



## INFORMATION PRIVACY POLICY

### POLICY STATEMENT

The City of Palo Alto (the “City”) strives to promote and sustain a superior quality of life for persons in Palo Alto. In promoting the quality of life of these persons, it is the policy of the City, consistent with the provisions of the California Public Records Act, California Government Code §§ 6250 – 6270, to take appropriate measures to safeguard the security and privacy of the personal (including, without limitation, financial) information of persons, collected in the ordinary course and scope of conducting the City’s business as a local government agency. These measures are generally observed by federal, state and local authorities and reflected in federal and California laws, the City’s rules and regulations, and industry best practices, including, without limitation, the provisions of California Civil Code §§ 1798.3(a), 1798.24, 1798.79.8(b), 1798.80(e), 1798.81.5, 1798.82(e), 1798.83(e)(7), and 1798.92(c). Though some of these provisions do not apply to local government agencies like the City, the City will conduct business in a manner which promotes the privacy of personal information, as reflected in federal and California laws. The objective of this Policy is to describe the City’s data security goals and objectives, to ensure the ongoing protection of the Personal Information, Personally Identifiable Information, Protected Critical Infrastructure Information and Personally Identifying Information of persons doing business with the City and receiving services from the City or a third party under contract to the City to provide services. The terms “Personal Information,” “Protected Critical Infrastructure Information”, “Personally Identifiable Information” and “Personally Identifying Information” (collectively, the “Information”) are defined in the California Civil Code sections, referred to above, and are incorporated in this Policy by reference.

### PURPOSE

The City, acting in its governmental and proprietary capacities, collects the Information pertaining to persons who do business with or receive services from the City. The Information is collected by a variety of means, including, without limitation, from persons applying to receive services provided by the City, persons accessing the City’s website, and persons who access other information portals maintained by the City’s staff and/or authorized third-party contractors. The City is committed to protecting the privacy and security of the Information collected by the City. The City acknowledges federal and California laws, policies, rules, regulations and procedures, and industry best practices are dedicated to ensuring the Information is collected, stored and utilized in compliance with applicable laws.

## **POLICY AND PROCEDURES 1-64/IT**

Revised: December 2017

The goals and objectives of the Policy are: (a) a safe, productive, and inoffensive work environment for all users having access to the City's applications and databases; (b) the appropriate maintenance and security of database information assets owned by, or entrusted to, the City; (c) the controlled access and security of the Information provided to the City's staff and third party contractors; and (d) faithful compliance with legal and regulatory requirements.

### **SCOPE**

The Policy will guide the City's staff and, indirectly, third party contractors, which are by contract required to protect the confidentiality and privacy of the Information of the persons whose personal information data are intended to be covered by the Policy and which will be advised by City staff to conform their performances to the Policy should they enjoy conditional access to that information.

### **CONSEQUENCES**

The City's employees shall comply with the Policy in the execution of their official duties to the extent their work implicates access to the Information referred to in this Policy. A failure to comply may result in employment and/or legal consequences.

### **EXCEPTIONS**

In the event that a City employee cannot fully comply with one or more element(s) described in this Policy, the employee may request an exception by submitting Security Exception Request. The exception request will be reviewed and administered by the City's Information Security Manager (the "ISM"). The employee, with the approval of his or her supervisor, will provide any additional information as may be requested by the ISM. The ISM will conduct a risk assessment of the requested exception in accordance with guidelines approved by the City's Chief Information Officer ("CIO") and approved as to form by the City Attorney. The Policy's guidelines will include at a minimum: purpose, source, collection, storage, access, retention, usage, and protection of the Information identified in the request. The ISM will consult with the CIO to approve or deny the exception request. After due consideration is given to the request, the exception request disposition will be communicated, in writing, to the City employee and his or her supervisor. The approval of any request may be subject to countermeasures established by the CIO, acting by the ISM.

### **MUNICIPAL ORDINANCE**

This Policy will supersede any City policy, rule, regulation or procedure regarding information privacy.

### **RESPONSIBILITIES OF CITY STAFF**

## **POLICY AND PROCEDURES 1-64/IT**

Revised: December 2017

### **A. RESPONSIBILITY OF CIO AND ISM**

The CIO, acting by the ISM, will establish an information security management framework to initiate and coordinate the implementation of information security measures by the City's government.

The City's employees, in particular, software application users and database users, and, indirectly, third party contractors under contract to the City to provide services, shall be guided by this Policy in the performance of their job responsibilities.

The ISM will be responsible for: (a) developing and updating the Policy, (b) enforcing compliance with and the effectiveness of the Policy; (c) the development of privacy standards that will manifest the Policy in detailed, auditable technical requirements, which will be designed and maintained by the persons responsible for the City's IT environments; (d) assisting the City's staff in evaluating security and privacy incidents that arise in regard to potential violations of the Policy; (e) reviewing and approving department-specific policies and procedures which fall under the purview of this Policy; and (f) reviewing Non-Disclosure Agreements (NDAs) signed by third party contractors, which will provide services, including, without limitation, local or 'cloud-based' software services to the City.

