT Confidential Information.

2. Vendor will permit CLIENT or its designee to conduct audits of CLIENT’s data maintained or stored by the Vendor.

Security Policy: Vendor agrees to maintain and enforce security policies consistent with security best practices, and all applicable regulatory and legal security and privacy requirements. Upon request, Vendor shall provide a copy of current security policy and standards as well as security architecture. Vendor shall comply with CLIENT’s Privacy Policy with respect to any CLIENT customer personal information it receives.

Protection of CLIENT Confidential Information: In addition to the requirements set forth above and in the Agreement to which this Exhibit is attached, Vendor agrees to protect CLIENT Confidential Information as it would its own. For purposes of clarity, in addition to Confidential Information as otherwise defined or described in the Agreement Confidential Information includes, but is not limited to:

(i) Employee medical information, merger and acquisition information, credit card numbers, unreleased annual reports, private label design, material non-public financial information (e.g., sales data, margin reports, profitability analyses and other key indicators of the Company’s performance), any information considered by DDD or by any law, rule or regulation to be personally identifiable information; and

(ii) individual employment status, network details and architecture, product designs, construction plans, research information, certain financial information, vendor or customer information, internal operating policies and procedures, internal communications (memorandum, reports, e-mails).

Personally identifiable information is always considered Confidential Information and includes, by way of example an individual’s first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such a person:

1. Social Security Number;

2. Other State or federal identification number (e.g., driver’s license, state identification card or passport number);

3. Date of birth;

4. Bank account number;

5. Credit or debit card number, pin code, number access code or password that would permit access to financial account or to obtain goods, services or other things of value;

6. Digitized electronic signatures;

7. Any customer e-mail address and/or telephone number;

8. Any unique persistent identifier, such as a customer number, unique pseudonym or user alias; and

9. Medical information (including medical history or diagnosis information contained in insurance applications and any claim form), Health Insurance Card or Policy Identification Number

Additionally, Vendor agrees to adhere to the following controls surrounding the Use and Protection of CLIENT Confidential Information:

1. CLIENT Confidential Information must be encrypted with a minimum of AES 256-bit encryption.

2. Clear text (ftp, telnet, etc.) protocols may not be used to access or transfer CLIENT Confidential information. CLIENT Confidential Information must be encrypted when at rest, in use or in transit including, without limitation, when stored on portable media, which by way of example shall include USB Sticks, Portable hard drives, Laptops, DVD/CDs, and when transmitted on wireless networks or across public networks.

3. CLIENT Confidential Information may not be copied, sold or used for solicitation purposes by the Vendor or its business partners. CLIENT Confidential Information may only be used in conjunction with and within the scope of the Agreement to which this Exhibit is attached.

4. CLIENT Confidential Information (data) must be segregated (physically and/or logically if in a database or virtual (VM) environment) from other Vendor customers. If data is not physically segregated from other customers, systems, or applications unrelated to CLIENT, vendor must provide appropriate data security controls over data at rest, including, access controls and encryption.

5. Payment Card information must be masked on display rendering in a manner consistent with the Payment Card Industry Data Security Standard (PCI-DSS), the Fair and Accurate Credit Transaction Act (FACTA) and all other applicable laws and regulations.

6. Vendor must disclose where CLIENT data will be stored and processed. Storage and processing of CLIENT Confidential Information shall take place within the United States.

7. Ensure secure processes and procedures (e.g., degaussing, anti-static bags, etc.) for handling or removal of physical media or equipment that may contain CLIENT Confidential Information.

System Monitoring: Vendor agrees to regularly audit and monitor information systems processing CLIENT’s business activities to ensure the protection of CLIENT’s information. Monitoring includes, but is not limited to, potential breaches or hacking activity and access to devices. Vendor must have defined processes for security alerting, escalation and remediation that are consistent with the Services procured pursuant to the Agreement. Vendor must ensure that event logs with CLIENT data are not provided to other subscribers. If Vendor is using virtual machines, Vendor must ensure there is granular monitoring of traffic that is crossing the virtual machine backplanes.

