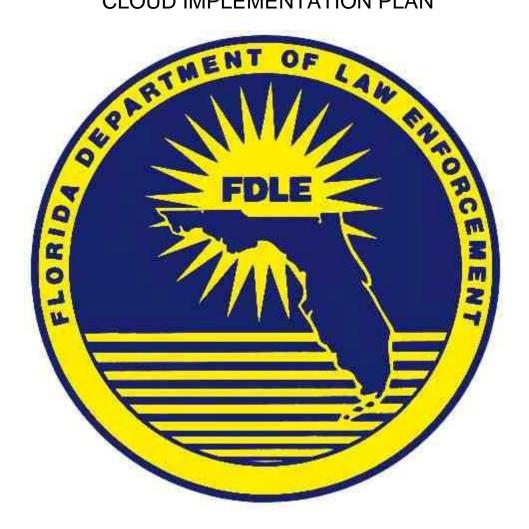
FLORIDA DEPARTMENT OF LAW ENFORCEMENT CRIMINAL JUSTICE INFORMATION SERVICES

CLOUD IMPLEMENTATION PLAN



AGENCY:

ORI:

AGENCY CONTACT:

PROJECT NAME:

The cloud subscriber (user, agency, tenant,) should be aware of security and legal requirements prior to entering into any agreement with a cloud service provider. The following general questions will help frame the process of determining compliance with the existing requirements of the CJIS Security Policy. Agencies must submit an updated network diagram along with the completed form. If you need additional space for answers, please attach a separate document.

Please answer the following questions:

- 1. What cloud service provider do you plan to use?
- 2. If applicable, who is the Lead Agency?
- 3. What product (s) or services do you plan to use?
- 4. What platform (s) do you plan to use? (laaS, PaaS, SaaS)
- 5. Will access to Criminal Justice Information (CJI) within a cloud environment fall within the category of remote access?
- 6. Will advanced authentication (AA) be required for access to CJI within a cloud environment?
- 7. Does/do any cloud service provider's datacenter(s) used in the transmission, storage, or processing of CJI meet all the requirements of a physically secure location?
 - What is the physical location(s) of the data center CJI will be stored in the cloud?
 - Has a site visit been conducted by your agency or the lead agency?
- 8. Are the encryption requirements being met?
 - Who will be providing the encryption as required in the CJIS Security Policy (client or cloud service provider)? Note: individuals with access to the keys can decrypt the stored files and therefore have access to unencrypted CJI.

2

Will the data be encrypted while at rest and in transit?

August 2019

Will the cloud subscriber be notified of any incident?
If CJI is compromised, what are the notification and response procedures?
10. Is the cloud service provider a private contractor/vendor? If so, they are subject to the same screening and agreement requirements as any other private contractors hired to handle CJI.
11. Will the cloud service provider allow the CSA and FBI to conduct compliance and security audits?
Note: Cloud facilities such as datacenters in which CJI will be stored or processed should be audited as would any other datacenter storing and/or processing CJI.
12. How will event and content logging be handled?
 Will the cloud service provider handle the event and content logging required by the CJIS Security Policy and provide that upon request?
 What are the cloud service provider's responsibilities with regard to media protection and destruction?

3

August 2019

9. What are the cloud service provider's incident response procedures?