CONSULTING AGREEMENT

I. INTRODUCTION

This Consulting Agreement, entered into this [____] day of [_____], 20[__] is by and between CLIENT COMPANY (hereinafter referred to as "CLIENT COMPANY"), whose principal place of business is 123 Main Street, Jacksonville, Florida 32222 and [_____], a _____ company (hereinafter referred to as "Consultant"), whose business address is [_____].

II. STATEMENT OF WORK

Consultant will provide the following professional services (hereinafter referred to as "Services"):

Services as described in the Statement of Work ("SOW") dated [___] day of [_____], 20[__] and attached to this Agreement as Exhibit A.

Consultant may perform other Services as directed by CLIENT COMPANY in the form of a separate SOW signed by an authorized officer on behalf of CLIENT COMPANY. Any additional SOWs shall be in the format prescribed in Exhibit A to this Agreement. Each SOW shall be governed by the terms of the Agreement. In the event of a conflict between any term of this Agreement and an SOW, the terms of this Agreement shall control unless the SOW expressly provides that it is intended to supersede a particular provision of this Agreement. Such provision must be clearly set forth in the SOW and such amendment of such provision shall be for that particular SOW only.

In the event of a conflict between a term of the Proposal and a term hereof, the term hereof shall control to the extent of such conflict and, to the extent of such conflict, the term of the Proposal shall be of no force or effect.

III. TERM

The Agreement is from [_____] [___], 20[___] to [____] [__], 20[__], unless sooner terminated pursuant to the termination provisions contained herein. This Agreement may be extended by written agreement of the parties. Any extension shall be negotiated as to the applicable fees and expenses.

IV. TERMINATION

This Agreement may be terminated at any time for any reason, or for no reason, by either party upon ten (10) days prior written notice of the terminating party to the other party. The parties shall mutually agree upon the handling of any uncompleted Services. Termination of the Agreement will automatically terminate all SOWs hereunder. Any SOW to this Agreement may be terminated at any time for any reason, or for no reason, by either party upon ten (10) days prior written notice of the terminating party to the other party. Termination of a SOW shall not terminate the Agreement.

V. INDEPENDENT CONTRACTOR

Consultant and its employees (if any) are independent contractors and not employees of CLIENT COMPANY. Neither Consultant nor any of its employees shall hold themselves out as agents or employees of CLIENT COMPANY in connection with the performance of Services hereunder or any other matter. Consultant agrees that all Services will be performed by employees of Consultant. Consultant is responsible for compliance with applicable federal and state laws and specifically assumes exclusive responsibility for payment of all taxes or contributions which, under such laws, may be payable based upon the amounts paid by CLIENT COMPANY to Consultant, including, by way of illustration but not limitation, federal and state income taxes; social security taxes; unemployment compensation taxes, worker's compensation assessment; and any other taxes, assessments, or business license fees required. At no time shall Consultant make any commitments or incur any charges or expenses for, or in the name of CLIENT COMPANY. Consultant acknowledges that none of Consultant's employees are entitled to participate in any of CLIENT COMPANY's benefit plans, even if a court or administrative body determines that any employee of Consultant is an employee of CLIENT COMPANY.

Consultant shall be free at all times to arrange the time and manner of performance of the Services to be rendered and will not be expected to maintain a schedule of duties or assignments. Consultant will not report to CLIENT COMPANY on a regular basis, but will work as it may so independently decide. Consultant guarantees CLIENT COMPANY that Consultant will provide CLIENT COMPANY with adequate and sufficient performance of all

Services set forth herein. In addition, Consultant agrees to submit frequent progress reports (monthly, at a minimum) showing the project status of all Services set forth herein.

CLIENT COMPANY does not retain or exercise the right to direct, control and supervise Consultant or Consultant's employees as to the details and means by which the Services are accomplished and Consultant shall be responsible for Consultant's expenses for securing secretarial and clerical support. However, due to the confidential nature of the Services to be performed under this Agreement and Consultant's need to have access to information which CLIENT COMPANY wishes to keep secure by maintaining it on its premises, Consultant may be required to perform some of its Services required herein on CLIENT COMPANY premises. If on CLIENT COMPANY premises, Consultant shall have access to secretarial and clerical support from CLIENT COMPANY, if available. Consultant will arrange the time and manner of performance of the Services at times mutually agreeable to CLIENT COMPANY, and as set forth in this Agreement. Consultant is not restricted in any way by this Agreement from providing consulting services to another entity or person.

VI. STATEMENTS

CLIENT COMPANY agrees to pay Consultant the fees as set forth in the applicable SOW. In addition, reasonable travel expenses incurred by Consultant in connection with this Agreement will be paid by CLIENT COMPANY as set forth in an applicable SOW, if approved by CLIENT COMPANY in advance. Statements submitted by Consultant are due and payable by CLIENT COMPANY within thirty (30) days of the receipt date of invoice.

VII. CONFIDENTIALITY

All materials furnished to Consultant pursuant to this Agreement (except information and materials obtained by Consultant from sources without an obligation of confidentiality to CLIENT COMPANY or otherwise available to the general public) are confidential and Consultant will treat such materials as confidential and will not reveal or discuss such materials or any other information learned as a result of this Agreement, with any other person or entity, except as authorized or directed by CLIENT COMPANY or by law or court order. In addition, working papers, copies, internal documents, procedures, methods and related materials which contain information furnished to Consultant by CLIENT COMPANY or which come into Consultant's possession as a result of this Agreement are considered confidential and/or proprietary and Consultant will treat such information as confidential and/or proprietary and will not reveal or discuss any such information with any other person or entity, except as authorized or directed by CLIENT COMPANY or by law or court order. All such records and materials will remain the property of CLIENT COMPANY and will be returned to CLIENT COMPANY by Consultant at the termination of this Agreement.

Without CLIENT COMPANY's prior written consent, Consultant shall not in any manner disclose, advertise or publish the existence or terms of or transactions under this Agreement.