Vulnerability Management Controls: Vendor agrees to employ effective vulnerability management control measures over all of its systems used to create, transmit, or process CLIENT Confidential Information, including; but, not limited to:

1. Third-party vulnerability scans or audits of any external-facing (public) infrastructure devices.

2. Annual (or quarterly if PCI related) third-party assessment of applications or processes supporting CLIENT customer credit card information.

3. Deploy and maintain currency of up-to-date commercially available anti-virus, anti-spam, anti-malware software on all information system components including personal computers, laptops, and interconnecting networks, where applicable, used for the purpose of managing CLIENT Confidential Information. Additionally, provide for regular scanning for viral infections and update virus signature files frequently.

4. Maintain a standard patch management process and practice to ensure the protection of any devices used to access, process or store CLIENT Confidential Information. Vendor agrees to provide CLIENT with their patch management policies and procedures upon request.

5. Regularly auditing and monitoring to ensure the protection of CLIENT Confidential Information.

6. Any security breach that involves CLIENT Confidential Information must be reported to CLIENT in accordance with the Notice provision of the Agreement without unreasonable delay. Vendor shall immediately perform a root cause analysis as well as provide detailed information about measures taken by the Vendor to prevent future breaches. All efforts to rectify or resolve the situation must include subsequent and regular notification for the reported incident.

7. Within one (1) hour of suspected fraudulent or malicious activity occurring on the Vendor site, Vendor will notify CLIENT’s {NAME OF CONTACT} by phone at {PHONE NUMBER} or {PHONE NUMBER} to inform the CLIENT team about the activity. Any request by the CLIENT team for such information will be provided to CLIENT within two (2) hours.

8. Vendor agrees to provide full cooperation with CLIENT and in the event of a data breach involving CLIENT Confidential Information including, but not limited to: server log information showing network and application traffic.

9. CLIENT must be immediately notified of any known attacks occurring against Vendor systems used to store or process CLIENT Confidential Information.

10. Vulnerabilities discovered by the CLIENT’s or Vendor’s Security Scanning tools must be resolved by following the schedule outlined below (the level of vulnerability will be determined by CLIENT):

a. P1 vulnerabilities: A successful exploit of this vulnerability may result in catastrophic and significant physical or property damage or loss, or there may be a catastrophic and significant loss of revenue or productivity (e.g., Denial of Service Attack, exploit ‘kits’ exist, buffer overflows high jacking, or source code exposure, etc.). Such vulnerability must be resolved before a site launch or within two (2) hours of discovery if the application is currently publicly available.

b. P2 vulnerabilities: A successful exploit of this vulnerability may result in moderate physical or property damage, or there may be a moderate loss of revenue or productivity to the organization (e.g., Weak encryption, or possible phishing opportunity, etc.). Such vulnerability must be resolved within two (2) days of site launch or within four (4) hours of discovery if the application is currently publicly available.

c. P3 vulnerabilities: A successful exploit of this vulnerability may result in minor physical or property damage, or there may be a minor loss of revenue or productivity to the organization (e.g., FTP use or missing service pack, etc.). Such vulnerability must be resolved within three (3) days of a site launch or within eight (8) hours of discovery if the application is currently publicly available.

Data Recovery and Availability: Vendor must provide detailed disaster recovery and business continuity plans that support the pre-defined recovery time objective (RTO) / recovery point objective (RPO) requirements defined by CLIENT:

1. Vendor must utilize industry best practices for data, services, and communications recoverability. Data and applications must be replicated across multiple independent sites and alternate communication channels must be available.

2. Vendor is expected to validate and verify their existing capabilities through realistic scenario testing. Vendor must agree to participate in periodic recovery testing with CLIENT. Proof of successful testing of the Vendor plan must be provided to CLIENT upon request.

3. Vendor systems must be device (computer machine) and provider independent in order to ensure portability and successful recovery of applications and backup or restoration services, or both.

4. Vendor must provide company name, address, and contact information on all third-party relationships as well as services provided by each wherever those services create, transmit or process CLIENT Confidential Information.

Data Destruction: Vendor shall ensure that residual magnetic, optical, or electrical representation of CLIENT Confidential Information that has been deleted may not be retrieved or reconstructed when storage media is transferred, become obsolete or is no longer usable or required by CLIENT and shall certify such destruction to CLIENT as provided in the Agreement.

