Schedule [#] - Information Security Requirements

Contractor agrees to maximize the security of its people, processes, and technologies throughout the term of this Agreement in accordance with the requirements set forth in this Schedule and all applicable laws (collectively, the "IS Requirements"). Company reserves the right to validate the effectiveness of the IS Requirements or Contractor shall provide evidence of third party independent validation, upon request by Company. Company shall be permitted to amend the IS Requirements upon written notification to Contractor. The term "product" as used herein means any service, equipment or software furnished by Contractor to Company hereunder.

1.0 Access Controls. Contractor will provide role-based access, authorization, and accountability controls within their product which conform to the guidelines and requirements set forth in the IS Requirements. Controls must be appropriate for the sensitivity of the information. In addition, the product will provide for separate roles for day to day users, administrators, developers, and support staff, and that the access shall provide access to authorized personnel only who have been properly trained on administrative responsibilities and security process and procedures. Access Control shall provide the minimum access required for each role and deny access for unauthorized users. Contractor's hosted products, if any, will include controls for securing service accounts and generic accounts and prevent their unauthorized modification or use. Service account and generic account passwords must be changed at least annually. Contractor shall verify and disclose all known methods for accessing the products, and shall not access or allow others to access products without Company's consent (other than hosted products, and even then only Contractor and its permitted subcontractors may access hosted products without such consent). Contractor further warrants that administrators for the hosted product production environment will utilize two-factor authentication when providing remote administrative support for the environment

2.0 Shared Architecture. Contractor agrees to identify where shared resources are utilized within its architecture by other clients and the security controls implemented to protect Company data from access by unauthorized users and third parties. If this Agreement contemplates a dedicated environment, such environment shall not contain shared resources including, but not limited to, all components, systems, and infrastructure.

3.0 Incident Response and Breach Notification. Contractor agrees that any breach or any other security incident, internal or external that has the potential to compromise multiple data sources must be reported to the [Company Name] Security Operations Center [email, phone number)] within 24 hours of knowledge of the breach followed by a plan for remediation within 72 hours remediation, and 2 business weeks from the initial notification for completion of the investigation.

4.0 Encryption. Where this Agreement provides for encryption, or if Company determines that encryption is acceptable to prevent unauthorized disclosure of Company information, in order to protect Company sensitive information, Contractor's product(s) will use cryptographic controls that satisfy the requirements of FIPS 197 such that Company's sensitive data and information is rendered inaccessible by an unauthorized user. Where Contractor's product uses encryption keys, Contractor's product will not store hard-coded encryption keys within source code. Encryption keys will be stored and secured separately from the product while in transit and while at rest and will be revocable for re-implementation and maintenance.

5.0 Password and Logon Standards. Contractor's product(s) will provide a unique ID (individually identifiable) for user accounts. Where individual accountability cannot be achieved for access to sensitive systems, multi-factor authentication must be employed. Contractor's product(s) will provide for password complexity which conforms with the following parameters: user accounts require a minimum of 8 characters, a combination of upper and lower case letters, numbers, and special characters, 90 days password aging, and 10 previous passwords history. Administrator accounts require a minimum of 10 characters, a combination of upper and lower case letters, numbers and special characters, 90 days password aging, and 10 previous passwords history. Logon credentials and passwords will be protected by transport encryption that meets the minimum encryption requirements of Section 4.0.

6.0 Data Security. Contractor certifies that their product provides the necessary security to meet all applicable laws and regulatory requirements for storing, processing, and transmitting data. This specifically includes, but is not limited to, all laws and regulations that require specific protections for personally identifiable information, credit card and financial information, and audit records. Contractor agrees to allow Company-designated third party validation of compliance with all legal and regulatory requirements.

7.0 Logging and Errors Details. Contractor agrees to log all product and application usage, access, misuse, and sufficient detailed error messages for monitoring and analyzing the use of the products, and will retain all information for a minimum of ninety (90) days from the log date. Contractor further agrees that the product includes an audit trail, time stamped log entries, and unique log identification with attribution. Company has the right to request logs at any time and at no cost to Company.

8.0 Operational Support. Contractor will perform background checks that include a 7 year criminal history, social security verification, drug screen, and credit history for personnel that support the hosted products (if any) prior to beginning work with Company and on an ongoing basis, at no cost to Company.

9.0 Vulnerabilities and Defects. Contractor agrees to maintain a vulnerability and defect tracking process which reviews potential defects for their security impact to Contractor's product(s) and the components and software packages that support it at no cost to Company. Contractor further agrees, at Contractor's expense, to test and remediate for all publicly disclosed software vulnerabilities posted to the National Vulnerability Database (http://nvd.nist.gov/) and by Open Web Application Security Project (www.owasp.org) within thirty (30) days of being posted. Generally, this will prevent the product from being easily susceptible to cross-site scripting, SQL injection, buffer overflows, input validation, and other similar attacks. Contractor further warrants that the product shall not contain any code that may facilitate unexpected or unapproved access or outages to the product, including, but not limited to: computer viruses, worms, time bombs, backdoors, trojan horses, easter eggs, and other forms of malicious code, and agrees to provide documentation detailing such processes upon request by Company and at no cost to Company

10.0 Security Assessments and Testing. Contractor agrees that it will engage an independent third party, to be agreed upon by both Contractor and Company, at Contractor's expense, to test the product for vulnerabilities through a detailed security test on an annual basis or Contractor may elect to certify to an accepted Industry Standard, to be approved by Company. If Contractor elects an annual security test, such test will include all security controls which support the product, its production hosting environment, and operational support infrastructure. Contractor shall require such third party to provide a report detailing the results of the test and Contractor shall provide Company a copy of such report within thirty (30) days of the test. In the event such report shows vulnerabilities in the product, Contractor shall promptly provide Company with a proposed remediation plan and timeline for completion all at no cost to Company. All product vulnerabilities, defects, or bugs disclosed to Contractor shall be corrected and remediated by Contractor, at Contractor's expense, within thirty (30) days from the date of such report.

11.0 Right to Report. Company and Contractor have the right to report to public vulnerability reporting organizations regarding any defects or configuration conditions which result in vulnerabilities to information handled by the deliverable, the deliverable itself, or other hardware, software or systems that would put Company or Company's interests at risk.

12.0 Destruction. Contractor agrees that when the lesser of (a) its own applicable data retention period or (b) any applicable data retention period specified in this Agreement has been exceeded, the data is no longer required, or at the request of Company, Contractor will destroy the data in a manner that will render it completely unusable and unrecoverable, and will provide Company with a certificate of destruction, upon Company's request.

13.0 Formal Documentation. Contractor agrees to provide formal documentation for the use, maintenance and secure implementation of Contractor's product. Product documentation will be updated within thirty (30) days of a product update, upgrade, patch, or similar change. Product documentation will include, but not be

limited to, an inventory of all components, a listing of all system accounts (i.e. generic and/or default), configurations, and dependencies. Contractor shall disclose in writing all known methods for administering the product including, but not limited to, any undocumented user accounts and all commands, configurations and operations used to manage the product.

14.0 Conflicts. Nothing contained herein shall be construed to limit any of Contractor's obligations contained elsewhere in this Agreement, including, without limitation, in the terms and conditions contained in the main body hereof.