County of San Mateo ISD

Information Services Department Technology Security Assessment

This document is to be completed for new or upgraded technology acquisitions, contracts, and projects including all design changes. Please submit all proposals and agreement terms for review to ISD B-1 Review process according to directives in Administrative Memorandum B-1. ***All questions must be answered fully.***

Submitting Department______________________________ **Submitter's Name**______________________________

Phone__________________________

Name: __________ Corporate Phone #: __________

Address: __________ City: __________ State: ____ ZIP: ______

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

Technical Support Coverage Hours: ○ 24x7x365 ○ Business Hours M-F 8-5 Pacific ○ Other Enter support hours here

Escalation procedure for incidents or problems provided? ○ Yes ○ No

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

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 two security audit, penetration test, and/or vulnerability assessment? ○ Yes ○ No

Does the vendor have any third-party certifications or attestations for its application, 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 If yes, please enter certifications or attestations here.

If cloud solution, does the vendor use a third-party storage solution? ○ Yes ○ No If yes, provide name of third-party data storage vendor Name of storage vendor

If yes, does the data storage 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 If yes, please enter third-party storage certifications or attestations here.

Section 2: Product Information

Product Name: __________ No. of Users: 1-10

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

Does the product have technical constraints to the number of concurrent users it can support? ○ Yes ○ No

Location: □ *On-Premise* □ *Hosted (Cloud/Off-site)* ○ *If hosted, GovCloud?* □ *Hybrid (On-Premise/Cloud)* ○ *If hosted, GovCloud?*

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

Please enter product description and purpose.

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 Please describe integrations here.

Does the vendor use third-party services, such as help desk, integration services, backup services, that would have access to the County's data? Please describe. ○ Yes ○ No Please describe third-party services accessing County data

Does product use open and published APIs? ○ Yes ○ No ○ N/A

Are APIs tested for potential security exploits? ○ Yes ○ No If no, describe what is used to mitigate exploitations and risks. Describe what is used to mitigate exploitations and risks.

List all ports/protocols required for any traffic outbound to the Internet or for the application. List all ports/protocols required.

Web Services: Is the product 100% web-based? ○ Yes ○ No ○ N/A   Is the County's data exposed through web services? ○ Yes ○ No ○ N/A

Does the product provide MFA for public access? ○ Yes ○ No ○ N/A   Does the administrative console require MFA? ○ Yes ○ No ○ N/A

Mobile Devices: Does the application provide mobile capabilities? ○ Yes ○ No   Is the mobile application a requirement for application? ○ Yes ○ No

Section 3: Administrative Controls

For details on Data Sensitivity and Data Criticality, please see the Section 7 References of this document

Data Sensitivity: □ Public □ Internal □ Confidential* □ Restricted * * May require NDA

Data Criticality: □ **Useful** □ **Important** □ **Essential**

Data Type: □ Data is not confidential □ PII □ HIPAA/PHI □ FTI □ EDD □ PCI-DSS □ CJI * * System may require DOJ compliance and approval

Is system HIPAA compliant? ○ Yes ○ No ○ N/A Is system CJI compliant? ○ Yes ○ No ○ N/A System meets regulatory requirements? ○ Yes ○ No ○ N/A

Configuration and System Hardening: Does the product offer baseline configuration or system hardening tool(s) that can protect the product against confidential data disclosure or service disruption? ○ Yes ○ No

Please provide additional detail on configuration and system hardening.

Please provide system configuration diagram and the transport route of data between systems (Required)

Backup and Restore: Does the product offer features to backup and restore user data, configurations, and application code? ○ Yes ○ No

Please provide additional detail on backup and restore.

Does the product integrate with Rubrik Storage Services and API (the County's backup platform)? ○ Yes ○ No ○ N/A

Is there is a backup process performed by Vendor: ○ Yes ○ No ○ N/A

How often: Please enter how often backup is performed.   Encrypted? ○ Yes ○ No

Retention period Please enter retention period.   Where stored? Please enter where the backup is stored.

