NM DEPARTMENT OF INFORMATION TECHNOLOGY

System Hosting Evaluation Questionnaire

FORM 22-361-EPMO-2

DATE:

AGENCY CODE: AGENCY NAME:

PROJECT NAME:

Questionnaire

1. Briefly describe the project's business need, project objective, and planned technical approach.

2. Will the proposed solution be hosted in a government-certified cloud? If not, include the type of cloud, such as commercial, private, or hybrid.

3. Who will have administrator access to the architecture and/or application, if applicable?

4. Describe the controls and process for administrator access.

5. Describe the different security measures defined for the solution such as user access, roles-based security, data access, and file access.

6. Is any of the following sensitive personal information collected, stored in the database, presented to users, and/or encrypted at rest/transit? Please enter **Y** (Yes) or **N** (No) for each of the associated data.

   In the last column, enter the acronym of the associated compliance category if applicable.

   Protected Health Information **(PHI)**
   Family Medical Leave Act **(FMLA)**
   Payment Card Industry-Data Security Standard **(PCI-DSS)**
   Health Insurance Portability & Accountability Act **(HIPAA)**
   Other, describe in additional rows below
   Federal Tax Information **(FTI)**
   Americans with Disabilities Act **(ADA)**
   Protection of Pupil Rights Amendment **(PPRA)**
   Family Education Rights & Privacy Act **(FERPA)**

Confidential or Protected Data	Collected	Stored in Database	Displayed	Encrypted at Rest	Encrypted During Transit	Confidentiality Law or Contract Provision
First & Last Name						
Date of Birth						
Address						
Social Security No.						
Driver's License No.						
Credit / Debit Card No.						
Checking / Savings Acct. No.						
Password						
Other						

7. Has agency general counsel confirmed that no law or agreement prohibits cloud storage or transit of any of the protected data to and/or from the cloud?

8. Does any law or agreement specify security protocol applicable to cloud storage or transit of any of the protected data?

9. Is intrusion detection in place for the solution? If yes, describe.

10. Are there firewalls, access control language (ACL), or virtual devices in place for separation of presentation, business and/or data layers of the proposed solution? Who is responsible for managing them? If none of the above are in place, describe why they are not required.

11. If the solution is SaaS, is there a Web Application Firewall (WAF)? If so, list what is defined in your Security Operations Center (SOC). If there is no WAF, describe why it is not required?

12. Does your solution have any batch processing? If so, explain the security measures defined.

    a. Who administers the batch process?

    b. Describe the controls and processes for creating and managing Service Accounts that are used for your batch process to access data and files.

13. Will your solution have a need to connect to the New Mexico state infrastructure for any data exchange? If so, explain.

    a. Describe the exchange mechanism for example, direct Structured Query Language (SQL) connection, Application Program Interface (API), Comma Separated Value (CSV) file, etc.).

    b. What security channel will be used for example, HTTPS, VPN, IP whitelist, etc.?

14. Describe your plans to monitor and review security logs/alerts and please identify the name and title of your agency's individual(s) who will be delegated for this task.

15. Describe identity management for example, username/encrypted password, dual-factor-athentication and/or biometric, etc. for your solution.

16. Describe encryption key management (if any) for your solution.

17. List the environments that your solution will include for example, development/test/staging. Do the security controls covered in questions 3, 4, 5, 6, 9, 10, 11, 12, 13, and 15 apply to these environment(s)? If not, explain why.

The completed Questionnaire and the following items must be emailed to exception.requests@doit.nm.gov:

1. A System Architecture Document that includes a summary of the software architecture and different tiers/layers for example, database, application, business, and presentation that are included in the solution.
2. A diagram with a written description that illustrates the platforms, networks, peripherals, hardware integration, and separation of database, application, business, and presentation tiers/ layers.
3. An independent security assessment report of the solutions and application, if applicable. If an assessment has not been conducted, please provide an estimated date for when it will be done.

Funding Type

☐ General Fund ☐ Federal Funds ☐ Other State Funds

Description	Initial	Recurring			
	FY23	FY24	FY25	FY26	Total
					0.00
					0.00
					0.00
Total	0.00	0.00	0.00	0.00	0.00

Agency Contact(s) for Additional Information

Name: Title:

Phone: Email:

Name: Title:

Phone: Email:

Agency Approvals

Agency Cabinet Secretary/Agency Director

Agency Date

Agency Chief Information Officer/IT Lead

Agency Date

For Department of Information Technology (DoIT) Use Only

Recommendation:

Decision by DoIT

☐ APPROVED ☐ DISAPPROVED

DoIT Cabinet Secretary or Designee