



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 NCRIC

Submitter's Name Brian Rodrigues

Phone 415-710-9702

### Section 1: Vendor Information

Name: Forensic Logic, LLC Corporate Phone #: 1-833-267-5465  
Address: 1255 Treat Boulevard, Suite 610 City: Walnut Creek State: CA ZIP: 94597

Technical Support Contact Methods: ☒ Phone: 1-833-267-5465 ☐ IM/Chat   
(Select all that apply) ☒ Email: support@forensiclogic.com ☐ Web Portal

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

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

Nancy Keena  
nkeena@forensiclogic.com  
520-437-3823

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? Yearly

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

We are FIPS 140-2 compliant, but not certified.

### Section 2: Product Information

Product Name: COPLINK

No. of Users: >100

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.

COPLINK is a lead generation tool for Law Enforcement.

**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

We are currently utilizing the email system for alerts.

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 breach and mitigation efforts.

Known Vulnerabilities?

☐ Yes ☒ No

Please describe known vulnerabilities here.

For details on Data Sensitivity and Data Criticality, please see the Section 6 References of this document

Data Sensitivity: ☐ Public ☐ Internal ☐ Confidential ☒ Restricted

Data Criticality: ☐ Useful ☒ Important ☐ Essential

### 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

Please provide additional detail on configuration and system hardening.

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

☒ Yes ☐ No

We provide these features which we are contractually obligated to provide.

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:

Monthly

Retention period

90 days

Encrypted?

☐ Yes ☒ No

When stored?

On the local SAN

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

What assurance is provided for complete removal?

We can provide certification that the data was destroyed.

### 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.

We have an in-house monitoring tool that tracks performance levels of the application.

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.

Security fixes are as needed and updates as required per contractual obligations.

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?

If hosted, please enter detail here on patching.

**Anti-Virus Protection:** Is anti-virus 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

Anti-virus is provided by the County.

**Employees:** Have employees undergone a background check process?

☒ Yes ☐ No

Will the provider use a subcontractor or 3<sup>rd</sup> 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.

**SaaS:** Is the product 100% web-based?

☐ Yes ☐ No

What are the browser security configuration requirements?

Please describe 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

Please provide location.

Is there a disaster recovery plan in place?

☐ Yes ☐ No



**Identity and Authentication Management:**

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

**Note: SAML is the preferred choice for integration with San Mateo County systems**

☒ Yes☐ No

If yes,  
please specify

☐ SAML☐ OAuth☐ MFA☒ Active Directory☒ LDAP☒ Other

If other, please indicate.

**Password Management:**

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

The Node Administrators handle this. Items 2-4 below are up to the County; COPLINK has the capability.

Does the product provide for password management that meets the County password policy for complexity, expiration, reuse, and lockout? **See Section 6 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

Does the product provide for password self-reset capability?

☐ Yes ☒ No

How are passwords stored?

Encrypted HASH inside the database.

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

Different levels of user privileges.

**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

Data is encrypted through secure SFTP.

Data-in-use

AES 128

Data-at-rest

Data is not encrypted at rest.

Credentials

User names and passwords, SQL authentication and SFTP

+

**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, dataexport, and permission changes.

☒ Yes ☐ No

Auditing through the Admin module to which the Node Administrators have access.

## 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.

Please enter location(s) here.

**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 details here.

**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 describe platform here.

**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

Please provide additional detail including names of vendors.

**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 here.

**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 here.

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

☐ Yes☐ No

If yes, please provide additional details.



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

☐ Yes ☐ No

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

**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

If yes, please provide additional details.

## 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 2, 'Product Information'.

Sensitivity Class	Description	Criticality Class	Description
Public	<p><b>Public data</b> 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"> <li>Information typically included on the San Mateo County website— County addresses, department phone numbers, generic department emails,</li> <li>Applications, request forms, press releases</li> </ul>	Useful	<p><b>Useful data</b> 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"> <li>Printers and Fax machines where there are multiple alternatives</li> <li>Images of workstations that can be rebuilt if necessary</li> <li>Training materials</li> <li>Reports that can be reproduced from original sources</li> </ul>
Internal	<p><b>Internal data</b> 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"> <li>Business plans, budgets, vendor lists, vendor contracts</li> <li>Memo's, meeting minutes, policies/procedures</li> </ul>	Important	<p><b>Important data</b> 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"> <li>Software systems that are only used during the weekday and/or normal business hours</li> <li>Software systems where data sets updates are not updated frequently, and business tasks can be deferred without service impact</li> <li>Managed Services run by the State of California</li> <li>Systems where contingency plans can maintain service levels</li> </ul>
Confidential	<p><b>Confidential data</b> 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"> <li>Social Security Numbers, Driver's license number, credit cards</li> <li>Personal addresses, phone numbers, private email addresses</li> <li>Access codes or passwords</li> </ul> <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><b>Essential data</b> 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"> <li>EMR Systems</li> <li>Identity Management Applications</li> <li>Core networking equipment</li> </ul>
Restricted	<p><b>Restricted data</b> 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"> <li>Medical Records and other Protected Health Information (PHI)</li> <li>Employee criminal background checks</li> </ul> <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/mitigation, if any.