VIII. COPYRIGHTS

The parties agree that, except for Third Party Materials, Client Materials, and Consultant Pre-Existing Material, all rights, title and interest in any and all of the following shall be owned by CLIENT COMPANY in perpetuity, including, without limitation, the copyright, patent, trademark, trade secret, and all other property and proprietary rights therein: (i) the results and proceeds of Consultant's Services provided hereunder (and those of its employees and contractors); (ii) any deliverables identified in and/or delivered in connection with any SOW; (iii) the Specifications; and (iv) any copies and derivations made thereof. All such results and proceeds and deliverables shall be deemed a work for hire for CLIENT COMPANY (hereinafter the material set forth herein above may together be referred to as "Service Results"). In the event, for any reason, any such Service Results are for any reason not a work for hire, then Consultant (and its employees and contractors) hereby assigns to CLIENT COMPANY all right, title and interest in all such Service Results in perpetuity to CLIENT COMPANY, other than in the Third Party Materials, Client Materials and Consultant Pre-Existing Material. Consultant shall ensure that the terms of this paragraph are complied with in all of its agreements and arrangements with its employees and contractors. Consultant shall complete (and shall require its employees and contractors to complete) such additional documents as are requested from CLIENT COMPANY and which are necessary from time to time to carry out the terms of this paragraph.

To the extent that any results and proceeds of Consultant's services to be provided hereunder or any deliverable to be delivered by Consultant under any SOW is to include any material owned by third parties for which a license is

required (other than Client Material or Consultant Pre-Existing Material), Consultant shall identify such material in the SOW and the parties shall reflect in the SOW who shall be responsible for securing for CLIENT COMPANY a license to use such material in the deliverable, which license, if to be secured by Consultant, shall be subject to CLIENT COMPANY approval. When used in this Agreement, the term Third Party Material shall refer only to third party material so identified in a SOW in accordance with this subparagraph.

To the extent that any results and proceeds of Consultant services to be provided hereunder or any deliverable to be delivered by Consultant under any SOW is to include any material that is owned by Consultant and was in existence prior to the Effective Date of this Agreement, Consultant shall identify such material in the SOW and hereby does grant to CLIENT COMPANY in perpetuity a nonexclusive royalty-free license to copy, modify, adapt, publish, distribute, sublicense, make derivative works of and otherwise use in any way, such material. When used in this Agreement, the term Consultant Pre-Existing Material shall refer only to material so identified in a SOW in accordance with this subparagraph.

Consultant agrees that no portion of the work prepared for CLIENT COMPANY in performance of this Agreement is either derived from any copyrighted material or is subject to any interest, proprietary or otherwise, or any claim of any third party, and that Consultant has disclosed this work product to CLIENT COMPANY only.

IX. HOLD HARMLESS AND INDEMNITY

Consultant agrees to indemnify and save harmless CLIENT COMPANY, its affiliates, officers, directors, employees, successors, and assigns from and against any and all losses, damages, claims, demands, suits, liability and expenses, including reasonable attorneys' fees, that arise out of or result from (1) any bodily injuries to any person or persons or any damages to property to the extent resulting from Consultant's negligent, illegal, or willful, wanton and reckless acts or omissions and/or (2) that Consultant's negligent acts or omissions or intentional wrongdoing in connection with that Consultant's performance of this Agreement. Consultant agrees to defend CLIENT COMPANY against any such claim, demand, or suit. CLIENT COMPANY agrees to notify Consultant within a reasonable time of any written claims or demands against CLIENT COMPANY for which Consultant is responsible under this clause.

X. INDIVIDUALLY IDENTIFIABLE HEALTH OR FINANCIAL INFORMATION

CLIENT COMPANY and Consultant agree that Consultant provides certain services for CLIENT COMPANY which may involve the use and/or disclosure of Protected Health Information and Nonpublic Personal Financial Information (both as hereinafter defined) and Consultant is a "Business Associate" as defined in 45 CFR § 160.103 of the federal rules implementing the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA-AS"), including but not limited to the Privacy and Security Rules, and a "Non-Affiliated Third Party Service Provider" as described in § 4-128.014 of the Florida rules implementing Title V of the Gramm-Leach-Bliley Act. Consultant specifically agrees to CLIENT COMPANY's standard Business Associate Agreement, which by this reference is incorporated into this Agreement and is attached hereto as Exhibit B. In the event of a conflict between the terms of this Agreement and the Business Associate Agreement, the Business Associate Agreement shall prevail. Further and notwithstanding the foregoing, including Exhibit B, Consultant is responsible for identifying and requesting the minimum information necessary to perform the Services necessary to fulfill the any SOW pursuant to this Agreement. Consultant accepts the obligation to verify that Consultant is requesting the minimum necessary information and will hold CLIENT COMPANY harmless for any consequences if Consultant fails its obligations under this Section, including Exhibit B.

XI. VENDOR SECURITY AGREEMENT

Consultant agrees to the terms and conditions of CLIENT COMPANY's Vendor Security Agreement attached to this Agreement as Exhibit C.

XII. INSURANCE

During the term of this Agreement, Consultant shall maintain in effect the following minimum levels of insurance:

a. Commercial General Liability. Combined bodily injury and property damage limits of liability of at least $1,000,000 per occurrence, $2,000,000 general aggregate and $2,000,000 products and completed operations aggregate. The policy must be endorsed to add CLIENT COMPANY, its subsidiaries and

Affiliates as additional insureds. The policy must provide primary coverage and be endorsed to provide waiver of subrogation in favor of CLIENT COMPANY, its subsidiaries and Affiliates.

b. Automotive Liability. Coverage for all owned, hired and non-owned vehicles used in the performance of the Services or brought onto the premises of CLIENT COMPANY or its Affiliates with a combined bodily injury and property damage limit of at least $1,000,000.

c. Workers' Compensation and Employers Liability. Coverage as required by Florida Workers' Compensation statutes or the Workers' Compensation statutes where the work is being performed, where employees reside and in accordance with the laws of each state. The policy will be endorsed to provide a waiver of subrogation in favor of CLIENT COMPANY and its subsidiaries and Affiliates. The policy will include Employers Liability coverage with limits of liability not less than $500,000 Each Accident; $500,000 Disease - Policy Limit; $500,000 Disease - Each Employee.

d. Commercial Umbrella Liability. Umbrella Liability coverage over a schedule of underlying liability coverages as described above including Commercial General Liability, Automobile Liability and Employers Liability for a combined bodily injury and property damage limit of at least $2,000,000 each occurrence and $2,000,000 general aggregate.

e. Employee Theft. Coverage with limits of at least $500,000 per occurrence, including coverage for clients' property.

f. Professional Liability. Professional or Errors & Omissions Liability with limits of at least $1,000,000 per claim and $3,000,000 aggregate.

g. Cyber/Privacy Liability. Cyber/Privacy Liability with limits of at least $5,000,000 per claim and $5,000,000 aggregate.

