Maryland
DEPARTMENT OF
INFORMATION TECHNOLOGY

Office of Security Management

Vendor Risk Assessment Questionnaire Form: Offshore Resource Utilization

Table of Contents

Purpose 4

Compliance Requirements 4

Revision Control History

Version	Author(s)	Date	Description
1.0.0	Miheer Khona	May 1, 2025	Initial Version

Purpose

The Vendor Risk Assessment Questionnaire: Offshore Resource Utilization form is required for any current or new vendors that are generating, receiving, storing, processing or transmitting State data, whether the system is hosted on the State network or by a third-party provider. This is a supplemental form for the Emergency Directive 2025-01-05 – Prohibited Offshore Resources, Personnel, Contractors.

Compliance Requirements

This form must be submitted for any request for products or services that include offshore resources to the Office of Security Management by emailing the GRC Team at doit.grc@maryland.gov.

Vendor Risk Assessment Questionnaire Form: Offshore Resource Utilization

Vendor / Contractor Information:

- Vendor Name:
- Vendor Address:
- Contact Person:
- Contact Email:
- Contact Phone:

I. Offshore Resource Details

1. **Location(s) of Offshore Resources:**
   - List all countries and specific locations where offshore resources are based or from which they operate.
2. **Function of Offshore Resources:**
   - Provide a detailed description of the specific functions performed by offshore resources as defined by “EMERGENCY DIRECTIVE 2025-01-05 Prohibited Offshore Resources, Personnel, Contractors”.
   - Specify which State of Maryland systems, applications, or data the offshore resources will interact with.
3. **Offshore Resource Access:**
   - Provide system name, a detailed justification outlining the necessity and the specific data or applications involved where access is required. Note that this questionnaire requires a waiver approval from the State CISO upon completion of an offshore resource risk assessment.
4. **Data Classification:**
   - Identify the types of data that will be accessed or processed by offshore resources.
   - Specify the classification level of the data according to the Maryland Data Classification Policy (e.g., public, protected internal only, confidential, or restricted, etc.).
5. **Data Processing Activities:**
   - Describe all data processing activities that offshore resources will perform.

     This includes, but is not limited to:

     - Collection
     - Recording

- Organization
- Structuring
- Adaptation or Alteration
- Retrieval
- Consultation
- Use
- Storage (prohibited)
- Disclosure by Transmission
- Dissemination
- Making Available
- Alignment or Combination
- Restriction
- Erasure
- Destruction

II. Security Controls and Compliance

1. **Non-Disclosure Agreement (NDA):**
    - Does a formal Non-Disclosure Agreement, confidentiality agreement, and data use agreement exist between the State and vendor(s) / contractor(s) and/or sub-contractor(s) that specifically covers the offshore resources and their handling of State of Maryland data? (Yes / No)
    - If "Yes," provide a copy of the agreement(s).
2. **IT Security Manual Controls:**
    - Does the organization have any security certifications (e.g., ISO 27001, etc.)?
    - Detail how the security controls from the State of Maryland IT Security Manual are applied to the offshore resources and their activities.
    - Provide evidence or documentation demonstrating the implementation and

effectiveness of these controls.

3. **SOC 2 Type II Report:**
    - Does the vendor have a current SOC 2 Type II report? (Yes / No)
    - If "Yes," provide a copy of the report, including third-party and subcontractor reports if applicable.
4. **Criminal Background Checks:**
    - Does the vendor conduct criminal background checks on contractors and employees who have access to State of Maryland data? (Yes / No)
    - If "Yes," describe the process and the scope of the background checks.

III. Risk Assessment and Management

1. **Risk Assessment:**
    - Were vendors that have resources on-shore (i.e., U.S.) considered? (Yes / No)
    - If “Yes,” provide detailed rationale for selection of vendor(s) with off-shore resources.
    - Has the unit of State government conducted a formal vendor risk assessment specific to the use of offshore resources for this project or service? (Yes / No)
    - If "Yes," provide a summary of the risk assessment findings, including identified risks, likelihood, impact, and mitigation measures.
2. **Incident Response:**
    - Describe the unit of State government’s incident response plan for security incidents involving offshore resources, including how the unit of State government will ensure timely notification to the State of Maryland.
3. **Data Security and Privacy:**
    - Detail the measures in place to protect the confidentiality, integrity, availability, accuracy and currentness of State of Maryland data processed or accessed by offshore resources.
    - Describe how the unit of State government will ensure compliance with relevant data privacy regulations.
    - Has a privacy threshold, and, if personal information is processed, a privacy impact assessment been completed?
4. **Monitoring and Audit:**
    - Explain how the unit of State government will monitor the activities of offshore resources and audit their compliance with security policies and procedures.

IV. Attestation

- I attest that the information provided in this questionnaire is accurate and complete to the best of my knowledge.
- I acknowledge that any misrepresentation or omission may be in violation of the Maryland Procurement Code. I understand that any false information or omission may result in the immediate termination of any agreement or contract with the State of Maryland agencies.

VENDOR:

Signature: _____

Printed Name: _____

Vendor: _____

Title: _____

Date: _____

MARYLAND AGENCY:

Signature: _____

Printed Name: _____

Agency Authority / Designee: _____

Title: _____

Date: _____