FLORIDA DEPARTMENT OF LAW ENFORCEMENT CRIMINAL JUSTICE INFORMATION SERVICES

CLOUD IMPLEMENTATION PLAN

AGENCY: Alachua County Court Services

ORI: FL001023G

AGENCY CONTACT: Louis A. Morales LASO

PROJECT NAME: Court Services Office 365 SaaS No CJIS/HIPAA Cloud Storage

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?

   Microsoft Azure Government

2. If applicable, who is the Lead Agency?

   Florida Department of Law Enforcement (FDLE)

3. What product (s) or services do you plan to use?

   Microsoft Office 365

4. What platform (s) do you plan to use? (IaaS, PaaS, SaaS)

   SaaS Software as a service. Office 365 from Microsoft Government CJIS AZURE Government.

5. Will access to Criminal Justice Information (CJI) within a cloud environment fall within the category of remote access?

   No CJI in the cloud. It will stored on Court Services SAN (Storage Area Network) behind the firewall.

6. Will advanced authentication (AA) be required for access to CJI within a cloud environment?

   N/A

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?

   Yes meets 5.10.1.2.1 Encryption for CJI in Transit

   - What is the physical location(s) of the data center CJI will be stored in the cloud?

     Court Services will be using Office-365 from the Microsoft Azure Government. Located in the Continental US.

   - Has a site visit been conducted by your agency or the lead agency?

     Yes by the Lead Agency-FDLE.

8. Are the encryption requirements being met?

   Yes they meet as minimum FIPS 140-2 Certified and use a symmetric cypher key strength of at least 128 bit strength to protect CJI in Transit https://docs.microsoft.com/en-us/compliance/regulatory/offering-fips-140-2

   - 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.*

     The application will be encrypted by Microsoft Government CJIS Cloud to Court Services network. https://docs.microsoft.com/en-us/compliance/regulatory/offering-fips-140-2

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

     The Data files for Microsoft 365 will be stored on the County SAN with access controlled by Active Directory and Vetted staff that meet CJIS requirements. They will be encrypted in transit to meet CJIS 5.10.1.2.1.

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

   There we be no CJIS or HIPAA data on the cloud and will be stored on Court Services part of the County SAN.

   - 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.

    The Cloud Vendor is Microsoft Azure Government and has been vetted by the Lead Agency-FDLE

11. Will the cloud service provider allow the CSA and FBI to conduct compliance and security audits?

    Yes - The Lead Agency-FDLE

    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?

    We will handle event and content logging using Corner Bowl to meet CJIS requirements

    - Will the cloud service provider handle the event and content logging required by the CJIS Security Policy and provide that upon request?

      Court Services meets this requirement for the internal network.

    - What are the cloud service provider's responsibilities with regard to media protection and destruction?

      No CJIS or HIPAA files will be maintained in the cloud.