XIV. NOTICES

Any notice, amendment, or consent required or permitted under this Agreement shall be in writing and transmitted to the recipient by either (i) courier delivery; (ii) Federal Express or similar overnight courier delivery; or (iii) U.S. certified mail, return receipt requested, postage prepaid. All notices are to be courier delivered or mailed to the addresses and persons identified on page one (1) of this Agreement, or to such other address as shall be furnished in writing by either party to the other. Notices or communications shall be deemed given upon the date of (a) courier of Federal Express delivery, or (b) in the case of transmittal by U.S. certified mail, return receipt requested, the date the return receipt is signed or delivery is rejected.

XV. COMPLIANCE PROGRAM

Consultant acknowledges that it has received and reviewed a copy of the Compliance Program[SM] booklet and will require all of its principals and employees who perform Services for CLIENT COMPANY pursuant to this Agreement to review the booklet. Consultant will execute the attached Acknowledgment Certificate evidencing receipt and review of the booklet and that Consultant and its principals and employees will comply with the business conduct policies and procedures set forth in the booklet. Consultant agrees to report any Compliance Program[SM] violations to CLIENT COMPANY's Business Ethics, Integrity and Compliance - Privacy Office.

XVI. EXCLUDED ENTITY

(a) As of [the Effective Date], Neither Consultant nor any of its owners, principals, agents, or employees performing the Services are excluded, debarred, suspended, proposed for suspension or debarment, or otherwise ineligible for participation in any federal procurement or federal health benefit program.

(b) Consultant shall promptly notify Plan in the event that Consultant or any of its owners, principals, agents, or employees are excluded, debarred, suspended, proposed for suspension or debarment, or otherwise ineligible for participation in any federal procurement or federal health benefit program.

XVII. SURVIVAL OF OBLIGATIONS

Any provision of this Agreement which requires or reasonably contemplates the performance or existence of obligations by either party after the termination of the Agreement shall survive such termination period.

XVIII. ASSIGNMENT AND DELEGATION

No right or interest in this Agreement shall be assigned by Consultant without the prior written permission of CLIENT COMPANY, and no delegation of Services or other obligations owed by Consultant to CLIENT COMPANY shall be made without CLIENT COMPANY's prior written permission. CLIENT COMPANY may assign this Agreement to a subsidiary or affiliate company upon written notice to Consultant. Any attempted assignment or delegation in contravention of the above provision shall be void and ineffective.

XIX. NON-EXCLUSIVE RIGHTS

This Agreement does not grant to Consultant any exclusive privileges or rights to provide to CLIENT COMPANY the Services of any type which CLIENT COMPANY may require, nor requires the purchase of such Services by CLIENT COMPANY. CLIENT COMPANY may contract with other companies or individuals for the procurement of comparable Services.

XX. SECTION HEADINGS

The headings of the several sections are inserted for convenience or reference only and are not intended to be part of, or to effect, the meaning or interpretation of this Agreement.

XXI. APPLICABLE LAW

The construction, interpretation and performance of this Agreement and all transactions under it shall be governed by the laws of the state of Florida.

XXII. NON-WAIVER

No course of dealing or failure of either party to strictly enforce any term, right or condition of the Agreement shall be construed as a waiver of such term, right or condition.

XXIII. SEVERABILITY

If any of the provisions of this Agreement shall be invalid or unenforceable, such invalidity or unenforceability shall not invalidate or render unenforceable the entire Agreement, but rather the entire Agreement shall be construed as if not containing the particular invalid or unenforceable provision or provisions, and the rights and obligations of each party shall be construed and enforced accordingly.

XXIV. ENTIRE AGREEMENT

This Agreement shall constitute the entire Agreement between the parties with respect to the subject matter of this Agreement and shall not be altered, varied, revised or amended except in writing signed by both parties. The provisions of this Agreement supersede all prior oral or written quotations, communications, agreements and understandings of the parties with respect to the subject matter of this Agreement.

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be executed by their respective duly authorized representatives as of the day and year first above written.

Consultant: [_____]	CLIENT COMPANY
BY: _____	By: _____
Title: _____	Title: _____

_____

Social Security Number or Federal Tax I.D. Number

Acknowledgment Certificate

The undersigned Consultant, on behalf of its principals and employees has received and reviewed the Compliance Program[SM] booklet, agrees to comply with the business conduct policies and procedures set forth in the booklet and report any Compliance Program[SM] violations to CLIENT COMPANY's Business Ethics, Integrity and Compliance - Privacy Office.

_____

CONSULTANT

Name: _____

Title: _____

Date: _____

Exhibit A

Statement of Work

STATEMENT OF WORK
NO. _____

to the Consulting Agreement ("Agreement")
by and between
CLIENT COMPANY ("CLIENT COMPANY")
and
_____ ('Consultant")

This STATEMENT OF WORK NO. [___] is made as of this [__] day of [_____], 20[__] by and between CLIENT COMPANY and Consultant and is hereby incorporated into and made a part of the Agreement dated [_____] as follows:

(1) Project Overview:

[Brief description of the purpose and main objectives of the project. This section should address such issues as why you are contracting for the SOW effort, how the SOW effort fits into the "big picture", and the primary technical/management objectives of the SOW effort.]

(2) Detailed Description of Services:

[Detailed description of all the services to be performed.]

(3) Key Personnel:

[List Names of Key Personnel required by CLIENT CPOMPANY to perform Services, if any.]

(4) Specifications of Deliverables:

[Specific specifications for the deliverables. The specification needs to be specific enough to let the contractor know what you expected of them, but general enough allow them to be creative in solving the problem.]

(5) Project Schedule:

[Provide a schedule broken down either hourly or into to tasks or milestones. There are a number of software tools available today that help a Consultant develop and manage a project schedule – list which one the Consultant uses and how often the scheduled maybe supplied. Include where and how deliverables will be delivered or implemented.]

(6) Fees :

[List time and materials or fixed fee payment, broken into hourly rates, estimated amounts, or for fixed fees for each deliverables.]

(7) Payment Schedule:

[Add payment schedule based on dates or milestones.]

(8) Third Party Technology:

[Add all pre-existing technology of the Consultant's or a third party that will be used in performing the services or provided with the deliverables.]