### **B. RESPONSIBILITY OF INFORMATION SECURITY STEERING COMMITTEE**

The Information Security Steering Committee (the "ISSC"), which is comprised of the City's employees, drawn from the various City departments, will provide the primary direction, prioritization and approval for all information security efforts, including key information security and privacy risks, programs, initiatives and activities. The ISSC will provide input to the information security and privacy strategic planning processes to ensure that information security risks are adequately considered, assessed and addressed at the appropriate City department level.

### **C. RESPONSIBILITY OF USERS**

All authorized users of the Information will be responsible for complying with information privacy processes and technologies within the scope of responsibility of each user.

### **D. RESPONSIBILITY OF INFORMATION TECHNOLOGY (IT) MANAGERS**

The City's IT Managers, who are responsible for internal, external, direct and indirect connections to the City's networks, will be responsible for configuring, maintaining and securing the City's IT networks in compliance with the City's information security and privacy policies. They are also responsible for timely internal reporting of events that may have compromised network, system or data security.

**POLICY AND PROCEDURES 1-64/IT**

Revised: December 2017

**E. RESPONSIBILITY OF AUTHORIZATION COORDINATION**

The ISM will ensure that the City's employees secure the execution of Non-Disclosure Agreements (NDA), whenever access to the Information will be granted to third party contractors, in conjunction with the Software as a Service (SaaS) Security and Privacy Terms and Conditions. An NDA must be executed prior to the sharing of the Information of persons covered by this Policy with third party contractors. The City's approach to managing information security and its implementation (i.e. objectives, policies, processes, and procedures for information security) will be reviewed independently by the ISM at planned intervals, or whenever significant changes to security implementation have occurred.

The CIO, acting by the ISM, will review and recommend changes to the Policy annually, or as appropriate, commencing from the date of its adoption.

**GENERAL PROCEDURE FOR INFORMATION PRIVACY****A. OVERVIEW**

The Policy applies to activities that involve the use of the City's information assets, namely, the Information of persons doing business with the City or receiving services from the City, which are owned by, or entrusted to, the City and will be made available to the City's employees and third party contractors under contract to the City to provide Software as a Service consulting services. These activities include, without limitation, accessing the Internet, using e-mail, accessing the City's intranet or other networks, systems, or devices.

The term "information assets" also includes the personal information of the City's employees and any other related organizations while those assets are under the City's control. Security measures will be designed, implemented, and maintained to ensure that only authorized persons will enjoy access to the information assets. The City's staff will act to protect its information assets from theft, damage, loss, compromise, and inappropriate disclosure or alteration. The City will plan, design, implement and maintain information management systems, networks and processes in order to assure the appropriate confidentiality, integrity, and availability of its information assets to the City's employees and authorized third parties.

**B. PERSONAL INFORMATION AND CHOICE**

Except as permitted or provided by applicable laws, the City will not share the Information of any person doing business with the City, or receiving services from the City, in violation of this Policy, unless that person has consented to the City's sharing of such information during the conduct of the City's business as a local government agency with third parties under contract to the City to provide services.

**POLICY AND PROCEDURES 1-64/IT**

Revised: December 2017

**C. METHODS OF COLLECTION OF PERSONAL INFORMATION**

The City may gather the Information from a variety of sources and resources, provided that the collection of such information is both necessary and appropriate in order for the City to conduct business as a local government agency in its governmental and proprietary capacities. That information may be gathered at service windows and contact centers as well as at web sites, by mobile applications, and with other technologies, wherever the City may interact with persons who need to share such formation in order to secure the City's services.

The City's staff will inform the persons whose Information are covered by this Policy that the City's web site may use "cookies" to customize the browsing experience with the City of Palo Alto web site. The City will note that a cookie contains unique information that a web site can use to track, among others, the Internet Protocol address of the computer used to access the City's web sites, the identification of the browser software and operating systems used, the date and time a user accessed the site, and the Internet address of the website from which the user linked to the City's web sites. Cookies created on the user's computer by using the City's web site do not contain the Information, and thus do not compromise the user's privacy or security. Users can refuse the cookies or delete the cookie files from their computers by using any of the widely available methods. If the user chooses not to accept a cookie on his or her computer, it will not prevent or prohibit the user from gaining access to or using the City's sites.

**D. UTILITIES SERVICE**

In the provision of utility services to persons located within Palo Alto, the City of Palo Alto Utilities Department ("CPAU") will collect the Information in order to initiate and manage utility services to customers. To the extent the management of that information is not specifically addressed in the Utilities Rules and Regulations or other ordinances, rules, regulations or procedures, this Policy will apply; provided, however, any such Rules and Regulations must conform to this Policy, unless otherwise directed or approved by the Council. This includes the sharing of CPAU-collected Information with other City departments except as may be required by law.