Disaster Recovery: Is the location of the server, if hosted, in an area prone to natural disaster? ○ Yes ○ No ○ N/A   Please provide location Please provide location.

Is there a disaster recovery plan in place? ○ Yes ○ No   How often is the disaster recovery plan tested? Please enter times tested.

What is the guaranteed uptime? Percentage Percentage   RTO Hours   RPO Hours

Data at Termination of Agreement: Will the data be returned? ○ Yes ○ No ○ N/A

What assurance is provided for secure and complete removal? Please enter how assurance will be provided that data is completely removed.

Section 4: Security Controls

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

Please describe steps in mitigation process including escalation and notification.

Are there known vulnerabilities? ○ Yes ○ No   List known vulnerabilities Please describe known vulnerabilities here.

Are these known vulnerabilities currently being addressed? ○ Yes ○ No ○ N/A   How often is software/system tested for vulnerabilities? Please enter how often.

Does the vendor use an automated/manual source code analysis tool for secure coding? ○ Yes ○ No ○ N/A

. **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.

Please enter detail here on monitoring and event management.

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 and how cloud servers will be protected.

Please enter detail here on patching including frequency.

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 lasted patch level?

If hosted, please enter detail here on version, patching, and how servers are maintained.

Anti-Virus Protection: Is anti-virus running? ○ Yes ○ No

Malware Protection: Is malware protection running? ○ Yes ○ No

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 ○ N/A

Please provide additional detail on malware protection including exclusions needed for the product to perform with anti-malware.

Employees: Have employees undergone a background check process? ○ Yes ○ No *Background check confirmation may be required

Are employees for this project located in the United States? ○ Yes ○ No If no, what country? Please provide location.

Are employees provided required training to handle confidential data, such as CJI, for this engagement? ○ 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. If yes, provide security and privacy agreement for each subcontractor.

Security Incident Response Plan: Immediate notification to impacted parties? ○ Yes ○ No What is the time frame? Timeframe

Identity and Authentication Management:
Does the product provide for, or support identity and authentication integration with via other credentialing systems or protocols? ○ Yes ○ No
Note: SAML is the preferred choice for integration with San Mateo County systems *SaaS requires OKTA integration and MFA

If yes, please specify □ SAML □ Active Directory □ OAuth □ LDAP □ MFA □ Other If other, please indicate.

Password Management:

How are accounts provisioned and managed (include deprovisioning and removal)? Please describe how accounts are provisioned and managed.

Does the product provide for password management that meets the County password policy for complexity, expiration, reuse, and lockout? ***See Section 7 References for more information about San Mateo County's Password Policy*** ○ Yes ○ No

1. All users have a single account with unique account ID? ○ Yes ○ No
2. First time password must be unique and changed upon initial login? ○ Yes ○ No
3. Password must be changed every 60 days? ○ Yes ○ No
4. Password must have at least 8 characters and 1 character from *three* of the following: lowercase, uppercase, number, special character? ○ Yes ○ No
5. Password cannot be re-used; system is configured to remember las 12 passwords ○ Yes ○ No

Does the product provide for password self-reset capability? ○ Yes ○ No

How are passwords stored? Please describe how passwords are stored. Encrypted? ○ Yes ○ No

Access Management: Does the product allow for privileges to be assigned to both individuals and 'groups' of individuals to support the use of 'Roles' for access permissions? Please describe method used. ○ Yes ○ No

Please describe method used for access permissions.

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.). **Include encryption methodology used**

Data-in-transit Describe if data is encrypted in transit.
Data-in-use Describe if data is encrypted in use.
Data-at-rest Describe if data is encrypted at rest.
Credentials Describe if and what credentials types are used.

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

Please describe auditing mechanism here.

Audit Logs: Does vendor provide audit logs upon request? ○ Yes ○ No

Will vendor work with County to ensure audit logs can be ingested into the County's SIEM? ○ Yes ○ No

How long are the audit logs stored? How long stored?