Consultant:	CLIENT COMPANY
By:_____	By:_____
Print Name:_____	Print Name:_____
Title:_____	Title:_____

Exhibit B

Business Associate Agreement

ADDENDUM TO THE CONSULTING AGREEMENT

This Addendum (the "Addendum"), dated as of the **[_____] day of [_____], 20[__]** (the "Effective Date") is added to the Consulting Agreement (the "Agreement"), dated the _____ day of _____, entered into by [_____] ("Business Associate") and CLIENT COMPANY ("CLIENT COMPANY"). The terms and conditions of this Addendum are incorporated by reference into and made a part of the Agreement.

WHEREAS, CLIENT COMPANY and Business Associate have entered into the Agreement whereby Business Associate provides certain services for CLIENT COMPANY which may involve the use and/or disclosure of Protected Health Information and Nonpublic Personal Financial Information (both as hereinafter defined); and

WHEREAS, CLIENT COMPANY and Business Associate agree that Business Associate is a "Business Associate" as defined in 45 CFR § 160.103 of the federal rules implementing the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA-AS"), including but not limited to the Privacy and Security Rules, and a "Non-Affiliated Third Party Service Provider" as described in § 4-128.014 of the Florida rules implementing Title V of the Gramm-Leach-Bliley Act; and

WHEREAS, CLIENT COMPANY and Business Associate desire to modify the Agreement to comply with the requirements of HIPAA-AS and Florida law as applicable to CLIENT COMPANY's relationship to Business Associate.

NOW, THEREFORE, in consideration of the mutual promises contained herein, CLIENT COMPANY and Business Associate hereby agree as follows:

1. **Definitions**

For purposes of this Addendum, the following terms shall have the meanings set forth below:

a) *Breach* shall mean the unauthorized acquisition, access, use or disclosure of PHI which compromises the security or privacy of the PHI.

b) *Electronic Protected Health Information or EPHI* shall have the meaning set forth in 45 CFR 160.103.

c) *Nonpublic Personal Financial Information* shall have the meaning set forth in Fla. Admin. Code 4-128.002 except Nonpublic Personal Financial Information shall be limited to that information created or received by a Business Associate for or on behalf of CLIENT COMPANY pursuant to this Agreement.

d) *Protected Health Information or PHI* shall have the meaning set forth in 45 CFR 160.103, limited to the information created or received by Business Associate from or on behalf of CLIENT COMPANY. For purposes of this Addendum, PHI encompasses CLIENT COMPANY's EPHI.

e) *Secure Computing Device* shall mean computing equipment in which access is limited and requires authorization; and appropriate preventative and detective security mechanisms are implemented and maintained. In addition, computing devices that are portable must have safeguards that render Electronic Protected Health Information unusable, unreadable or indecipherable to unauthorized individuals and is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute. Portable computing devices include but are not limited to, portable computers; Personal Digital Assistants; Smart Phones; Blackberry or equivalent technologies; portable or removable storage devices; or other portable electronic equipment capable of storing electronic information; networking equipment either wired or wireless.

f) *Security Incident* shall mean the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

g) *Unsecured PHI* shall mean PHI that is not secured through the use of technology or methods approved by the Secretary of Health and Human Services to render the PHI unusable, unreadable or indecipherable to unauthorized individuals.

Other capitalized terms used throughout this Addendum, including Required by Law, Health Care Operations, Payment and Treatment, shall have the meanings as are set forth in relevant HIPAA regulations.

2. Privacy and Security of Protected Health Information.

a) **Permitted Uses and Disclosures**. Except as otherwise limited in this Addendum, Business Associate may use, disclose or request the minimum necessary Protected Health Information and Nonpublic Personal Financial Information to perform functions, activities, or services for, or on behalf of, CLIENT COMPANY as specified in the Agreement, provided that such use, disclosure or request would not violate the HIPAA-AS Privacy Rule if done by CLIENT COMPANY.

b) **Prohibition on Unauthorized Use or Disclosure**. Business Associate shall not use or disclose Protected Health Information or Nonpublic Personal Financial Information other than as permitted or required by this Addendum or as Required by Law.

c) **Information Safeguards and Breach Reporting**.

(i) **Privacy of Protected Health Information**. Business Associate shall use appropriate safeguards to prevent use or disclosure of Protected Health Information and Nonpublic Personal Financial Information not provided for by this Addendum.

Business Associate shall report in writing to CLIENT COMPANY's Business Ethics, Integrity and Compliance - Privacy Office any use or disclosure of Protected Health Information or Nonpublic Personal Financial Information not provided for by this Addendum, including a Breach of Unsecured PHI, as soon as practicable but no later than five (5) days after Business Associate becomes aware of such unauthorized use or disclosure. Unless otherwise directed by CLIENT COMPANY's Business Ethics, Integrity and Compliance - Privacy Office, Business Associate shall include in the report the following:

(A) the date of the unauthorized use or disclosure;

(B) the name and (if known) address of the person or entity which received Protected Health Information pursuant to the unauthorized disclosure;

(C) a brief description of the Protected Health Information that was the subject of the unauthorized use or disclosure;

(D) a brief statement of the nature of the unauthorized use or disclosure;

(E) the name and date of birth of the individual(s) whose Protected Health Information was the subject of the unauthorized use or disclosure, and each such individual's contract number;

(F) the corrective action that Business Associate has taken or will take to prevent further unauthorized uses or disclosures; and

(G) the steps Business Associate has taken or will take to mitigate any known harmful effects of the unauthorized use or disclosure.

Upon notification by Business Associate, CLIENT COMPANY shall be responsible for determining the need for and directing the implementation of any notification concerning any Breach of Unsecured PHI, and Business Associate shall, at CLIENT COMPANY's direction, cooperate with or perform any additional investigation and/or assessment necessary to determine and document whether a Breach of Unsecured PHI has occurred and shall provide any and all related documentation to CLIENT COMPANY.

(ii) **Security of Electronic Protected Health Information**. Business Associate shall implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of Electronic Protected Health Information. Business Associate shall only store Electronic Protected Health Information on Secure Computing Devices, controlled and/or maintained by the Business Associate.

Business Associate shall report in writing to CLIENT COMPANY's Business Ethics, Integrity and Compliance - Privacy Office any successful Security Incident as soon as practicable but no later than five (5) days after Business Associate becomes aware of such Security Incident and shall submit follow-up documentation pursuant to the direction of CLIENT COMPANY's Business Ethics, Integrity and Compliance - Privacy Office. Upon CLIENT COMPANY's request and pursuant to CLIENT COMPANY's direction, Business Associate shall report in writing any attempted but unsuccessful Security Incident of which Business Associate becomes aware.

d) **Mitigation**. Business Associate shall mitigate to the extent practicable any harmful effect of which Business Associate is aware that is caused by any use or disclosure of Protected Health Information or Nonpublic Personal Financial Information not provided for by this Addendum.

e) **Agents and Subcontractors**. Business Associate shall ensure that its agents and subcontractors to whom it provides Protected Health Information agree in writing to the same privacy and security restrictions and conditions that apply through this Addendum to Business Associate with respect to such information.

f) **Business Associate Guidance**. Business Associate shall comply with any policy, procedure or guidance with respect to Business Associate's responsibilities under this Addendum that CLIENT COMPANY may, from time to time, issue and communicate in writing to Business Associate.

