HURON

HURON SUPPLIER INFORMATION SECURITY REQUIREMENTS ADDENDUM

This Huron Supplier Information Security Requirements Addendum is incorporated into and made a part of the Agreement between Company and Contractor. These Huron Supplier Information Security Requirements list the security controls that Huron's Suppliers are required to adopt when Supplier is doing any of the following: (a) accessing Huron or Huron client or customer facilities, networks and/or information systems, (b) handling Huron or Huron client Confidential Information, including related Personal Data, Personal Information, and Protected Health Information ("PHI") or (c) having custody of Huron hardware assets.
Any of the above activities alone or together are considered to be within the scope of the Requirements. Additional security compliance requirements may be specified by Huron in Supplier's agreement or individual statements of work. The Requirements are in addition to any specific terms and restrictions related to the handling and processing of Personal Data, Personal Information, or PHI on behalf of Huron and its clients, which will be set forth in a separate data processing agreement and/or Business Associate Agreement, as necessary.

Supplier shall for the entire term of the Agreement, and for as long as Supplier falls within the scope of the Requirements, strictly adhere to the Requirements, and not change its security policies or practices in any way which may have the effect of weakening the security protections afforded to Huron or Huron Data.

Supplier is responsible for compliance with the Requirements, including ensuring that all Supplier individuals and entities are bound by contractual terms consistent with the Requirements.

Definitions

Capitalized terms used but not defined in this Huron Supplier Information Security Requirements Addendum will have the meanings set forth in the Agreement.

"Affiliate(s)" will mean any entity under control of, controlling, or under common control with a party to this Agreement.

"Agreement" means any underlying agreement(s) including any master services agreement, statements of work, project arrangement letters, engagement letters, or any other written agreement between Huron and Supplier.

"Huron" means Huron Consulting Group Inc. and all of its controlled subsidiaries and affiliates.

"Huron Data" means Huron or Huron client Confidential Information (as defined in the Agreement), including related Personal Data, Personal Information, and Protected Health Information ("PHI") (as such terms are defined by applicable law).

"Huron Supplier Information Security Requirements" or **"Requirements"** means this Addendum.

"Security Incident" means any security incident or data breach, as such or similar terms are defined by applicable law which relates to Huron Data or the product or services Supplier provides to Huron, which shall include but not be limited to any occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of Supplier's security policies, security procedures, or acceptable use policies.

"Supplier" means Supplier and all of its Affiliates, employees, agents, contractors, and subcontractors.

1. Compliance with Applicable Law

1.1 Supplier will comply with all of its obligations under privacy, security, and breach notification laws, as well as all regulations and guidance issued by competent supervisory or regulatory authorities, applicable to Supplier's provision of services under the Agreement, including those laws which are directly applicable to Supplier's business or the services Supplier provides.

1.1.1 For the avoidance of doubt, Supplier agrees to comply with all U.S. federal and state privacy, security, and breach notification laws of general applicability (e.g., Massachusetts 201 CMR 17.00 et seq., and the California Consumer Privacy Act ("CCPA")), which are directly applicable to Huron based on Huron's operations throughout the U.S.

1.1.2 Supplier agrees to comply with all applicable privacy, security, and breach notification laws outside of the U.S. where Huron is established and operates (currently, Canada, India, the United Kingdom, Singapore, and Switzerland) when performing services for Huron that are known by Supplier or reasonably should be known to Supplier to entail Huron's non-U.S. operations or clients.

1.1.3 If pursuant to the terms of the Agreement, Supplier is acting as a direct subcontractor or subprocessor to Huron on behalf of Huron's client(s) which are themselves located outside of the U.S. or the countries where Huron operates as described in Sections 1.1.1 and 1.1.2, and Huron provides notice to Supplier with regard to serving such Huron client(s) in specific additional third countries, then Supplier agrees to comply with all laws then applicable to the services; or to notify Huron in writing, prior to agreeing to perform the services, that Supplier will be unable to comply with applicable local law.

