



This document is to be completed for new or upgraded technology acquisitions, contracts, and projects. Please submit with all other proposals and agreement terms for review by the County Information Security Officer according to directives in Administrative Memorandum B-1. All questions must be answered fully.

Submitting Department _____

Submitter's Name _____

Phone _____

Section 1: Vendor Information

Name: Corporate Phone #:

Address: City: State: ZIP:

Technical Support Contact Methods: Phone: IM/Chat
(Select all that apply) Email: Web Portal

Technical Support Coverage Hours: 24x7x365 Business Hours M-F 8-5 Pacific Other

Does the vendor provide a dedicated account manager or representative for escalating problems or incidents? Yes No
If yes, please provide name.

Does the vendor maintain any formal security policies & procedures to comply with industry requirements? Yes No

How often is the vendor's security posture reviewed?

Will the vendor provide a copy of their last security audit? Yes No

Does the vendor have any third-party certifications or attestations, such as FedRamp, FIPS 140 -2, FISMA and DIACAP, HIPAA, ISO 27001, PCI DSS, TRUSTe or SOC 1/SOC 2/SSAE 16/ISAE 3402? If yes, provide certification or attestations. Yes No

Section 2: Product Information

Product Name: No. of Users: Does the product have technical constraints to the number of concurrent users it can support? Yes No

This is an upgrade or renewal for existing technology currently in use in the County

Location: On-Premise Hosted (Cloud/Off-site) Hybrid (On-Premise/Cloud)

Product Description and Purpose: Please include information that will identify the function, business process, and the departments/divisions who will use it.

Integration: Does the product integrate or interface with any other existing or planned products or services used either at the County, or with another third-party County vendor? This would include requirements for integration or use of the County's email System, ServiceNow, or other systems. Yes No

Has the application been subjected to any breaches? If yes, include separately, enacted steps to mitigate including response and escalation processes. Yes No

Known Vulnerabilities? Yes No

Data Sensitivity: Public Internal Confidential Restricted
Data Criticality: Useful Important Essential

For details on Data Sensitivity and Data Criticality, please see the References section of this document

Section 3: Administrative Controls

Configuration and System Hardening: Does the product offer a baseline configuration or system hardening tool that can protect the product against confidential data disclosure or service disruption? **Please provide system configuration diagram

Yes No

Backup and Restore: Does the product offer features to backup and restore user data, configurations, and application code?

Yes No

Does the product integrate with CommVault Storage Services and API (the County's backup platform)?

Yes No

If there is a backup process performed by Vendor: Yes No

How often:

Encrypted? Yes No

Retention period

Where stored?

Data at Termination of Agreement: Will the data be returned? Yes No

What assurance is provided for complete removal?

Section 4: Security Controls

Monitoring and Event Management: Describe how the product can be monitored for performance, reliability, and security. Include how the product reacts to events that are raised during normal operations.

Can the product forward events to a central log repository or System Event and Incident Management (SEIM) platform?

Yes No

Patching: Describe how the product is patched and updated. Include how frequently the vendor provides security fixes and updates.

If the hardware is onsite, can County engineers apply patches?

Yes No

If hosted, please provide version, service pack, patches, and how will the server be maintained to the latest patch level?

Malware Protection: Will the product be affected by servers or endpoints that run anti-virus/anti-malware protection? If yes, provide details on what exclusions are required for the product to work effectively.

Yes No

Employees: Have employees undergone a background check process? Yes No

Will the provider use a subcontractor or 3rd party service provider? Yes No

If yes, please attach and provide for each subcontractor, the security and privacy agreement.

SaaS: Is the product 100% web-based? Yes No

What are the browser security configuration requirements?

Is the portal ADA compliant with Section 508 of the Rehabilitation Act and follows the principles of responsive web design? Yes No

Disaster Recovery: Is the location of the server, if hosted, in an area prone to natural disaster? Yes No

Is there a disaster recovery plan in place? Yes No

Identity and Authentication Management:

Does the product provide for, or support *identity and authentication integration with via other credentialing systems or protocols?*

Note: SAML 2.0 and OAuth 2.0 are the preferred choice for integration with San Mateo County systems (older versions are not compatible).

 Yes No

If yes, please specify

 SAML Active Directory OAuth LDAP MFA Other

***If OKTA integration is selected for application integration, answering the Password Management section below will not be required.**

Password Management:

How are accounts provisioned and managed (include deprovisioning and removal)?

Does the product provide for password management that meets the County password policy for complexity, expiration, reuse, and lockout? **See References section for more information about San Mateo County's Password Policy**

 Yes No

- All users have a single account with unique account ID?
- First time password must be unique and changed upon initial login?
- Password must be changed every 60 days?
- Password must have at least 8 characters and 1 character from 3 of: lowercase, uppercase, number, and special character?

 Yes No Yes No Yes No Yes No

Does the product provide for password self-reset capability?

 Yes No

How are passwords stored? Encrypted?

 Yes No

Access Management: Does the product allow for privileges to be assigned to both individuals and 'groups' of individuals in order to support the use of 'Roles' for access permissions? Please describe method used.

 Yes No

Encryption: Identify and describe whether the product encrypts data during different states – i.e., at rest, in use, and in transit. Also include credentials (usernames, passwords, etc).

Data-in-transit	<input type="text"/>
Data-in-use	<input type="text"/>
Data-at-rest	<input type="text"/>
Credentials	<input type="text"/>

Auditing: Does the product provide a mechanism for auditing system activity and/or reporting of that activity? Examples of auditing include user login/logoff, user actions, data export, and permission changes.