1. Vendor should be utilizing minimum 256-bit encryption that renders data unreadable when storage is recycled, disposed of, or accessed by any means outside of authorized applications.

2. Vendor data retention and destruction must align with CLIENT requirements and policies as provided to Vendor (as updated by CLIENT from time to time) as well as comply with applicable laws or regulations.

3. CLIENT information stored on vendor media (e.g., hard drive, optical discs, tapes, paper, etc.) must be rendered unreadable or unattainable using the NIST Guidelines for Media Sanitization (Special Pub 800-88), prior to the media being recycled, disposed of, or moved off-site.

Application Vendor: Vendor agrees to adhere to the following controls surrounding application development for applications developed and hosted off-site as well as off-site application development for on-site deployment:

1. Vendor must provide supporting documentation that commonly accepted web application security guidelines and frameworks are used for developing Internet-facing applications (e.g. Open Web Application Security Project [OWASP], SANS).

2. Vendor must provide a data flow diagram that includes the entry points (the main pages and the i-framed pages as may be applicable), a description of the data flowing from each node in the system (e.g., username, password, address, etc.), a listing of all attributes stored, processed, or transmitted, and how the data is securely stored. The diagram must also demonstrate all security controls in place.

3. Vendor must demonstrate how Internet-facing applications are tested for security vulnerabilities and remediated prior to the source code being promoted to production.

4. If Vendor has performed prior security testing, the results of such testing must be made available to CLIENT for evaluation prior to launch. If Vendor has not performed such testing, Vendor shall allow penetration/vulnerability testing and/or application source code review to be performed by CLIENT, when requested.

5. Vendor must provide supporting documentation describing how fraud is detected and prevented when requested by CLIENT.

6. Vendor agrees to supply, within the requested timeframe, detailed information, and demonstrate full cooperation with CLIENT, pertaining to all inquiries deemed necessary by CLIENT to determine the risk of any third-party systems and procedures related to and affecting CLIENT. This includes, but is not be limited to, inquiries pertaining to servers, server logs showing detailed application traffic, operating systems, applications, databases, network configuration, data encryption algorithms being utilized, fraud detection and prevention controls, physical inspection of facilities, incident response procedures, and disaster recovery measures.

7. Vendor agrees to allow all relevant sites to be monitored by CLIENT or a third-party for availability and performance. While monitoring requirements may change based on the applications in scope, typically about 600 page requests would be made per hour by the monitoring application(s).

Personnel Roles and Responsibilities: Vendor agrees to identify in writing the person who will be responsible for overall security of the application development, management, and update process throughout the Contract period. The person identified shall be a single senior technical security specialist, to be known as the project Security Lead. The Security Lead shall confirm in writing the security of each deliverable. The Security Lead shall confirm to CLIENT in writing that the software meets the security requirements, all security activities have been performed, and all identified security issues have been documented and resolved. Any exceptions to the confirmation status must be fully documented with the delivery.

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

**Security & Privacy Agreement – Sample 2**

PRIVACY AND INFORMATION SECURITY AGREEMENT

This Privacy and Information Security Agreement (“Agreement”), made by and between \_\_\_\_\_ and their respective parents, subsidiaries and affiliates (collectively, “Client”), having a principal place of business located at \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ and \_\_\_\_\_\_\_\_\_\_\_\_\_\_, a [STATE] corporation (“Service Provider”), having a principal place of business located at ¬¬¬¬¬¬¬¬¬¬\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, sets forth terms and conditions relating to the protection of security, confidentiality and integrity of information associated with services to be or being rendered by Service Provider to Client from time to time (the “Services”).

In consideration of the mutual covenants and agreements in this Agreement and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties hereto hereby agree as follows:

1. Definitions. For purposes of this Agreement, the following terms shall be defined as follows:

(a) “Authorized Subcontractor” shall mean a subcontractor who (i) has been approved in writing in advance by Client for performance of Services; (ii) has agreed in writing to abide by the duties and obligations applicable to Service Provider under this Agreement; and (iii) Service Provider can reasonably expect to be suitable and capable of performing the Services and Service Provider’s obligations under this Agreement.

