|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Vendor Name:** | | | | **Completed by:** | **Date Completed:** |
| **Date Updated:** |
| **Reviewed by (HHS/DOM DoIT Use Only):** | | | | | |
| **Describe all areas of the vendor’s environment in which HHS data (hardcopy or softcopy) will be accessed, stored and/or processed (email, network shares, cloud, etc.):** | | | | | |
| **Describe the flow of data through the vendor’s environment:** | | | | | |
| **Question** | | | | **Response** | |
| **Data Protection** | | | | | |
|  | | In what geographic location(s) will HHS data be stored? |  | | |
|  | | From what geographic location(s) will vendor support be provided? |  | | |
|  | | How does the vendor detect changes to the integrity or availability of HHS data and what measures are in place to ensure HHS data is not lost, modified or destroyed? |  | | |
|  | | Define a security incident. |  | | |
|  | | Describe the vendor’s incident response and reporting program. How does the vendor report incidents to HHS? |  | | |
| **Cloud Service Providers** | | | | | |
|  | Will HHS data be stored in the cloud? | | |  | |
|  | Who is the cloud service provider? | | |  | |
|  | Is the cloud service provider FedRAMP authorized and if so, what impact level? | | |  | |
| 1. 1 | If not FedRAMP authorized, specify the security framework for which the cloud service provider is certified. | | |  | |
| **Access Control** | | | | | |
|  | Who has access to the systems providing HHS data and services? How is this access controlled? | | |  | |
|  | What authentication method is required to access HHS data and applications (e.g. username and password)? | | |  | |
|  | Which multi-factor authentication methods does the vendor support? | | |  | |
|  | Does the vendor allow the use of personal devices for access to HHS data? Do you monitor for unauthorized devices on the network? | | |  | |
|  | Does the vendor allow remote access? If so, how is this managed? | | |  | |
|  | Specify the frequency vendor staff access to HHS data is reviewed. | | |  | |
|  | Which access control methodology does the vendor support: Role-based access control (RBAC), mandatory access control (MAC), or discretionary access control (DAC)? Define how you meet this methodology. | | |  | |
| **Regulatory Compliance** | | | | | |
|  | Is the vendor a HIPAA covered entity? | | |  | |
|  | Is the vendor a business associate of HHS? If yes, does the vendor have downstream business associate agreements with subcontractors? | | |  | |
|  | Define the vendor’s HIPAA training. How frequency are vendor staff trained? | | |  | |
|  | Define the vendor’s security awareness training. How frequent are vendor staff trained? | | |  | |
|  | Is the vendor audited or assessed by a third party? If yes, specify the security framework. | | |  | |
|  | Explain how the vendor performs an information security risk assessment. What is the frequency? | | |  | |
|  | Explain how the vendor manages their information security risk assessment program. | | |  | |
| **Business Continuity and Resiliency** | | | | | |
|  | Does the vendor have a business continuity plan? | | |  | |
|  | How often is the business continuity plan tested? | | |  | |
|  | How does the vendor ensure HHS can continue doing business at all times, even if there is a catastrophic failure or natural or man-made disaster where HHS data or services are located? | | |  | |
|  | What guarantees does the vendor provide for recovery time objectives (RTO) and recovery point objectives (RPO)? | | |  | |
| **Service and Data Integrity** | | | | | |
|  | Is HHS data encrypted in transit? If so, specify the encryption algorithm and cipher strength.  Who owns the encryption key? | | |  | |
|  | Is HHS data encrypted at rest? Is so, specify the encryption algorithm and cipher strength.  Who owns the encryption key? | | |  | |
|  | Are all devices used by vendor staff to access HHS information encrypted? Describe encryption methodology. | | |  | |
|  | Specify the network security tools used to monitor data flow into the vendor’s network for malware or cyber-attacks. | | |  | |
|  | What tools and procedures does the vendor utilize for intrusion detection and at what frequency? How is this capability tested for functionality at the hardware, network, and database levels? | | |  | |
| **Multi-Tenancy** | | | | | |
|  | How does the vendor separate HHS data and services from those of other clients? | | |  | |
|  | In what ways could the vendor’s other client’s affect the quality of the service or service levels provided to HHS? | | |  | |
|  | What resources will HHS share with other clients? | | |  | |
| **Infrastructure and Application Security** | | | | | |
|  | Who owns and operates the vendor’s data centers and what physical and environment security measures are in place? | | |  | |
|  | What parts of the vendor’s infrastructure are owned and operated by the vendor and what parts are obtained from a colocation service? | | |  | |
|  | What standards are followed for hardening network equipment, operating systems, and applications? | | |  | |
|  | Specify the tools used to perform vulnerability scans and the frequency. What is the timeframe to re-mediate high and critical findings? | | |  | |
|  | Specify the frequency of third-party penetration tests to assess infrastructure security. Include the type of third-party report received. | | |  | |
|  | What specifications does the vendor follow to purge data when equipment is retired or replaced? How does the vendor purge any resident HHS data? | | |  | |
|  | Does the vendor utilize a web application for this service? If so, does the vendor follow the OWASP Top 10 List? | | |  | |
| **Non-production Environment Exposure** | | | | | |
|  | Is production HHS data loaded to a test environment? | | |  | |
|  | How is the production data de-identified? | | |  | |