1.2 Adherence to Data Protection by Design and Default and the European Union General Data Protection Regulation ("GDPR") Security Principles. Supplier shall adopt internal policies and implement measures which meet in particular the industry standard principles of data protection by design and data protection by default, as a best practice and based on Huron's presence and operations in Europe, regardless of whether services are to be provided in the European Union. Supplier shall specifically, at all times, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including *inter alia as appropriate*: (a) the pseudonymization and encryption of Personal Data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

1.2.1 In assessing the appropriate level of security, Supplier shall take account in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Persona Data transmitted, stored or otherwise processed.

1.2.2 Supplier shall take steps to ensure that any natural person acting under its authority who has access to Personal Data does not process it except on instructions from Huron unless he or she is required to do so by applicable law.

2. Adherence to Industry Standards

2.1 Supplier has obtained one or more of the following industry recognized certifications from an independent and authorized third party auditor or certification body, provided a copy of such in Annex A below, and will continue to maintain its systems so as to be able to, at all times, meet the requirements of such certification(s):

2.1.1 Certification to one or more International Organization for Standardization ("ISO") standards which are service-line or sector-specific (e.g., ISO 27017, 27018, 27019, 27799)

2.1.2 ISO 27001

2.1.3 STAR/CLOUD Security Alliance

2.1.4 SyTrust or Webtrust engagement

2.1.5 Health Information Trust Alliance ("HITRUST") Cybersecurity Framework ("CSF") certification

2.1.6 Asia-Pacific Economic Cooperation ("APEC") Privacy Recognition for Processors ("PRP") certification

2.1.7 Federal Risk and Authorization Management Program ("FedRAMP")

2.1.8 Another appropriate industry recognized and standard information security management certification which consists of appropriate technical and organizational measures to ensure protection of Huron Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure, or access.

2.2 If Supplier does not hold a valid and current industry recognized certification as referenced in Section 2.1, Supplier represents, warrants, and covenants that it is either (a) in the active process of attaining such certification(s) with an independent and authorized third party auditor or certification body, or (b) that its information security program takes into consideration or is based on one or more of the following industry recognized and standard frameworks (as such are amended, superseded, or replaced from time to time), and it meets the Requirements (including but not limited to the Information Security Management System ("ISMS") requirements found in Section 7 et seq.) and Supplier will continue to maintain its information security program and information security systems so as to be able to, at all times, strictly adhere to such controls. If Supplier does not hold a current certification as described in Section 2.1, Supplier

© 2016 Huron Consulting Group Inc. and affiliates. All Rights Reserved. Proprietary and Confidential.

must provide a summary (which includes, but is not limited to, an overview of its written information security policies, penetration test results for the systems in scope performed by a third-party, and management of critical incidents) of its ISMS program in Annex A below.

2.2.1 National Institute of Standards and Technology ("NIST") SP 800-53

2.2.2 NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.1

2.2.3 Center for Information Security ("CIS") Controls v7.1

2.2.4 Information Systems Audit and Control Association ("ISACA") Control Objectives for Information and Related Technologies ("COBIT")

2.3 If services provided to Huron by Supplier pursuant to the terms of the Agreement involve the processing of payment card information, Supplier will maintain compliance with the then current version of the Data Security Standards ("DSS") which applies to Supplier's activities from the Payment Card Industry Security Standards Council ("PCI SSC") for the duration of the services provided to Huron. On written request, Supplier will provide Huron with the most recent PCI SSC "Attestation of Compliance" reports prepared by a third-party PCI Qualified Security Assessor for both Supplier's systems and for any third parties used by the Supplier for handling payment card data on behalf of Huron.

3. Adherence to Huron Policies

3.1 In addition to any general terms in the Agreement, Supplier shall comply with all Huron work rules, policies, and standards as the same are communicated to Supplier in writing from time to time, including those rules, policies, and standards of Huron relating to security of and access to Huron Data, facilities, telephone systems, electronic mail systems, and computer systems. Huron shall notify Supplier of any material change in Huron work rules, policies and standards that affect Supplier.