(b) “Background Screening” shall mean, collectively, (i) a national federal criminal database check; (ii) a seven-year county of residence criminal conviction search (i.e., a search of all counties in which the individual has resided within the preceding seven-year period); and (iii) any additional searches, screenings or checks required under any Service Provider Agreement or otherwise requested by Client in its reasonable discretion consistent with then-prevailing industry best practices, in each case to the extent not prohibited by Legal Requirements.

(c) “Cross-Border Data Transfer” shall mean to (i) transfer, distribute, send, process, handle, maintain, store, download, use or otherwise access any Personal Information outside of the national jurisdiction from which such Personal Information originated, or (ii) make any Personal Information available to or accessible by any person or entity, including, without limitation, Personnel, outside of the national jurisdiction from which such Personal Information originated, or (iii) otherwise engage in any activity which would constitute a cross-border data transfer under any Legal Requirement.

(d) “Information Security Program” shall mean a written, comprehensive information security program that protects the security, confidentiality and integrity of Personal Information, as more particularly described in Section 2(a) below.

(e) “Legal Requirements” shall mean, individually and collectively, all applicable international, federal, state, provincial and local laws, rules, regulations and governmental requirements now or hereafter in effect, including, without limitation, those relating to privacy, data protection, confidentiality or security of Personal Information.

(f) “Personal Information” shall mean any and all information that relates to or identifies an individual or can be used to identify an individual, including, without limitation: (i) name; (ii) home or other physical address, including street name and name of city or town; (iii) email address or other online contact information that reveals the email address; (iv) telephone number; (v) date of birth; and (vi) any information that is combined with any of the foregoing, and any information derived therefrom, all of the foregoing whether in individual or aggregate form, in any media.

(g) “Personnel” shall mean all Service Provider personnel, including, without limitation, personnel of any Authorized Subcontractor.

(h) “Satisfactory Background Screening” shall mean, to the extent not prohibited by Legal Requirements, a Background Screening, the results of which do not contain (a) any felony conviction, the disposition of which is within seven (7) years of the date of search; (b) any misdemeanor conviction related to fraud or theft (including, without limitation, shoplifting, larceny, embezzlement, forgery, credit card fraud, check fraud, computer fraud or abuse, data theft, identity theft or other cyber crime), the disposition of which is within seven (7) years of the date of search; or (c) any other violation, conviction or other matter specified in a Service Provider Agreement. In no event shall the foregoing limit Service Provider’s obligation to comply with any stricter or additional requirements set forth in a Service Provider Agreement.

(i) “Security Incident” shall mean any theft or loss of, unauthorized or unlawful disclosure, use, alteration or destruction of, unauthorized or unlawful access to, or other compromise of, Personal Information or any network, server, site or system that contains any Personal Information that is subject to this Agreement, and including, without limitation, any misuse, release or compromise of any Access Tool (as defined in Rider 2) or any password or other security feature.

(j) “Service Provider Agreement” shall mean any agreement between Service Provider and Client relating to the Services, including, without limitation, that certain Advertising Agency Agreement dated as of May 2009, as amended in writing from time to time, and including all schedules, addenda, statements of work and exhibits thereto, if any.

(k) “Client Information Security Policies” shall mean Client information security policies, privacy policies, and other policies, procedures, standards, guidelines and/or requirements provided to Service Provider from time to time.

(l) “Client IT Environment” shall mean Client’s information technology infrastructure, network, systems, applications, databases, files or hardware, or any part of the foregoing.

2. Privacy and Information Security. Service Provider represents and warrants to, and covenants with, Client as follows:

(a) Service Provider hereby certifies that it has implemented and maintains an Information Security Program, and that such program includes appropriate administrative, technical and physical safeguards and other appropriate security measures (including, without limitation, measures to protect computer hardware, software and internet security systems with regard to Service Provider’s collection, processing, storage, use, disclosure or disposal of Personal Information), that ensure that Service Provider and its Personnel (A) maintain the security, confidentiality and integrity of Personal Information; (B) protect against any anticipated threats or hazards to the security, confidentiality and integrity of Personal Information; and (C) protect against any Security Incident. Without limiting the generality of the foregoing, Service Provider’s administrative, technical and physical safeguards with respect to Personal Information shall include, without limitation, maintenance of a data security incident response plan, data retention and destruction policies, and training programs or similar instruction to raise awareness and ensure that Personnel assigned to carry out Service Provider’s obligations hereunder and the Services are properly informed of and fully understand their obligations hereunder.

