

# 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: Forensic Logic COPLINK

## Departmental Contact Information:

Name and title of Originator: NCRIC Assistant Deputy Director, Brian Rodrigues

Email and Phone Number of Originator: brodrigues@ncric.ca.gov 415-710-9702

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

Password Management, 60 day rotation requirement

### Summary of the request:

COPLINK has no technical capability to enforce 60 day password lifespan and rotation.

### Overview of the service/system impacted:

COPLINK, hosted at and maintained by the NCRIC

### 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:**  
 Continued use of COPLINK application to support regional law enforcement access to, and analysis of, shared criminal history data. Coplink is used by hundreds of agencies statewide to help identify suspects and solve cases.

**Describe the impact to the system/project/users if the risk is not accepted:**  
 Coplink is a crucially important tool for many crime analysts and investigators. Though we plan to migrate to a newer platform later this year, we need a final term to handle that transition without abandoning users.

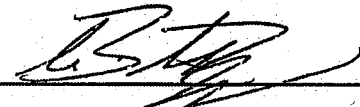
**Describe mitigating controls in place:**  
 Active removal of expired accounts, and limiting new access to the system.

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

**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.

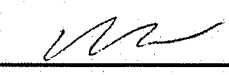
Signed by: , Service or Business Owner

Department: NCRIC

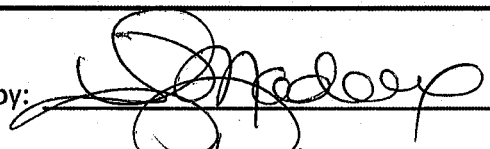
Signature Date: 1/10/20

---

Signed by: Mike Sena, Department/Agency Head

Signature Date: 

---

Signed by: , Information Security Officer

Signature Date: 1/16/2020

---

Date of Next Review: 1/15/2021 (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>