4. Annual Audit Reports

4.1 Subject to the exception found in Section 4.2, during each calendar year in which Supplier provides services to Huron under the Agreement, Supplier will, at Supplier's cost, cause to be conducted a Statement on Standards for Attestation Engagements ("SSAE") 18 (Reporting on Controls at a Service Organization) (as amended, superseded, or replaced from time to time)) SOC 1, Type 2 audit and an AT 101 (Attest Engagements (as may be modified from time to time), issued by the American Institute of Certified Public Accountants ("AICPA")) SOC 2, Type 2 audit for the Supplier service location and Supplier Business Continuity Planning ("BCP") site by an independent public accounting firm; or other rigorous third party independent assessment of the Supplier's security safeguards relevant to the processing of Huron Data or services provided to Huron.

4.1.1 Supplier will upon written request provide Huron with a summary of the resulting reports so long as they pertain to Supplier's services to Huron. Supplier will comply with future applicable guidance relating to SSAE 18 and AT 101 as issued by the AICPA or competent regulatory authority.

4.1.2 Supplier shall promptly remediate any material weakness or deficiency revealed by any such audit. Huron and its external auditors will be provided summaries of relevant reports (pertaining directly to the services provided to Huron) relating to Supplier's remediation of material weaknesses or deficiencies, as soon as reasonably possible after the conclusion of each such audit. Huron shall have the right, as reasonably appropriate, to provide a copy of such reports to any competent regulators subject to confidentiality provisions as restrictive as those herein. At Huron's written request, Supplier shall confirm in writing that there have been no changes to the relevant policies, procedures and internal controls since the completion of any such audit or, as applicable, that material weaknesses or deficiencies have been remediated.

4.2 If Supplier does not have a current audit report, Supplier represents, warrants and covenants that it presently meets, and will continue to meet for the entire term of the Agreement, the requirements in Section 2.2.

5. Security Incident Notification

5.1 Supplier must report any Security Incident of which it becomes aware without undue delay (but at the latest within one (1) business day) to Supplier's business contacts at Huron for the applicable services impacted by the Security Incident, and additionally by sending an e-mail to securityincident@hcg.com.

5.1.1 The notification shall at least include, to the extent known at the time (and updated as necessary without undue further delay):

5.1.1.1 A brief description of the nature of the Security Incident,

© 2016 Huron Consulting Group Inc. and affiliates. All Rights Reserved. Proprietary and Confidential.

5.1.1.2 A description of the types of information that were involved in the Security Incident,

5.1.1.3 Whether Personal Data, Personal Information, or PHI were potentially compromised in the Security Incident, and if so, the categories and approximate number of affected individuals and approximate number of records concerned,

5.1.1.4 The steps affected individuals (to the extent there are affected individuals) should take to protect themselves from potential harm,

5.1.1.5 A brief description of what the Supplier is doing to investigate the Security Incident, mitigate the harm or possible adverse effects, and prevent further Security Incidents, and

5.1.1.6 Name, title, phone number, and email address for Supplier's point of contact responsible for follow-up and coordination with Huron with regard to the Security Incident.

6. Audits and Questionnaires

6.1 Supplier shall make available to Huron all information necessary to demonstrate adherence to the obligations set forth in the Requirements and compliance with applicable privacy, security, and breach notification laws related to Supplier's services under the Agreement, and allow for and contribute to audits, including inspections, conducted by Huron or an independent auditor on Huron's behalf (subject to confidentiality terms). Huron retains the right at any time to collect all additional information, evidence, and assurances from Supplier that Huron deems necessary, including through the use of security questionnaires and/or audits.

6.1.1 Not more than once per calendar year and with at least thirty (30) days' written notice (unless preceded by a Security Incident), Huron may send to Supplier a security questionnaire. Supplier shall promptly respond to such security questionnaire with the required information.

6.1.2 Not more than once per calendar year and with at least thirty (30) days' written notice (unless preceded by a Security Incident), Huron may audit and inspect Supplier's information systems and facilities used to host/process Huron Data, as well as Supplier's non-automated policies, systems, and means related to the hosting/processing of Huron Data (i.e. hardcopy filing systems).