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

Please explain areas of non-compliance.

## Section 8: Other Documents

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

Documents included? ☒ Yes ☐ No

# Information Security Risk Acceptance Form

*Instructions: Fill out all portions of the form applicable. If you require more space, please attach your responses to this form. Once finished, please send this form to the Information Security Officer – ISD – Stormy Maddux.*

**Vendor Name:** \_\_\_\_\_

**Departmental Contact Information:**

Name and title of Originator: \_\_\_\_\_

Email and Phone Number of Originator: \_\_\_\_\_

Policy/Standard/Guideline you are requesting an exception from:

Summary of the request:

Overview of the service/system impacted:

Risk Classification:

**LOW**

**MEDIUM**

**HIGH**

Does the application/service for which the security exception applies store, process, transmit, or use any of the following types of data in any way?

	Yes	No
Social security numbers		
Driver's license numbers or state identification numbers (for CA or any state)		

Visa or passport numbers or related data		
County employee records		
Credit or debit card numbers		
Credit card transaction approval data		
Personal health information (whether included in medical records or otherwise)		
Banking account or other financial account numbers and/or access codes or passwords for the County of San Mateo or any other person or entity		
Computer user names and/or passwords		
Personal contact data for County workforce, business partners, or members of the public		

If you answered “yes” to any of the above items, please provide a brief explanation of how the data is used in the application/service:

Benefits of accepting this risk:

Describe the impact to the system/project/users if the risk is not accepted:

Describe mitigating controls in place:

After controls what is the remaining risk and what is the risk level:

**Risk Acceptance Request:**

I understand that compliance with County policies and standards is expected for all workforce members, departments, organizational units, information systems, and communication systems. The service, application or business owner is seeking a risk acceptance decision for the following deployment.

I accept responsibility for the risk associated or created by the exception described above. I also understand that this exception is temporary and will work to implement the plan to ensure compliance in the future.

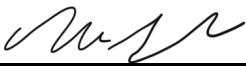
Signed by: \_\_\_\_\_, Service or Business Owner

Department: \_\_\_\_\_

Signature Date: \_\_\_\_\_

---

Signed by: \_\_\_\_\_, Department/Agency Head

Signature Date:  \_\_\_\_\_

---

Signed by: \_\_\_\_\_, Information Security Officer

Signature Date: \_\_\_\_\_

**Date of Next Review:** \_\_\_\_\_ (AT LEAST ANNUAL)



## Appendix A

### Criticality Matrix

	<b>Most Critical</b> <i>Highest level of sensitivity</i>	<b>Critical</b> <i>Moderate level of sensitivity</i>	<b>Least Critical</b> <i>Very low, but still requiring some protection</i>
<b>Legal Requirements</b>	Protection of data is required by law (e.g., HIPAA and Criminal Justice data elements and other personal identifying information protected by law)	The institution has a contractual obligation to protect the data	
<b>Reputation Risk</b>	High	Medium	Low
<b>Other Institutional Risks</b>	Information that provides access to resources, physical or virtual	Smaller subsets of Most Critical data from a department	
<b>Data Examples</b>	<ul style="list-style-type: none"> <li>• Medical</li> <li>• Criminal Justice</li> <li>• Prospective employee</li> <li>• Personnel</li> <li>• Financial</li> <li>• Contracts</li> <li>• Physical plant detail</li> <li>• Credit card numbers</li> <li>• Certain management information</li> <li>• Personally identifiable information</li> </ul>	<ul style="list-style-type: none"> <li>• Information resources with access to Most Critical data</li> <li>• Financial transactions that do not include Most Critical data (e.g., telephone billing)</li> <li>• Unidentifiable small subsets of Most Critical data</li> </ul>	<ul style="list-style-type: none"> <li>• Personal directory data (e.g., contact information)</li> <li>• E-mail</li> <li>• Institutionally published public data</li> </ul>