 Yes No

Section 5: Cloud/Hosted Services

Data Sovereignty: Does the vendor keep all the data within the United States? Please provide location(s) where San Mateo County's data will be stored.

Tenancy: Describe how San Mateo County data resides with other customer data in the hosted environment-- i.e., is the data co-mingled in a single database, or are there separate customer databases?

Hosted Platform: Please describe the vendor's technology platform in the hosted environment-- both application, database, and/or other layers (e.g., Ruby on Rails, Redis Cache, MongoDB)

Third Party Services: Does the vendor use any third-party services (e.g., for development, QA, helpdesk, integration services, offsite backup locations, etc.) where the third party vendors have access to San Mateo County data?

 Yes No

Network Defenses: Please describe how the vendor's network perimeter is protected, including whether an IPS/IDS and anti-virus system is activated, and whether there is a central logging facility for perimeter events

Service Levels and Incident Response:

What is the service level for this hosted product, and how does the vendor guarantee that level for its customers? Include how the vendor notifies customers of incidents that do not meet service levels.

Data Loss Events: Has the vendor experienced any data loss incidents which required reporting to regulatory authorities in the past 24 months?

 Yes No

Forensic Analysis: Who would perform a forensic analysis of a breach if one were to occur at the vendor site?

IP Restrictions: Does the vendor's hosted site have the capability to restrict access to San Mateo County's public IP address space? Yes No

Section 6: References

Password Policy

The County of San Mateo's Information Security Policy requires new technology implementations that use passwords to adhere to the following password requirements:

County of San Mateo Password Requirements

1. All users must have unique account IDs that identifies a single account owner
2. First time password must be unique to an individual, and require change upon initial login
3. The permanent / long term password requires an enforceable change every 60 days
4. The password must enforce a minimum of at least 8 characters, and contain at least one character from three of the following:
 - a. Lower Case
 - b. UpperCase
 - c. Numbers
 - d. Special Characters

Data Classification Standards

In order to apply the proper security safeguards to digital assets, the County of San Mateo classifies new technology both to a Sensitivity and Criticality class. The following information defines those classification standards, and is added as a resource to answering the questions in Section 3, 'Product Information'.

Sensitivity Class	Description	Criticality Class	Description
Public	<p>Public data is information assets that can be disclosed without restrictions. Permission to release or share data does not require approval. Examples:</p> <ul style="list-style-type: none"> Information typically included on the San Mateo County website— County addresses, department phone numbers, generic department emails, Applications, request forms, press releases 	Useful	<p>Useful data is information assets helpful to the mission of the health system, but whose availability isn't necessary to maintain day-day operations. Useful data is often characterized with low risk in case of loss or compromise. Examples:</p> <ul style="list-style-type: none"> Printers and Fax machines where there are multiple alternatives Images of workstations that can be rebuilt if necessary Training materials Reports that can be reproduced from original sources
Internal	<p>Internal data is intended to be used only within San Mateo County, but disclosure poses minimal business impact, and may even be subject to release per the County's Open Data Policy. Permission to share publicly is to be given by the data steward or through committee approval. Examples:</p> <ul style="list-style-type: none"> Business plans, budgets, vendor lists, vendor contracts Memo's, meeting minutes, policies/procedures 	Important	<p>Important data is information assets whose availability is valuable for maintaining day-day operations, but service-levels can tolerate an unscheduled period of downtime. Downtime for Important data is acceptable at certain days/hours in given week, but usually no longer than three (3) consecutive days for any single event. Examples:</p> <ul style="list-style-type: none"> Software systems that are only used during the weekday and/or normal business hours Software systems where data sets updates are not updated frequently, and business tasks can be deferred without service impact Managed Services run by the State of California Systems where contingency plans can maintain service levels
Confidential	<p>Confidential data is information assets that, if compromised, could adversely impact customers or San Mateo County business. This information is to receive data protection for storage and transport, should only be used for business purposes, and where possible be identified as confidential by those who use it. Examples:</p> <ul style="list-style-type: none"> Social Security Numbers, Driver's license number, credit cards Personal addresses, phone numbers, private email addresses Access codes or passwords <p>A compromise of Confidential data is to be reported as a security incident, as outlined in the County's Incident Response Plan.</p>	Essential	<p>Essential data requires nearly continuous uptime. Business processes are adversely affected with even a small amount of unscheduled downtime, impacting the job performance of the workforce and services to customers. Access to these information assets typically requires 24x7x7 availability, and must be rigorously protected. Examples:</p> <ul style="list-style-type: none"> EMR Systems Identity Management Applications Core networking equipment
Restricted	<p>Restricted data is Confidential data—except, the business impact for compromise is much greater. This includes civil penalties, regulatory redaction for organizational credentials, and formal notification to federal, state, and local authorities. Restricted data typically involves information that has contractual, legal, or regulatory obligations to protect the data in the utmost manner. Examples:</p> <ul style="list-style-type: none"> Medical Records and other Protected Health Information (PHI) Employee criminal background checks <p>The organization as a whole— along with data stewards— is responsible for designating data as Restricted. A compromise of Restricted data is to be reported as a security incident, as outlined in the County's Incident Response Plan, and included notification to the County's Privacy Officer.</p>		

Section 7: Non-Compliance

Please explain area(s) of non-compliance. Provide information as to the services or systems that would be impacted as well as the proposed remediation, if any.

NOTE: All Non-Compliance must file an Information Security Risk Acceptance Form

Section 8: Other Documents

Please include any pertinent documents, diagrams of network, and/or data flow architecture

Documents included? Yes No

This assessment was prepared by (Print Name) _____

Signature _____

Date _____

Phone _____