(b) Service Provider hereby further certifies that its Information Security Program is in compliance with Legal Requirements, including, without limitation, the regulations established by the State Office of Consumer Affairs entitled “Standards for the Protection of Personal Information of Residents of the Commonwealth” (201 C.M.R. 17.00, et seq.).

(c) Service Provider shall comply with its Information Security Program, Legal Requirements, Client Information Security Policies and industry best practices concerning privacy, data protection, confidentiality or security of Personal Information.

(d) Service Provider shall hold in strict confidence all Personal Information that may be disclosed at any time to Service Provider or Personnel in anticipation of, in connection with or incidental to the performance of the Services, or that may be created, collected, procured, received, used, processed, maintained, accessed, observed or otherwise obtained at any time by Service Provider or Personnel in anticipation of, in connection with or incidental to the performance of the Services. Service Provider shall only create, collect, process, store, maintain, use, disclose, access or dispose of Personal Information for the benefit of Client and only for the purpose of performing the Services in compliance with this Agreement, any Service Provider Agreement, and Client’s written instructions. Except with the express prior written consent of Client, Service Provider shall not share, transfer, disclose or otherwise provide access to any Personal Information (or any portion thereof) to any third party, except to Personnel who have a bona fide business need to know the Personal Information as a necessary condition to Service Provider’s performance of the Services. Service Provider shall not have or obtain any rights in any Personal Information.

(e) Service Provider shall obligate all Personnel to comply with the terms and conditions of this Agreement in the same manner as Service Provider is bound hereby. Service Provider shall be responsible for and liable to Client for any and all violations of the requirements of this Agreement (including, without limitation, any Security Incident) by Personnel. Service Provider shall be responsible for and liable to Client for any Security Incident caused by any third parties who obtain access to Personal Information directly or indirectly from or through Service Provider.

(f) Client may from time to time provide Service Provider with guidelines relating to information security that are consistent with Service Provider’s obligations under this Agreement. Upon the request of Client, Service Provider agrees to provide such guidelines to Personnel prior to the performance of Services by such Personnel, or as otherwise directed by Client. Service Provider acknowledges and agrees that Client may, in its discretion, provide such guidelines directly to Personnel and require such Personnel to acknowledge and agree to such guidelines in writing. Client shall have the right to prohibit the performance of Services by any Personnel who fail to provide such written acknowledgment.

(g) Upon the occurrence of a Security Incident or other material breach of this Agreement, Service Provider shall immediately notify the Client Chief Information Security Officer or Chief Privacy Officer, and the Client Legal Department, in each case by telephone at 508-390-1000 (or at such other telephone number that Client may provide), and shall also give Client prompt written notice thereof. Service Provider shall promptly take all necessary and advisable corrective actions in accordance with Legal Requirements, and shall cooperate fully with Client in all reasonable and lawful efforts to prevent, mitigate, remedy and/or rectify such occurrence. Service Provider shall reasonably cooperate with Client and its auditors, assessors and investigators, and, in conjunction with Client, shall cooperate with any third parties investigating the same, including, without limitation, any federal or state agencies, and any payment card processors and/or card issuers, and allow them to reasonably investigate, review and audit Service Provider’s facilities, systems, files, procedures and records related to such occurrence. Any public disclosures required by Legal Requirements, or deemed advisable regarding the Security Incident shall, unless prohibited by Legal Requirements, be made by Service Provider only with the prior approval of Client, such approval not to be unreasonably withheld or delayed.

(h) Service Provider shall promptly notify Client if Service Provider receives any notice, demand, summons or complaint from any governmental or regulatory authority, agency or other body that calls into question or relates to Service Provider’s compliance with its obligations under this Agreement. Service Provider agrees to notify Client immediately in writing of any subpoena or other judicial or administrative order or proceeding seeking access to or disclosure of Personal Information. Client shall have the right to defend against such action in lieu of and on behalf of Service Provider. Client may, if it so chooses, seek a protective order. Service Provider shall reasonably cooperate with Client in such defense.

