

SECURITY ADDENDUM

Section 1. Definitions:

“City’s Information” or “City Information” means any and all City information or data, including but not limited to, City-specific information, user information, data, materials, processes, documents, citizen information, and any other information, materials, or data Vendor receives or to which Vendor has access to, in any form whatsoever including oral, written, and machine-readable form, video, audio, phonorecord, recorded media, drawings, schematics, samples, devices, software, formulas, services, processes, procedures, protocols, trade secrets, intellectual property, and business or strategic plans.

“Incident” means as defined in Section 4.1 of this Security Addendum.

“Mitigate” means deployment of security controls as necessary to reduce the adverse effects of threats and reduce risk exposure to a level reasonably acceptable by City.

“Remediation” or “Remediate” means, as applicable, that Vendor has completely resolved a security exposure or Incident, such that the vulnerability no longer poses a risk to City Information, Vendor systems in which City Information is stored or transferred through, and City systems.

Section 2. Vendor’s General Obligations and Responsibilities:

2.1 Vendor shall maintain the security of all City Information, including but not limited to, all City-specific data, user data, citizen data, and any other data that is provided to or made accessible to Vendor by City, by any user, by any citizen, or that Vendor generates, creates, compiles, or analyzes for the City, as further described below and in this Agreement. Vendor shall regularly test and audit the systems, controls, and procedures outlined in this Agreement, which tests and audits shall occur at least once per calendar month. Vendor shall implement and maintain, at least at industry standards, administrative, technical, and physical controls, safeguards, measures, and procedures to (i) protect and safeguard the privacy, security, integrity, and confidentiality of the City’s Information, (ii) prevent, detect, contain, and correct security breaches in, involving, or against the City’s Information, and (iii) ensure that the City’s Information is not accessed, processed, stored, transmitted, transferred, copied, disposed of, archived, or disclosed contrary to the provisions of this Agreement or applicable laws concerning information technology security, network or data security, and privacy laws. At a minimum, Vendor shall develop, implement, and maintain a reasonable written security program that includes appropriate administrative, technical, organizational, and physical safeguards and security measures that: (i) maintain user identification and access controls designed to limit access to authorized users; (ii) protect the City’s Information from unauthorized activity; (iii) use encryption technology, and (iv) comply with any specifications as requested by the City.

2.2 Vendor shall be responsible and liable for the acts and omissions of Vendor’s personnel, temporary employees, agents, contractors, representatives, counsel, and subcontractors in connection with the provision of the services required under this Agreement, as if such acts or omissions were Vendor’s acts or omissions. With respect to any of Vendor’s personnel, temporary employees, agents, contractors, representatives, counsel, and subcontractors who process, store, transmit, access, dispose of, or have access to the City’s Information or the Software in so far as it

relates to or is the result of Vendor's performance of this Agreement, Vendor shall: (i) Advise these persons of and require that they comply with the provisions of this Agreement, which includes this Security Addendum, applicable to each person, including without limitation, the provisions relating to the privacy, security, integrity, and confidentiality of the City's Information; (ii) Require these persons to execute and deliver to Vendor written agreements that are a direct flow-down of, or substantially similar to (or no less restrictive than) the terms of this Agreement, including this Security Addendum, and including without limitation, with respect to privacy, security, integrity, and confidentiality of the City's Information; and (iii) With respect to Vendor's personnel, temporary employees, agents, contractors, representatives, counsel, and subcontractors with access to the City's physical property or premises, Vendor shall advise these persons of applicable visitor policies and require that they comply with them and only access authorized areas. Pursuant to this Agreement, Contractor shall be responsible for any fraudulent or dishonest acts committed by Contractor's employees, personnel, temporary employees, agents, contractors, representatives, counsel, subcontractors, directors, or officers.

2.3 Vendor shall ensure that, at all times, all of the City Information shall remain in networks, systems, facilities, data centers, gateways, hosting facilities, and cloud facilities physically located solely in the continental United States. Vendor shall not transmit, disclose, have access to, or process City Information outside of the continental United States of America. At all times, Vendor shall provide support calls from within the boundaries of the continental United States of America.