Section 5: Cloud/Hosted Services

Data Sovereignty: Does the vendor keep all the data within the United States? ○ Yes ○ No

Please provide location(s) where San Mateo County's data will be stored. Please enter storage location(s) here.

Vendor will consult and advise the County of geographical location of data storage if data will be moved to location other than stated in this document. ○ Yes ○ No

Does the cloud solution use industry standard devices? ○ Yes ○ No

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?

Please enter tenancy details here.

Does vendor have the ability logically segment or encrypt data so that the data can be produced for a single tenant only ○ Yes ○ No

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)

Please enter details of technology platform.

Does vendor provide configuration and optimization of cloud services? ○ Yes ○ No

Does the vendor provide space availability to avoid resource exhaustion issues? ○ 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 if there is a central logging facility for perimeter events

Please enter details of network defenses used.

Does the vendor conduct network penetration tests on cloud service infrastructure regularly? ○ Yes ○ No

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

Please enter details of service levels and incident response. Include how the County will be notified.

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

Please provide name(s)/role(s), and or third-party organization(s) who may be involved.

Data Loss Events: Has the vendor experienced any data loss incident which required reporting to regulatory authorities in the past 24 months?
○ Yes ○ No

If yes, please provide additional details of data loss event.

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

If yes, please provide additional details of IP restrictions.

Section 6: Support and Maintenance

Does the vendor provide proactive system monitoring tool(s) for health check and latency detection that extends to cloud services, as needed? ○ Yes ○ No If yes, identify tool(s) used

If yes, identify system monitoring tool(s) used.

Is monitoring 24x7 ○ Yes ○ No If not, how often? If not, how often?

Does the vendor track performance against SLAs? ○ Yes ○ No

Is provided vendor support located in the US? ○ Yes ○ No If no, provide location Vendor support location.

Will vendor require VPN? * ○ Yes ○ No Is site-to-site VPN required? * ○ Yes ○ No *Vendor required to fill out request form

Does vendor use own remote access tool? * ○ Yes ○ No If yes, identify remote access tool used Identify remote access tool(s) used.
* Review required; subject to approval of ISD

Are there ports/protocols required to be open for support or VPN access? ○ Yes ○ N/A

List ports and protocols List ports and protocols required.

Does the vendor provide maintenance procedures? ○ Yes ○ No

How often are patches/upgrades/maintenance performed on the system?

Indicate how often system maintenance performed.

Will vendor notify County at least 2 weeks in advance for maintenance? ○ Yes ○ No

Is there anticipated downtime related to upgrades or maintenance? ○ Yes ○ No

Is there a strategy including methodology for upgrading the infrastructure to ensure technology advances and security? ○ Yes ○ No

Section 7: References

Password Policy

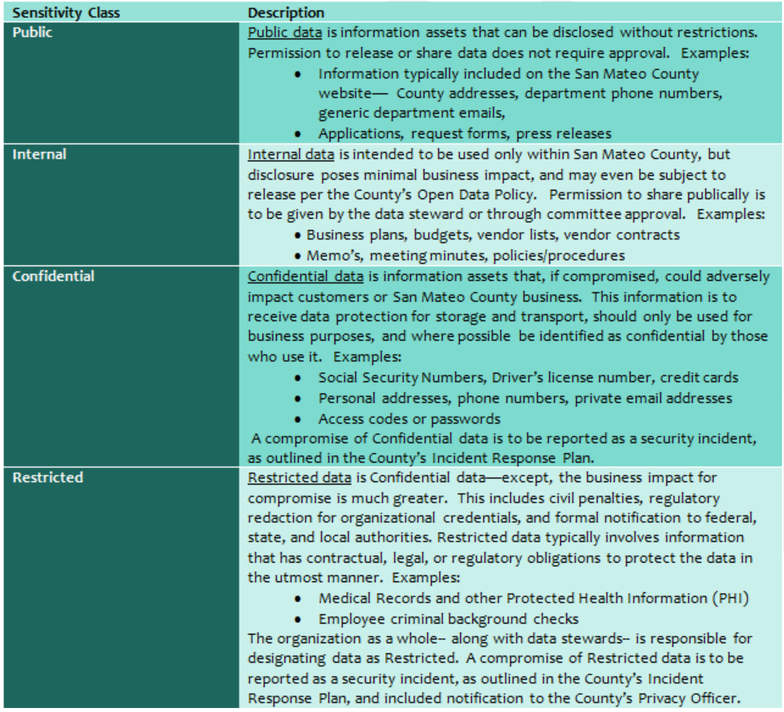
The County of San Mateo's Information Security Policy requires new technology implementations that use passwords to adhere to the following password requirements:

County of San Mateo Password Requirements

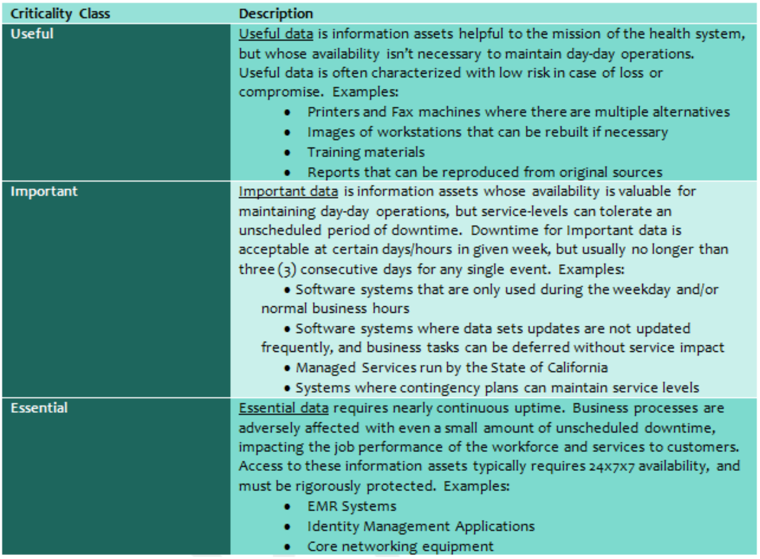
1. All users must have unique account IDs that identifies a single account owner
2. First time password must be unique to an individual, and require change upon initial login
3. The permanent / long term password requires an enforceable change every 60 days
4. The password must enforce a minimum of at least 8 characters, and contain at least one character from *three* of the following:
   a. Lower Case
   b. UpperCase
   c. Numbers
   d. Special Characters
5. Password may not be reused – system is configured to remember last 12 passwords

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 2, 'Product Information'.



Sensitivity Class	Description
Public	Public data is information assets that can be disclosed without restrictions. Permission to release or share data does not require approval. Examples: • Information typically included on the San Mateo County website— County addresses, department phone numbers, generic department emails, • Applications, request forms, press releases
Internal	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 publically is to be given by the data steward or through committee approval. Examples: • Business plans, budgets, vendor lists, vendor contracts • Memo's, meeting minutes, policies/procedures
Confidential	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: • Social Security Numbers, Driver's license number, credit cards • Personal addresses, phone numbers, private email addresses • Access codes or passwords A compromise of Confidential data is to be reported as a security incident, as outlined in the County's Incident Response Plan.
Restricted	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: • Medical Records and other Protected Health Information (PHI) • Employee criminal background checks 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.



Criticality Class	Description
Useful	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: • 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
Important	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: • 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
Essential	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: • EMR Systems • Identity Management Applications • Core networking equipment

Section 8: 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/mitigation, if any.

NOTE: All non-compliance must file an Information Security Risk Acceptance Form

Please explain all areas of non-compliance as well the mitigation or remediation.

Section 9: Other Documents

Please include any pertinent documents, diagrams of network, and/or data flow architecture. Please note other documents may be requested.

Documents included? ○ Yes ○ No

Network Diagrams * required ○ Yes ○ No

Data flow diagram * required ○ Yes ○ No

Other security documents ○ Yes ○ No

This assessment was prepared by (Print Name) ______________________________

Signature ______________________________

Date ____________________

Phone ____________________