(i) Promptly upon the expiration or earlier termination of any Service Provider Agreement, completion of the Services, or such earlier time as Client requests, Service Provider shall return to Client or its designee or render unreadable or undecipherable if return is not desirable or reasonably feasible in the reasonable discretion of Client, each and every original and copy in every medium of all Personal Information in the possession, custody or control of Service Provider. Promptly following any return or alternate action taken to comply with this section, Service Provider shall, upon request, provide to Client a written affidavit signed by an executive officer of Service Provider certifying that such return or alternate action occurred.

3. Satisfactory Background Screening. Service Provider shall not assign any Personnel to perform Services or otherwise permit Personnel to have access to Personal Information unless Service Provider has obtained, at Service Provider’s own expense and in a manner compliant with all Legal Requirements, a Satisfactory Background Screening with respect to such Personnel. Promptly upon request by Client, Service Provider shall verify in writing its compliance with the foregoing requirements by providing Client with a written affidavit signed by an executive officer of Service Provider, certifying that Service Provider has obtained a Satisfactory Background Screening with respect to all Personnel with access to Personal Information in accordance with this Agreement. In no event shall any screening results, reports or confidential information of any individual be provided to Client hereunder. Service Provider agrees to update any Background Screening upon reasonable request by Client, it being agreed that any request based upon the occurrence of any Security Incident involving Service Provider, the reasonable suspicion of illegal activity by Service Provider or its Personnel involving Personal Information, any Legal Requirements requiring such updates, or any breach by Service Provider of this Agreement shall be deemed reasonable hereunder.

4. Additional Technical Requirements. Service Provider shall not transmit, transfer, maintain or store Personal Information without the express prior written consent of Client. Without limitation of any other term or provision herein, if Service Provider obtains such express prior written consent of Client, and transmits, transfers, maintains or stores Personal Information, Service Provider covenants and agrees to comply with Rider 1 attached hereto which is incorporated by reference into and made part of this Agreement.

5. Access to Client Information Technology Environment. Without limitation of any other term or provision herein, if Service Provider has access to the Client IT Environment, Service Provider covenants and agrees to comply with Rider 2 attached hereto which is incorporated by reference into and made part of this Agreement.

6. Cross-Border Data Transfer. Service Provider shall not engage in or permit any Cross-Border Data Transfer without the express prior written consent of Client. Without limitation of any other term or provision herein, if Service Provider obtains such express prior written consent of Client, and engages in or permits a Cross-Border Data Transfer to occur, Service Provider represents and warrants that Service Provider shall be in compliance with all applicable Legal Requirements, and that Service Provider’s activities for or on behalf of Client in connection with the Services will not cause Client or Service Provider to violate any such Legal Requirements.

7. Ongoing Review; Audit. Client shall have the right to monitor Service Provider’s compliance with the terms of this Agreement, and review and assess Service Provider’s information security systems, policies, procedures and IT operations that are involved in performance of the Services or that may affect the security, confidentiality or integrity of Personal Information. Such review may include the provision by Service Provider of written information (including, without limitation, questionnaires, audit reports, scan summaries, logs and information security policies) and/or interviews with Personnel (either by telephone or in person), and other reasonable disclosures regarding Service Provider’s administrative, technical and physical safeguards for the protection of Personal Information. During normal business hours, and with reasonable prior notice, Client and/or its authorized representatives may also inspect and review the facilities and equipment of Service Provider and its relevant agents, consultants, contractors and subcontractors. Service Provider shall allow reasonable access and provide information for such inspection and review, and Client shall make reasonable efforts to minimize any unreasonable interference with the conduct of Service Provider’s business. The foregoing requirements shall not relieve Service Provider of any of its obligations under this Agreement or any Service Provider Agreement, imply acceptance or approval by Client, or waive or derogate from any rights of Client.

8. Indemnity. Service Provider agrees to indemnify and hold harmless Client and its officers, employees, directors and agents from, and, at Client’s option, defend against, any and all claims, losses, liabilities, costs and expenses, including, without limitation, third-party claims, reasonable attorneys’ fees, consultants’ fees and court costs, arising from, or in any way attributable or relating to (a) any violation of Service Provider’s covenants, agreements or obligations set forth in this Agreement, or any breach by Service Provider of any certification, representation or warranty made hereunder; (b) the negligence, gross negligence, bad faith or intentional or willful misconduct of Service Provider or its Personnel, Authorized Subcontractors or other agents; and (c) any Security Incident for which Service Provider or any Personnel, Authorized Subcontractors or other agents are responsible. Service Provider’s obligations hereunder shall not be subject to any limitation on, or disclaimer or release of, any liability, or any disclaimer of warranties set forth in, any Service Provider Agreement or any other prior agreement or writing between Service Provider and Client.