7. Maintenance of an ISMS that Protects the Confidentiality, Integrity, and Availability of Huron Data

7.1 Supplier shall at all times maintain a commercially reasonable ISMS that:

7.1.1 Includes administrative, technical and physical safeguards that shall ensure the protection of confidentiality, integrity, and availability of information throughout the data lifecycle;

7.1.2 Incorporates accountability and assurance;

7.1.3 Follows industry best practices, including through the utilization of a certification program and/or framework referenced in Section 2;

7.1.4 Includes the development, implementation, maintenance, enforcement, and audit of a written information privacy and security program that at a minimum includes:

7.1.4.1 A requirement that Supplier comply, in all material respects, with all applicable laws,

7.1.4.2 A requirement that all confidential and personal information shall only be transmitted in an encrypted format and that access to confidential or personal information shall be restricted to those individuals with a need to access such information, with access to such data granted by secure username and password only,

7.1.4.3 A plan to assess and manage system failures,

7.1.4.4 A regular assessment of data security risks, with adjustments made to the information privacy and security program to reduce such risks, and

7.1.4.5 Notice and incident response procedures.

8. Data Transmission

8.1 File Transmission and Encryption. Electronic transfer of files containing Huron Data must meet the following conditions:

8.1.1 Exchanges must use a current industry standard encryption protocol;

HURON

© 2016 Huron Consulting Group Inc. and affiliates. All Rights Reserved. Proprietary and Confidential.

8.1.2 Exchanges over public networks shall take place over a current industry standard encrypted communication channel;

8.1.3 User IDs and passwords must be protected from disclosure using current industry standard, or better, security protocols (e.g., TLS or SSH) during authentication;

8.1.4 When delivered to externally facing or shared file transfer servers, transfers must also have the data encrypted using current industry standard, or better, security protocols (e.g., SFTP & PGP encryption) during transmission and while at rest on such servers;

8.1.5 Files must be removed from externally-facing or shared file transfer servers after successful receipt; and

8.1.6 Decryption of encrypted files shall occur on secure systems with restricted access located behind a firewall.

8.2 Email. Any email communications between Supplier and Huron shall use current industry standard, or better, security protocols (e.g., enforced transport layer security (TLS)).

9. Networks

9.1 Encryption in Transit. Huron Data shall be encrypted when transmitted over any network.

9.2 IP Filtering. Supplier shall only allow authorized access (e.g., allow list) to its computing infrastructure from Huron provided IP addresses.

9.3 Monitoring and Logging. Supplier shall monitor systems/networks to detect potential cybersecurity events and Security Incidents and shall retain and review event logs on a regular basis or upon notification of any suspicious activities.

10. Data Storage

10.1 Data at Rest. All Huron Data must be encrypted at rest.

10.2 Backups. Backups containing Huron Data must be encrypted.

10.3 Portable Devices and Removable Media. Huron Data shall not be stored unencrypted on any removable media or portable device (e.g., laptop, smart phone, or tablet). In the event that Supplier requires the use of Huron Data on such devices, the Supplier shall disclose the purpose of such use to Huron in advance and in writing to Huron's information security department and ensure the following requirements are satisfied:

10.3.1 Supplier shall have policies, procedures, and controls requiring appropriate use of storage encryption solutions;

10.3.2 Supplier shall ensure that end user devices are secured and maintained properly to reduce the risk of compromise or misuse. This includes securing device operating systems, applications, and communications (e.g., encrypting wired and wireless network traffic); and

10.3.3 Supplier shall make all members of Supplier's workforce (including employees, agents, contractors, and subcontractors) aware of their responsibilities for storage encryption, such as encrypting sensitive files, physically protecting mobile devices and removable media, and promptly reporting loss or theft of devices and media.

10.4 Disposal of Files, Media, or Products Containing Huron Data. When Supplier is required to destroy files, media, or other materials containing Huron Data pursuant to the Agreement, such destruction shall be performed in the following manner:

10.4.1 Magnetic Media. Magnetic media such as tapes, diskettes, hard drives, shall be securely sanitized of all information in accordance with the then current version of the requirements of the NIST Special Publication 800-88 ("NIST SP800-88") such that the data is no longer reasonably retrievable from the media. Degaussing and overwriting are acceptable methods of purging information from magnetic media.

10.4.2 Non-magnetic media. Non-magnetic media such as hard copies, CDs or DVDs shall be physically destroyed in accordance with the then current version of the requirements of NIST SP800-88 such that the data is no longer reasonably retrievable from the media. Acceptable methods of physical destruction include shredding, burning and disintegration. If Supplier uses a shredder, Company may not use a strip shredder, and shall use a cross-cut shredder or higher technology rated P-5 or above under DIN 66399.

