**EXHIBIT F**

**CYBERSECURITY TERMS AND CONDITIONS**

In order to assure the privacy and security of the personal information of the City's customers and people who do business with the City, including, without limitation, vendors, utility customers, library patrons, and other individuals and companies, who are required to share such information with the City, as a condition of receiving services from the City or selling goods and services to the City, including, without limitation, the Software as a Service services provider (the "Consultant") and its subcontractors, if any, including, without limitation, any Information Technology ("IT") infrastructure services provider, shall design, install, provide, and maintain a secure IT environment, described below, while it renders and performs the Services and furnishes goods, if any, described in the Statement of Work, Exhibit B, to the extent any scope of work implicates the confidentiality and privacy of the personal information of the City's customers. The Consultant shall fulfill the data and information security requirements (the "Requirements") set forth in Part A below.

A "secure IT environment" includes (a) the IT infrastructure, by which the Services are provided to the City, including connection to the City's IT systems; (b) the Consultant's operations and maintenance processes needed to support the environment, including disaster recovery and business continuity planning; and (c) the IT infrastructure performance monitoring services to ensure a secure and reliable environment and service availability to the City. "IT infrastructure" refers to the integrated framework, including, without limitation, data centers, computers, and database management devices, upon which digital networks operate.

In the event that, after the Effective Date, the Consultant reasonably determines that it cannot fulfill the Requirements, the Consultant shall promptly inform the City of its determination and submit, in writing, one or more alternate countermeasure options to the Requirements (the "Alternate Requirements" as set forth in Part B), which may be accepted or rejected in the reasonable satisfaction of the Information Security Manager (the "ISM").

**Part A. Requirements:**

The Consultant shall at all times during the term of any contract between the City and the Consultant:

1. Appoint or designate an employee, preferably an executive officer, as the security liaison to the City with respect to the Services to be performed under this Agreement.
2. Comply with the City's Information Privacy Policy:
3. Have adopted and implemented information security and privacy policies that are documented, are accessible to the City, and conform to ISO 27001/2 – Information Security Management Systems (ISMS) Standards. See the following:

<http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=42103>

<http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297>

1. Conduct routine data and information security compliance training of its personnel that is appropriate to their role.
2. Develop and maintain detailed documentation of the IT infrastructure, including software versions and patch levels.
3. Develop an independently verifiable process, consistent with industry standards, for performing professional and criminal background checks of its employees that (1) would permit verification of employees' personal identity and employment status, and (2) would enable the immediate denial of access to the City's confidential data and information by any of its employees who no longer would require access to that information or who are terminated.
4. Provide a list of IT infrastructure components in order to verify whether the Consultant has met or has failed to meet any objective terms and conditions.
5. Implement access accountability (identification and authentication) architecture and support role-based access control ("RBAC") and segregation of duties ("SoD") mechanisms for all personnel, systems, and Software used to provide the Services. "RBAC" refers to a computer systems security approach to restricting access only to authorized users. "SoD" is an approach that would require more than one individual to complete a security task in order to promote the detection and prevention of fraud and errors.
6. Assist the City in undertaking annually an assessment to assure that: (1) all elements of the Services' environment design and deployment are known to the City, and (2) it has implemented measures in accordance with industry best practices applicable to secure coding and secure IT architecture.
7. Provide and maintain secure intersystem communication paths that would ensure the confidentiality, integrity, and availability of the City's information.
8. Deploy and maintain IT system upgrades, patches and configurations conforming to current patch and/or release levels by not later than one (1) week after its date of release. Emergency security patches must be installed within 24 hours after its date of release.
9. Provide for the timely detection of, response to, and the reporting of security incidents, including on-going incident monitoring with logging.
10. Notify the City within one (1) hour of detecting a security incident that results in the unauthorized access to or the misuse of the City's confidential data and information.
11. Inform the City that any third party service provider(s) meet(s) all of the Requirements.
12. Perform security self-audits on a regular basis and not less frequently than on a quarterly basis, and provide the required summary reports of those self-audits to the ISM on the annual anniversary date or any other date agreed to by the Parties.
13. Accommodate, as practicable, and upon reasonable prior notice by the City, the City's performance of random site security audits at the Consultant's site(s), including the site(s) of a third-party service provider(s), as applicable. The scope of these audits will extend to the Consultant's and its third-party service provider(s)' awareness of security policies and practices, systems configurations, access authentication and authorization, and incident detection and response.
14. Cooperate with the City to ensure that to the extent required by applicable laws, rules and regulations, and the Confidential Information will be accessible only by the Consultant and any authorized third-party service provider's personnel.
15. Perform regular, reliable secured backups of all data needed to maximize the availability of the Services. Adequately encrypt theCity of Palo Alto's data, during the operational process, hosted at rest, and the backup stage at the Vendors' environment (including Vendor's contracting organization's environment).
16. Maintain records relating to the Services for a period of three (3) years after the expiration or earlier termination of this Agreement and in a mutually agreeable storage medium. Within thirty (30) days after the effective date of expiration or earlier termination of this Agreement, all of those records relating to the performance of the Services shall be provided to the ISM.
17. Maintain the Confidential Information in accordance with applicable federal, state, and local data and information privacy laws, rules, and regulations.
18. Encrypt the Confidential Information before delivering the same by electronic mail to the City and or any authorized recipient.
19. Provide Network Layer IP filtering services to allow access only from the City of Palo Alto's IP address to the Vendor environment (primarily hosted for the City of Palo Alto).
20. Offer a robust disaster recovery and business continuity (DR-BCP) solutions to the City for the systems and services the Vendor provides to the City.
21. Provide and support Single Sign-on (SSO) and Multifactor Authentication (MFA) solutions for authentication and authorization services from the "City's environment to the Vendor's environment," and Vendor's environment to the Vendor's cloud services/hosted environment." The Vendor shall allow two employees of the City to have superuser and super-admin access to the Vendor's IT environment, and a cloud-hosted IT environment belongs to the City.
22. Unless otherwise addressed in the Agreement, shall not hold the City liable for any direct, indirect or punitive damages whatsoever including, without limitation, damages for loss of use, data or profits, arising out of or in any way connected with the City's IT environment, including, without limitation, IT infrastructure communications.
23. The Vendor must provide evidence of valid cyber liability insurance policy per the **City’s EXHIBIT “D”** **INSURANCE REQUIREMENTS.**

**Part B. Alternate Requirements:**