9. Miscellaneous.

(a) Service Provider agrees that any non-compliance with Section 2 of this Agreement, the occurrence of any Security Incident, or a violation of any Privacy Requirement may cause immediate and irreparable harm to Client for which money damages may not constitute an adequate remedy. Accordingly, Service Provider agrees that Client may (i) immediately suspend Service Provider’s performance or otherwise immediately terminate any and all agreements then in effect with Service Provider, and (ii) obtain specific performance and injunctive or other equitable relief for any such violation, in addition to its remedies at law, without proof of actual damages. Service Provider agrees to waive any requirement for the securing or posting of any bond in connection with such remedy.

(b) Service Provider’s obligations under this Agreement shall survive the termination of any Service Provider Agreement and the termination or completion of the Services.

(c) This Agreement and all controversies arising from or relating to performance of this Agreement shall be governed by, and construed and enforced in accordance with, the laws of The Commonwealth of Massachusetts without giving effect to its rules concerning conflicts of laws that might provide for any other choice of law. Client and Service Provider hereby (i) irrevocably consent to personal jurisdiction in the appropriate Commonwealth court in the County of Middlesex, Massachusetts, or any Federal court sitting in the District of Massachusetts for the purposes of any suit, action or other proceeding arising out of the Agreement or any of the agreements or transactions contemplated hereby, which is brought by either party hereto against the other party, (ii) waive any objection to venue with respect thereto, and (iii) agree that all claims in respect of any such suit, action or proceeding shall be heard and determined in any such court, and that such courts shall have exclusive jurisdiction over any claims arising out of or relating to such agreements or transactions.

(d) Notices provided hereunder must be in writing and sent by certified mail, return receipt requested, all postage prepaid; courtesy copies may be sent via facsimile or electronically. Notices to Service Provider shall be sent to: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. Notices to Client shall be sent to: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

(e) This Agreement and each Rider hereto constitutes the complete agreement between the parties and supersedes any prior oral or written agreement between the parties concerning the subject matter hereof. In the event of any conflict between this Agreement and any Service Provider Agreement, nondisclosure, confidentiality or other agreement, this Agreement shall govern.

(f) If any provision of this Agreement is held invalid or unenforceable, the remaining provisions shall remain in effect. A waiver by either party of any term or condition of the Agreement in one or more instances shall not constitute a permanent waiver of the term or condition or any other term or condition of the Agreement or a general waiver.

(g) Service Provider may not transfer, modify, amend or assign this Agreement, in whole or in part, except in a writing signed by both parties. Any such transfer, modification, amendment or assignment without Client’s prior written consent shall be null and void. If an assignment occurs, the assignment shall not relieve the assigning party of its liabilities or obligations under the Agreement. Client may, without restriction, transfer or assign this Agreement, in whole or in part, or transfer or assign any of its rights or obligations hereunder, by delegation, subcontracting, operation of law, or otherwise without the prior written consent of Service Provider. The Agreement is binding upon successors and assigns of the parties, including, without limitation, any successor to or assignee of Service Provider’s rights or obligations under any Service Provider Agreement.

(h) Service Provider shall keep strictly confidential the existence of this Agreement, the terms and conditions contained herein, and all information and materials disclosed to or shared with Service Provider in connection with this Agreement or the Services (including, without limitation, any Client Information Security Policy, any Access Tool (as defined in Rider 2) or any other information regarding the Client IT Environment). In no event shall the foregoing limit Service Provider’s obligation to comply with any stricter confidentiality obligations set forth in any Service Provider Agreement.

WITNESS THE EXECUTION HEREOF as a Massachusetts instrument under seal by duly authorized representatives of the parties hereto as of the \_\_\_\_ day of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, 2009.

CLIENT VENDOR

By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_