3 Management of Protected Health Information.

a) Access. Business Associate shall, within seven (7) days following CLIENT COMPANY's request, make available to CLIENT COMPANY for inspection and copying Protected Health Information about an individual that is in Business Associate's custody or control, so that CLIENT COMPANY may meet its access obligations under the HIPAA-AS Privacy Rule.

b) Amendment. Business Associate shall, within fourteen (14) days following CLIENT COMPANY's request, amend or permit CLIENT COMPANY to amend any portion of Protected Health Information that is in Business Associate's custody or control so that CLIENT COMPANY may meet its amendment obligations under the HIPAA-AS Privacy Rule.

c) Disclosure Accounting. Business Associate shall record the information specified below ("disclosure information") for each disclosure of Protected Health Information that Business Associate makes, excluding disclosures identified in 45 CFR § 164.528(a)(1) including but not limited to disclosures for Treatment, Payment, and Health Care Operations and disclosures pursuant to a HIPAA-AS compliant authorization, and shall report the disclosure information to CLIENT COMPANY's Business Ethics, Integrity and Compliance - Privacy Office in writing within five (5) days of Business Associate making the accountable disclosure. Disclosure information shall include:

(i) the disclosure date;

(ii) the name and (if known) address of the person or entity to which Business Associate made the disclosure;

(iii) a brief description of the Protected Health Information disclosed;

(iv) a brief statement of the purpose of the disclosure;

(v) the name and date of birth of the individual whose Protected Health Information was disclosed; and

(vi) that individual's contract number.

d) Inspection of Internal Practices, Books and Records. Business Associate shall make its internal practices, books, and records relating to its use and disclosure of Protected Health Information and its protection of the confidentiality, integrity, and availability of Electronic Protected Health Information available to CLIENT COMPANY and the U.S. Department of Health and Human Services ("HHS") as requested or required to determine CLIENT COMPANY's compliance with the HIPAA-AS Privacy Rule and Security Rule.

4 Breach of Privacy and Security Obligations.

a) Termination of Addendum.

(i) Term. The Term of this Addendum shall commence on the Effective Date and shall terminate upon termination of the Agreement.

(ii) Breach of Addendum. CLIENT COMPANY and Business Associate specifically acknowledge and agree that a breach of any term of this Addendum shall be considered a breach of a material term of the Agreement and CLIENT COMPANY may terminate this Addendum and the Agreement in accordance with the Agreement's termination provision.

b) Obligations on Termination.

(i) Return or Destruction of Protected Health Information. Upon termination of the Agreement, Business Associate shall, if feasible, return to CLIENT COMPANY or destroy all Protected Health Information in its custody or control in whatever form or medium, including all copies and all derivative data, compilations, and other works that allow identification of any individual who is a subject of the Protected Health Information. Business Associate shall in writing identify to CLIENT COMPANY any Protected Health Information that cannot feasibly be returned to CLIENT COMPANY or destroyed and explain why return or destruction is infeasible. Business Associate shall limit further use or disclosure of such Protected Health Information to those purposes that make its return or destruction infeasible. Business Associate shall complete these obligations as promptly as possible, but not later than thirty (30) days following the effective date of the termination of the Agreement.

(ii) Continuing Privacy and Security Obligations. Business Associate's obligation to protect the privacy and confidentiality and safeguard the security of Protected Health Information as specified in this Addendum shall be continuous and survive termination of the Agreement.

5. HITECH Compliance

Business Associate shall comply with all applicable requirements of Title XIII, Subtitle D of the Health Information Technology for Economic and Clinical Health Act ("HITECH"), 42 U.S.C. Sections 17921-17954 and all applicable HITECH implementing regulations issued by the Department of Health and Human Services as of the date by which Business Associate must comply with such statutory and regulatory requirements.

6. General Provisions.

a) Amendment to Addendum. This Addendum shall automatically amend upon the compliance date of any final regulation or amendment to final regulation promulgated by HHS or a Florida regulatory agency concerning the subject matter of this Addendum such that Business Associate's obligations remain in compliance with the final

regulation or amendment to final regulation, unless CLIENT COMPANY or Business Associate elects to terminate this Addendum by giving the other party written notice of termination at least ninety (90) days before the compliance date of such final regulation or amendment to final regulation.

b) No Third Party Beneficiaries. No party shall be deemed a third party beneficiary of this Addendum.

c) Conflicts. This Addendum shall supersede any conflicting term or provision in the Agreement. In all other respects, the terms and conditions of the Agreement shall remain unchanged and in full force and effect.

IN WITNESS WHEREOF, the parties have executed this Addendum as of the Effective Date.

CLIENT COMPANY

By:_____
(Signature)

Name:_____
(Print)

Title:_____

[_____]

By:_____
(Signature)

Name:_____
(Print)

Title:_____

Exhibit C

Vendor Security Agreement

to the Consulting Agreement ("Agreement")
by and between
CLIENT COMPANY ("CLIENT COMPANY")
and
Consultant

This Exhibit B (the "Exhibit") is made as of the Effective Date by and between CLIENT COMPANY and Consultant, as follows:

1. "Protected Information" (PI) includes all information protected under various legislative and state and federal regulatory requirements including, but not limited to, Gramm-Leach-Bliley (GLB) for financial information, HIPAA-AS for protected health information (PHI), the Privacy Act, agency requirements for federal and state health programs (Medicare, Medicaid, FEP, etc.), as well as any applicable state restrictions on sensitive health data. It also applies to information transmitted or maintained electronically, orally, on paper or other media. Examples of Protected Information includes, but is not limited to:
   - **a.** Past, present or prospective members and employees of CLIENT COMPANY
   - **b.** Past, present or future physical or mental health, or condition of an individual
   - **c.** Past, present or future provision of health care or financial services
   - **d.** Past, present or future payment for the provision of health care or financial services.

2. **"Security Incident"** is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with systems operations in an information system.