2.4 Vendor represents and warrants it has used and will use commercially reasonable efforts utilizing generally accepted industry tools and practices to provide services under this Agreement that does not contain any time bombs, worms, viruses, Trojan horses, protect codes, data destruct keys, or other programming devices that are intended to access, modify, delete, damage, deactivate, or disable software or services. Furthermore, Vendor shall utilize up-to-date and comprehensive virus and malware protection capabilities, and commercially reasonable practices, including but not limited to, detection, scanning, and removal of known viruses, worms, and other malware on any Vendor-controlled, owned, or hosting systems. These cyber protection and detection capabilities shall be in force on all computers, equipment, and/or devices utilized in connection with the services provided under this Agreement, as well as scanning data files or other transfers that have access or are connected to Vendor's hosting systems. Vendor shall mitigate security vulnerabilities through the use of perimeter and host countermeasures such as intrusion prevention, web application firewall, IP address shunning, and other measures designed to prevent exploitation of vulnerabilities.

2.5 Vendor shall use best efforts to prevent, monitor, mitigate, and remediate against: (i) services that sends or stores infringing, obscene, threatening, libelous, or otherwise unlawful or tortious material, including material harmful to children or violative of third party privacy rights; (ii) any upload to the services or use the services to send or store viruses, worms, time bombs, Trojan horses or other harmful or malicious code, files, scripts, agents, or programs; (iii) interference with or disruption of the integrity or performance of the services or the data contained therein; attempts to gain unauthorized access to the services or its related systems or networks; or (iv) export, re-export, transfer, or make available, whether directly or indirectly, any regulated item or information to anyone outside of the United States in connection with this Agreement without first complying with all applicable export control laws and regulations that may imposed by the U.S.

Government and any country or organization of nations within whose jurisdiction Vendor operates or does business, and shall not Cause City to violate the same.

2.6 Vendor shall proactively address security risks by applying released security patches, including, but not limited to, Windows security patching and updates to patch known vulnerabilities in an applicable operating system.

2.7 Vendor shall provide City and Director with the vendor name, location, and any other security information of any third-party hosting or cloud facility that will be utilized to hold, store, transmit, or otherwise have access to City Information within two (2) days of the Director's request. Vendor shall provide City and Director with at least 90 days' prior written notice of any relevant material changes to Vendor's information technology infrastructure, facilities (including but not limited to, vendor or location changes of any third-party hosting or cloud facility), or resources associated with information security governance and oversight, security, network, and infrastructure operations and any key personnel responsible for ensuring a secure environment spanning Vendor, any of its subcontractors, and the City.

Section 3. Vendor's Security Assessment Requirements:

3.1 Vendor shall maintain an information security program that provides for the security and protection of the City Information, including, but not limited to, processes and procedures to respond to security incidents. Vendor shall operate in conformance with the physical, technical, operational and administrative measures and protocols regarding data security as set forth in its then current Standards for Attestation Engagements ("SSAE") No. 18 SOC2 Report (or equivalent report), received from its third-party auditors. Vendor shall, upon written request, provide City with copies of then-current SSAE No. 18 report issued by its third-party independent auditors in relation to the data security policies and procedures designed to meet the requirements set forth in this Agreement, which includes this Security Addendum. This provision shall survive the expiration or termination of this Agreement so long as Vendor holds or has access to City Information.

Section 4. Security Monitoring and Response:

4.1 Vendor shall maintain formal processes to detect, report, respond to, and mitigate and remediate Incidents in a timely manner. If Vendor learns or has reasonable suspicion that any person (including without limitation, Vendor's personnel and third parties) has gained unauthorized access to City Information, or any person has gained unauthorized access to Vendor's network and/or data storage facilities such that any City Information is obtained by an outside party, or the City Information has otherwise been disclosed to unauthorized parties (other than in the proper performance of those services or support therefor), each an "Incident", then Vendor shall promptly (within 24 hours) (i) notify the City Attorney and Director in writing of the nature and extent of the Incident; (ii) conduct an investigation to determine when and, if possible, how the Incident occurred, and then (iii) assist the City in investigating and assessing the extent and nature of the Incident; (iv) use all reasonable endeavors to promptly remedy the Incident and prevent the occurrence of any similar Incident; and (v) inform the City upon request as to the current status of such endeavors. Vendor shall be liable for such data breach or unauthorized access, including but not limited to, any related costs or expense (including cost of notification) and any notification required by law or regulation.