Businesses and residents with standard utility meters and/or having non-metered monthly services will have secure access through a CPAU website to their Information, including, without limitation, their monthly utility usage and billing data. In addition to their regular monthly utilities billing, businesses and residents with non-standard or experimental electric, water or natural gas meters may have their usage and/or billing data provided to them through non-City electronic portals at different intervals than with the standard monthly billing.

**POLICY AND PROCEDURES 1-64/IT**

Revised: December 2017

Businesses and residents with such non-standard or experimental metering will have their Information covered by the same privacy protections and personal information exchange rules applicable to Information under applicable federal and California laws.

**E. PUBLIC DISCLOSURE**

The Information that is collected by the City in the ordinary course and scope of conducting its business could be incorporated in a public record that may be subject to inspection and copying by the public, unless such information is exempt from disclosure to the public by California law.

**F. ACCESS TO PERSONAL INFORMATION**

The City will take reasonable steps to verify a person's identity before the City will grant anyone online access to that person's Information. Each City department that collects Information will afford access to affected persons who can review and update that information at reasonable times.

**G. SECURITY, CONFIDENTIALITY AND NON-DISCLOSURE**

Except as otherwise provided by applicable law or this Policy, the City will treat the Information of persons covered by this Policy as confidential and will not disclose it, or permit it to be disclosed, to third parties without the express written consent of the person affected. The City will develop and maintain reasonable controls that are designed to protect the confidentiality and security of the Information of persons covered by this Policy.

The City may authorize the City's employee and or third party contractors to access and/or use the Information of persons who do business with the City or receive services from the City. In those instances, the City will require the City's employee and/or the third party contractors to agree to use such Information only in furtherance of City-related business and in accordance with the Policy.

If the City becomes aware of a breach, or has reasonable grounds to believe that a security breach has occurred, with respect to the Information of a person, the City will notify the affected person of such breach in accordance with applicable laws. The notice of breach will include the date(s) or estimated date(s) of the known or suspected breach, the nature of the Information that is the subject of the breach, and the proposed action to be taken or the responsive action taken by the City.

**H. DATA RETENTION / INFORMATION RETENTION**

**POLICY AND PROCEDURES 1-64/IT**

Revised: December 2017

The City will store and secure all Information for a period of time as may be required by law, or if no period is established by law, for seven (7) years, and thereafter such information will be scheduled for destruction.

**I. SOFTWARE AS A SERVICE (SAAS) OVERSIGHT**

The City may engage third party contractors and vendors to provide software application and database services, commonly known as Software-as-a-Service (SaaS).

In order to assure the privacy and security of the Information of those who do business with the City and those who received services from the City, as a condition of selling goods and/or services to the City, the SaaS services provider and its subcontractors, if any, including any IT infrastructure services provider, shall design, install, provide, and maintain a secure IT environment, while it performs such services and/or furnishes goods to the City, to the extent any scope of work or services implicates the confidentiality and privacy of the Information.

These requirements include information security directives pertaining to: (a) the IT infrastructure, by which the services are provided to the City, including connection to the City's IT systems; (b) the SaaS services provider's operations and maintenance processes needed to support the IT 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. The term "IT infrastructure" refers to the integrated framework, including, without limitation, data centers, computers, and database management devices, upon which digital networks operate.

Prior to entering into an agreement to provide services to the City, the City's staff will require the SaaS services provider to complete and submit an Information Security and Privacy Questionnaire. In the event that the SaaS services provider reasonably determines that it cannot fulfill the information security requirements during the course of providing services, the City will require the SaaS services provider to promptly inform the ISM.

**J. FAIR AND ACCURATE CREDIT TRANSACTION ACT OF 2003**

CPAU will require utility customers to provide their Information in order for the City to initiate and manage utility services to them.

Federal regulations, implementing the Fair and Accurate Credit Transactions Act of 2003 (Public Law 108-159), including the Red Flag Rules, require that CPAU, as a "covered financial institution or creditor" which provides services in advance of payment and which can affect consumer credit, develop and implement procedures for an identity theft program for new and existing accounts to detect, prevent, respond and mitigate potential identity theft of its customers' Information.

**POLICY AND PROCEDURES 1-64/IT**

Revised: December 2017

CPAU procedures for potential identity theft will be reviewed independently by the ISM annually or whenever significant changes to security implementation have occurred. The ISM will recommend changes to CPAU identity theft procedures, or as appropriate, so as to conform to this Policy.

There are California laws which are applicable to identity theft; they are set forth in California Civil Code § 1798.92.

NOTE: Questions regarding this policy should be referred to the Information Technology Department, as appropriate.

Recommended:	<div>DocuSigned by: <i>Jonathan Reichental</i> 7914D9897578424...</div> <hr/>	<div>12/5/2017</div> <hr/>
	Director Information Technology/CIO	Date
Approved:	<div>DocuSigned by: <i>J. K. Forge</i> 39E7298FB2064DB...</div> <hr/>	<div>12/13/2017</div> <hr/>
	City Manager	Date