© 2016 Huron Consulting Group Inc. and affiliates. All Rights Reserved. Proprietary and Confidential.

10.4.3 Documentation regarding disposition of Huron Data. Supplier shall maintain records sufficient to document the disposition of all Huron Data in its possession. Documentation shall include a description of the information and medium, the date and method, and party responsible.

11. Hosting

11.1 Data Segregation. Supplier shall ensure that Huron Data is segregated, either physically or logically, from any other Supplier and Supplier's customer/client data.

11.2 Location of Hosting. Huron Data shall at all times be hosted and processed on Supplier's servers and other computers that are physically located in the U.S. or other locations as authorized in writing by Huron, and subject to all data transfer restrictions in applicable law.

11.3 Huron Access. Huron shall at all times have free and unfettered access to Huron Data.

11.4 Physical Security. Supplier shall ensure adequate and commercially reasonable physical security controls for all premises where Huron Data is processed.

12. Data Analytics

12.1 Supplier shall not use any Huron Data for testing or data analytics purposes (other than those which are a necessary part of the services under the Agreement) without the prior written consent of Huron. Supplier is at all times prohibited from using any Huron Data in a way that would be create the appearance of a "sale" of Personal Information as defined by the CCPA.

13. Access Controls

13.1 Least Privilege. Supplier shall have documented policies and procedures to limit and review access to Huron Data to those persons who have a business need to access it.

13.2 Credentials. Supplier shall have policies, procedures, and controls requiring appropriate use of access credentials (e.g., user IDs and passwords) to prevent unauthorized access to or use of such credentials and ensure that each user credential is only used by one authorized individual (e.g., a single user ID shared by multiple users is not permitted). Access right levels and access credential shall be reviewed periodically and adjusted as necessary, (such review period must meet or exceed industry best practices). Supplier shall immediately terminate credentials of individuals associated with Supplier who no longer have authorized access (such as terminated or reassigned employees).

13.3 Multifactor Authentication. Supplier's written policies and procedures for access controls shall include use of multifactor authentication for any individual accessing the Supplier's internal network from an external network.

14. Patching and Anti-Virus

14.1 All workstations, servers and other systems that process, store and/or have access to Huron Data or access directly Huron or Huron client or customer networks and/or information systems must have supported security agent software, which includes malware and anti-virus software solutions with automated mechanisms to ensure up-to-date software and definitions. Supplier shall remain up-to-date on available patches created to correct known software security vulnerabilities and shall promptly apply patches to computer systems after testing, as applicable.

14.2 Supplier will maintain a vulnerability assessment and remediation program to identify systems in need of patching.

15. Training and Awareness

15.1 All Supplier employees, agents, and relevant contractors and subcontractors shall upon onboarding/hire, and at least annually thereafter, be trained on Supplier's information security policies, proper use of computer security systems, and the importance of securing sensitive data. All Supplier employees, agents, contractors, and subcontractors who perform services for or on behalf of Huron must also be trained on the Requirements and the relevant responsibilities thereunder.

16. Applicability and Incorporation

16.1 The Requirements are incorporated into and form an integral part of the Agreement by the parties hereto, regardless of how the Agreement has been formed. The Requirements supersede any and all prior agreements or understandings between Huron and Supplier with regard to the subject matter of the Requirements, and may be cancelled, modified, or amended only by a written supplement to the Agreement or Requirements signed by both parties.

HURON

© 2016 Huron Consulting Group Inc. and affiliates. All Rights Reserved. Proprietary and Confidential.

Annex A

Supplier Certificate or Summary of Supplier ISMS Program

NOTICE TO SUPPLIER: You are required to add to this Annex a copy of **your current ISO or other relevant certificate** (from the list found in Section 2.1 above).

If you do not have a current certification as described in Section 2.1, you must provide below **an executive summary of your ISMS program** which includes but is not limited to, an overview of your written information security policies, penetration test results, and management of critical incidents.

© 2016 Huron Consulting Group Inc. and affiliates. All Rights Reserved. Proprietary and Confidential.