Section 5. Incident Remediation:

5.1 Upon becoming aware of an Incident, Vendor shall Mitigate or Remediate any Incident within 48 hours from the time Vendor becomes aware of the Incident. With respect to Incidents that are Mitigated (but not Remediated), Vendor shall Remediate such Incidents within five business days after being Mitigated. If Vendor fails to Mitigate or Remediate any Incident within the required timeframe: (a) such failure shall be deemed a material breach of this Agreement; and (b) City may immediately terminate this Agreement or Vendor's access to City Information, including any system interfaces, connectors, or links without cost or penalty, and Vendor shall not be relieved of its obligation to continue to provide services under this Agreement, except to the extent such services are directly impacted by the termination of access.

Section 6. Data Recovery:

6.1 If as a result of Vendor's performance under this Agreement, any City Information is lost or corrupted, Vendor shall restore the data to the previous day's uncorrupted state. Loss or corrupted data means data that is inaccessible, and not merely one that contains inaccurate data due to service defects or other reasons.

6.2 Vendor shall maintain and implement disaster recovery and avoiding procedures to ensure that the services provided by Vendor are not interrupted during any disaster and the City's Information is not lost or destroyed during any disaster. For any of the City's Information that is managed, maintained, stored, or hosted by or on behalf of Vendor, Vendor shall execute nightly database or systems backups to a backup server.

Section 7. Confidentiality Obligations and Information Disposal Procedures

7.1 Vendor and its personnel, temporary employees, agents, contractors, representatives, counsel, and subcontractors shall hold all City Information that they receive, or to which they have access, in strictest confidence. Vendor and its personnel, temporary employees, agents, contractors, representatives, counsel, and subcontractors shall not disclose, disseminate, or use the City Information unless the Director authorizes it in writing prior to such disclosure, dissemination, or use. Vendor shall obtain written agreements from its personnel, temporary employees, agents, contractors, representatives, counsel, and subcontractors which bind them to the terms in this Security Addendum and shall provide a copy of such written agreement to City upon request by City or the Director. The placement of a copyright notice on any City Information will not be construed to mean that such information has been published and will not release Vendor from its obligation of confidentiality hereunder. The terms and conditions of this Confidentiality section shall survive the expiration or termination of this Agreement for any reason.

7.2 Upon request by the Director at any time during the Term of this Agreement and upon expiration or termination of this Agreement, Vendor shall retain, migrate, or dispose of the City's Information as directed by the Director. Within two (2) days of Vendor's receipt of the Director's written request to retain, migrate, or dispose of the City's Information, Vendor shall notify the Director in writing of the estimated storage size and types of data to be retained, migrated, or disposed of. Within thirty (30) days of Vendor's receipt of the Director's written request to retain, migrate, or dispose of the City's Information, Vendor shall perform the following to the extent applicable unless otherwise directed by the Director at no additional cost to the City:

- (1) deliver the City's Information (in whole or in part, as directed by the Director) and physical media owned or provided by the City to the Director, in the format and on the media requested by the Director;
- (2) destroy the City's Information (in whole or in part, as directed by the Director) and provide a certified statement of destruction to the Director;
- (3) destroy physical media using secure industry standard methods;
- (4) remove the City's Information (in whole or in part, as directed by the Director) from the hosted database, storage device, server, or other repository or storage means; or
- (5) retain the City's Information (in whole or in part, as directed by the Director) and migrate the designated information to a mutually agreed upon, secure location, database, or storage device for storage and retention of City Information.

7.3 In the event the Director directs the Vendor to destroy City Information without the destruction of the physical media, then Vendor shall destroy City Information in a manner that prevents attempts to restore that City Information.