3. Consultant shall implement the security measures set forth herein and maintain documentation confirming such implementation. Such documentation shall be made available upon the request of CLIENT COMPANY. Failure of Consultant to materially comply with the provisions and requirements of this Exhibit shall entitle CLIENT COMPANY to terminate immediately, upon notice to Consultant, the services agreement between the parties and the Consultant Security Agreement**.**

4. **Security Compliance**
   a. Within thirty (30) days of the date this Exhibit is executed (hereafter referred to as the "Effective Date"), Consultant shall provide CLIENT COMPANY with a detailed written notification of any and all instances of Consultant non-compliance with the requirements described in this Exhibit, as well as, a summary of corrective actions to achieve compliance with each outstanding requirement.
   b. Consultant shall provide immediate notification should Consultant become non-compliant during the period of the Consultant Security Agreement, as well as, a summary of corrective actions to achieve compliance with each outstanding requirement.
   c. Consultant shall implement the outstanding controls within the first year following the Effective Date.
   d. Consultant shall require that all third parties, including subcontractors, comply with the security requirements set forth herein.

5. **Certification**
   a. Within one (1) year of the Effective Date, and at Consultant's expense, Consultant shall earn an information security certification from a firm that specializes in enterprise information security assessment and certification. The certification must be maintained by Consultant for the entire duration of the services agreement with CLIENT COMPANY. The following certification programs are acceptable for the purposes of this Exhibit:
      i. CyberTrust (Verizon Business Services) Security Management Program and Certification,
      ii. VeriSign's Information Security Program,
      iii. a properly scoped annual SAS70 Type 2 review that includes assessment of the entire IT infrastructure that supports the services provided by Consultant and related security policies and practices, or
      iv. an ISO 27001 Certification from a nationally recognized accrediting body.

b. Upon request, Consultant will complete a CLIENT COMPANY-supplied Security Certification annually.

6. Confidentiality

a. Consultant shall restrict access to CLIENT COMPANY's information to only employees, contractors, and other third parties (hereafter referred to as "Consultant Personnel") who are performing business functions specific to CLIENT COMPANY.
b. Consultant shall grant access to CLIENT COMPANY's information only as part of a documented process to determine the appropriate "minimum necessary" access requirements.
c. Consultant shall review access to CLIENT COMPANY's information to ensure access has only been granted to authorized Consultant Personnel:
    i. at least once every twelve (12) months for CLIENT COMPANY information accessed, stored or processed on Consultant systems, and
    ii. at least monthly for all Consultant Personnel that have been issued credentials to CLIENT COMPANY systems.
d. Under no circumstances shall user names or passwords associated with accounts that allow access to CLIENT COMPANY's information be shared or transferred among Consultant Personnel.

7. Information Sharing or Transfer

a. Related to any of CLIENT COMPANY's information, Consultant must obtain written authorization from CLIENT COMPANY at least 30 days prior to the first instance of any recurring information sharing or transfers to Consultant's subcontractors or other third parties (including but not limited to CD, DVD, diskette, tape, USB drive or network-based information transfers). Consultant shall obtain written authorization from CLIENT COMPANY at least 30 days prior to all one-time or non-recurring information sharing or transfers of CLIENT COMPANY's information by Consultant to any other party.
b. When sharing information with subcontractors or other third parties, Consultant shall maintain an instance specific accounting of all CLIENT COMPANY's customer specific information to include the following:
    i. the date the information was shared,
    ii. the recipient of the information,
    iii. a description of the information,
    iv. a member by member accounting, and
    v. the reason the information was shared.
c. For all network-based information transfers between CLIENT COMPANY and Consultant and involving CLIENT COMPANY's information, Consultant will use secure transmission methods (such as private circuits, frame relay connections, virtually private encrypted connections, or encrypted information transfer protocols), as agreed upon by CLIENT COMPANY and Consultant.
d. Consultant will transfer network-based information between Consultant and any subcontractor or other third party either:
    i. via a private network between Consultant and the other third party (such as a private circuit or frame relay connection), or
    ii. if sent over the open Internet, via a wholly encrypted communication tunnel (such as LAN to LAN VPN), or
    iii. if sent using FTP, via an encrypted information transfer protocol.
e. Consultant shall utilize secure protocols (such as Secure FTP and Secure Shell (SSH) in place of standard FTP and standard Telnet) to move or transfer CLIENT COMPANY's information over internal networks owned/operated by Consultant, subcontractors or other third parties**.**
f. Consultant, subcontractor, or other third party must use encrypted Email when transmitting confidential, proprietary, or protected information.

8. Backups

a. Consultant shall backup CLIENT COMPANY's information in accordance with a documented backup plan developed by Consultant.
b. For Consultant's utilizing offsite backup facilities (including offsite vaulting services such as Iron Mountain), Consultant shall encrypt all CLIENT COMPANY's information stored on backup media and the encryption key shall be stored separately from the media at all times.

c. All backup media shall be stored in a secured area accessible only by authorized individuals**.**
d. If Consultant maintains their own backup media, they Consultant shall maintain a log of all parties entering/exiting the area where the backup media is kept. Additionally, Consultant shall implement a process and procedure for conducting monthly log reviews for persons entering the area.
e. If Consultant outsources media storage services, then Consultant shall require vaulting service to maintain a log of all parties entering/exiting the area where the backup media is kept.

9. Disposal and Lingering Information

a. Consultant shall immediately remove electronic information from temporary locations controlled by Consultant (such as, but not limited to laptops, workstations, web servers, FTP servers, database servers or test environments) after the information's intended business purpose has passed.
b. Consultant shall remove all of CLIENT COMPANY's electronic information, prior to disposal, utilizing the methods described by the National Institute of Standards and Technology to clear, purge or destroy the storage media. Consultant shall document the disposal of any hardware or media (such as, but not limited to tape drives, thumb drives, diskettes, CD's, DVD's, laptop drives, workstation drives or server drives) storing CLIENT COMPANY's information. At a minimum, documentation should include equipment description, serial numbers, dates of disposal, reason for disposal, method of disposal and individuals performing the disposal.

10. Training

a. Personnel (employees, independent contractors, subcontractors, consultants or other third parties) that handle CLIENT COMPANY's information must complete a security awareness training course prior to accessing any sensitive information supplied by CLIENT COMPANY and periodically (at least once every twelve (12) months) thereafter complete update and refresher security training.
b. Such training must include administrator and end user responsibilities related to the requirements herein, as well as administrative, technical, and physical information security controls.
c. Such training must be documented, including the names and signatures of those individuals who received the training.

11. Wireless (802.11)

a. If Consultant utilizes wireless (802.11) in their environment, and CLIENT COMPANY's information is accessible wirelessly by authorized Consultant Personnel, the following minimum security configuration standard must be implemented:
    i. the broadcast of the network name (SSID) must be disabled,
    ii. strong encryption (WPA2 or the highest standard supported by the wireless infrastructure) must be utilized,
    iii. MAC address filtering must be enabled to limit network access to authorized devices,
    iv. the wireless LAN must be segmented from the wired network utilizing a firewall, and
    v. once wireless access is established, additional authentication of authorized Consultant Personnel must be performed prior to allowing access to wired LAN resources.
b. Consultant desktop or laptop workstations that access, store or process CLIENT COMPANY's information shall not have wireless capabilities configured for automatic connection. Additionally, any built-in wireless technologies such as Intel's Centrino technology must be set for manual connection.
c. Wireless features on Consultant desktops and laptops must be disabled whenever they are connected to Consultant's wired LAN.
d. Consultant will notify CLIENT COMPANY in writing at least 30 days prior to allowing wireless access to or use of CLIENT COMPANY information.

12. Logging and Monitoring

a. In regards to systems accessing, storing or processing CLIENT COMPANY's information, Consultant shall develop logging and log monitoring policies and procedures, and implement an ongoing log analysis process.
b. Consultant shall also develop, implement, and adhere to a log retention policy requiring that system activity and user access logs be kept for a minimum of one year, and logs associated with Security Incidents be kept for six (6) years.

13. Intrusion Prevention and Detection

a. Consultant shall implement a network-based IDS or IPS solution on all network segments containing systems that house CLIENT COMPANY's information.
b. Consultant shall implement a host-based IDS or IPS solution on all hosts accessing, storing or processing CLIENT COMPANY's information.

14. Authentication and Passwords

a. Consultant shall develop, document and adhere to an identity verification process.
b. Consultant shall adhere to the following account password policy for all systems (network devices and hosts) accessing, storing or processing CLIENT COMPANY's information:
    i. requires password complexity where technically possible,
    ii. requires frequent password changes (maximum of every forty-five (45) calendar days between changes),
    iii. requires that a password history be configured to prevent passwords from being reused within the prior twelve (12) months,
    iv. invokes an account lock-out after five (5) consecutive failed attempts, and
    v. requires an administrator or automated challenge response system to verify the user's identity prior to reinstating the account.

15. Infrastructure Architecture

a. Consultant must not store any CLIENT COMPANY information on a device located on a DMZ segment (the data must be stored on an internal segment and accessed by the application layer of the application providing said access).
b. If Consultant makes CLIENT COMPANY information available to public-facing entities (Internet, B2B, etc):
    i. a dedicated switch for DMZ hosts must be utilized (not shared with systems located on other segments),
    ii. the switch must have all ports disabled that are not in use,
    iii. the switch must have port level security enabled to disabled the port when the device is unplugged and also to prevent other systems from being plugged into this port by accident,
    iv. each hosted application component (web, application and database) must reside on its own host system, totally isolated from one another via firewall interfaces (i.e. a separate firewall or separate ports in a single firewall),
    v. port level restrictions (access control lists) must be in place at each firewall interface allowing only required ports inbound/outbound to/from each layer (source/destination IP/ports where possible with all other traffic denied), and
    vi. systems located on the outer most DMZ segment (web layer) must not be permitted to initiate outbound communications to non-trusted networks (Internet, etc.).

16. Patch Management

a. Consultant shall develop, document, and adhere to a patch management process for all aspects of Consultant's environment.
b. Consultant shall apply applicable critical security patches within 72 hours.
c. Consultant shall apply applicable non-critical security patches on at least a quarterly basis.

17. Vulnerability Scanning and Penetration Testing

a. Consultant shall develop, document, and adhere to vulnerability scanning policies and procedures.
b. Consultant shall conduct vulnerability scans on at least a quarterly basis on:
    i. any equipment that stores and/or processes CLIENT COMPANY's information, and
    ii. non-CLIENT COMPANY devices that share common network resources with the equipment described above in 17(b)(i).
c. Within the first year of this agreement, and annually thereafter, Consultant shall engage a third party (approved by CLIENT COMPANY) to conduct penetration testing against Consultant's infrastructure.

18. Web Hosting

a. For hosting arrangements in which CLIENT COMPANY users (including, but not limited to, customers, employees, etc.) access Consultant's website from CLIENT COMPANYL.com, Consultant will redirect that user to CLIENT COMPANYL.com upon completion or log-off of Consultant's site.

b. Consultant agrees to implement a one-way (CLIENT COMPANY to Consultant single sign-on interface within 12 months of CLIENT COMPANY request at no additional fee to CLIENT COMPANY. Consultant agrees to comply with one of two implementation standards for single-sign-on provided to Consultant by CLIENT COMPANY.

c. Consultant agrees to redirect any CLIENT COMPANY user to the CLIENT COMPANYL.com website for logon or site registration rather than allowing such logon or registration directly on Consultant's website.

d. Consultant will scan all Internet-facing applications that access CLIENT COMPANY information prior to production implementation to verify that all applicable Open Web Application Security Project (OWASP) Top 10 and SANS Top 20 vulnerabilities have been prevented.

e. CLIENT COMPANY may scan Consultant's Internet-facing applications, without notice to Consultant. Consultant agrees to remediate any OWASP Top 10 or SANS Top 20 vulnerabilities found as a result of these scans within 48 hours of notification from CLIENT COMPANY. Should CLIENT COMPANY identify what it, in its sole discretion, deems a serious exposure, Consultant will inactivate the Internet site until the exposure is removed.

19. Software

a. All Consultant Personnel shall be prohibited from installing personal or downloaded software (or any software not pre-approved in writing by Consultant management) on any hardware that may access CLIENT COMPANY's information.

b. Consultant shall not implement keystroke monitoring software/hardware on systems processing and/or storing CLIENT COMPANY's information.

20. PC and Host Configuration Controls

a. Consultant shall implement Automatic Lockup as follows:
   i. electronic sessions on any hardware (i.e., laptops, workstations, PDAs, servers, etc.) that access, store, or process CLIENT COMPANY information shall lock the screen and/or console after thirty (30) minutes of inactivity and require the user to re-authenticate, and
   ii. Consultant shall require a valid logon (i.e., user ID and password) to re-authenticate and gain access to a locked device.

b. Consultant shall implement Virus Protection as follows:
   i. All hardware used to conduct business for CLIENT COMPANY has current antivirus software protection installed, and
   ii. All hardware used to conduct business for CLIENT COMPANY has up-to-date virus definitions.

c. For the purpose of this agreement, "up-to-date" means that virus definition updates occur at least once per day in order to obtain and apply the latest virus signature files.

21. Portable Media

a. Consultant shall limit the use of portable media (such as, but not limited to, USB Drives, mp3 players, CD's, ZIP drives, Laptops, PDA's, cameras, camera phones) by Consultant or Consultant Personnel to only media owned/supplied by Consultant.

b. Consultant Personnel shall not connect personally owned portable media to any hardware that is used to conduct business for or on behalf of CLIENT COMPANY.

c. Consultant shall encrypt, using a corporate solution, any and all portable media used for storage of CLIENT COMPANY's information. The encryption software used must encrypt the entire device (all partitions) and must not allow the option of individual folder and/or file level encryption.

d. Any and all portable media used for storage of CLIENT COMPANY's information must be transported as carry-on (hand) baggage when using public transportation and must be concealed and/or locked when in an unattended private vehicle (e.g. locked in the trunk of an automobile).

22. Remote Access

a. Remote access to Consultant's internal network:
    i. For all remote access to Consultant's internal network for any reason, traffic with the remote device must be encrypted and the remote user must utilize strong authentication (Authentication and Password requirements listed in item Fourteen (14) above apply).
    ii. Remote access to or use of CLIENT COMPANY information may not occur from a public location (e.g., airports, coffee shops, etc.).
b. Remote access to CLIENT COMPANY's network:
    i. Consultant understands and agrees that remote users can only connect to CLIENT COMPANY Citrix MetaFrame XP servers over TCP/IP only on the Internet. Terminal Services in Windows® does not support remote connections over IPX/SPX, NetBIOS, or any other asynchronous transports.
    ii. Consultant Personnel will not access the CLIENT COMPANY network from public spaces in which unauthorized persons are present (including, but not limited to, airports, coffee shops, etc.).
    iii. Consultant agrees that users will maintain an active connection only for the required time and purpose and will disconnect when the user is no longer has this requirement. Consultant is responsible for all activity that occurs during the connected session.
    iv. Consultant agrees to maintain the integrity of the data by not storing data in other than the designated user directory assigned to their CLIENT COMPANY account (H\: Drive) and only within the BCBCF network. This is the only drive where Consultant Personnel will store data.
    v. Consultant Personnel will not print, download, email, or otherwise copy CLIENT COMPANY information to destinations outside of the CLIENT COMPANY network. Destinations outside the CLIENT COMPANY network include, but are not limited to, personal email accounts, non-CLIENT COMPANY owned devices including printers, computers, personal digital assistants, cell phones, portable storage devices, etc.
    vi. Consultant will comply with CLIENT COMPANY's Consultant FOB Request Information Standard Operating Procedure, which defines procedures for requesting, using, controlling and deleting access to the CLIENT COMPANY network.

23. Physical Security Plan

a. Consultant shall limit physical access to work areas and to systems that may access, contain or process CLIENT COMPANY's information to only those Consultant Personnel that have a business need for such access.
b. At no time will CLIENT COMPANY dedicated personnel perform the Services work on behalf of CLIENT COMPANY within the general population of the processing center.
c. Consultant shall document all physical security controls at least annually, or following moves or building additions, and shall supply said documentation to CLIENT COMPANY for review, upon CLIENT COMPANY's request, or prior to such move or building addition.
d. Consultant shall include the following physical security controls in locations where CLIENT COMPANY information is stored and/or accessed:
    i. Electronically controlled access, restricting access to only those with a business need,
    ii. Provide a segregated, enclosed workspace, separate from other businesses, without windows,
    iii. Establish a clean desk policy for staff, with no phones, paper, purses or cases,
    iv. Cameras, with recording capability, at all entrances.

24. Security Incidents

a. Consultant shall report any Security Incident involving the confidentiality of information, including, without limitation, customer facing outages, loss of information, degradation of information integrity, identity theft, compromise of user account(s) or password(s), or virus outbreaks experienced by Consultant within five (5) business days of such Security Incident, or sooner if reasonably necessary given the circumstances.
b. *Should Consultant have a* malicious code *infection* spreading via a worm mechanism, *Consultant* shall report the *incident* to CLIENT COMPANY immediately upon discovering the outbreak.

25. Background Checks

a. Consultant shall conduct complete background checks on all Personnel (including, but not limited to, independent contractors, subcontractors or consultants) prior to allowing said Personnel access to perform work for or on behalf of CLIENT COMPANY.
b. As part of the background check, Consultant shall include Federal, state and local criminal history checks.
c. Consultant will provide to CLIENT COMPANY confirmation that the required background checks have been completed and that no personnel with criminal histories are assigned to perform CLIENT COMPANY work.

26. Business Continuity

a. Consultant shall have business continuity plans in place to ensure that the goods and/or services contracted for by BCSBF will be delivered in accordance with schedules agreed to by both parties. These plans should address the performance failure of a Consultant's subcontractors.
b. Consultant shall follow a process that results in the development of plans for the prevention, mitigation, emergency operations/response, business continuity and recovery as specified in NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs.
c. Consultant is subject to and shall comply with an annual Consultant Business Continuity Assessment, at which time, a summary of the current-state Business Continuity program will be made be available upon request. CLIENT COMPANY has the right to make additional inquiries regarding Consultant's Business Continuity program. Plans shall be subject to regular maintenance throughout the currency of the contract.

27. Cyber Insurance

a. In addition to maintaining the insurance required in the Master Services Agreement, Consultant will maintain Cyber & Privacy Liability Insurance in a form acceptable to CLIENT COMPANY in an amount not less than $5,000,000 per claim and aggregate. Such insurance will be endorsed to include CLIENT COMPANY (including its subsidiaries) as an additional insured.

28. Right to Audit

a. CLIENT COMPANY retains the right to audit, with prior notice, Consultant's information security controls, CLIENT COMPANY information, or status of third party certification.

29. Annual Compliance Attestation

a. Upon CLIENT COMPANY request, but no more than annually, Consultant shall complete and sign an Annual Compliance Attestation Form attesting to compliance with the items in the Exhibit, and return the Form to CLIENT COMPANY.