MISSISSIPPI STATE DEPARTMENT OF HEALTH

MSDH
Vendor Risk Management (VRM) Policy

Overview

The Mississippi Department of Health (MSDH) forms partnerships with third-party vendors to maximize operational efficiency and deliver services to our customers, partners, and stakeholders. While these vendors offer valuable support and services to our agency, they are also a source of risk, and MSDH must utilize available resources to ensure we have taken all reasonable precautions to protect our operations and public health from supply chain risks.

Purpose

This policy establishes baseline principles for selecting and onboarding vendors providing IT services, require network access to MSDH, or require a badge to physically access MSDH, to indefinitely protect MSDH's interests, property, and data throughout the vendor lifecycle.

This policy is applicable to any vendors providing IT products and/or services to MSDH. This policy is effective once approved by the agency for new contracts entered. For all previous agreements entered prior to this policy, MSDH will be required to add this policy at the renewal period.

Definitions

- Vendor: A company/individual that provides an IT product/service for MSDH, or requires remote network access to MSDH, and/or requires badge access to MSDH facilities.
- Vendor Matrix: A tiered system based on the level of criticality associated with the outsourced products/services. MSDH ranks vendors on a scale of 1 to 4, where 1= critical risk and 4= low risk
- Compliance Risks: Risks associated with vendors mishandling the personally identifiable information (PII), or electronic protected health information (ePHI) of customers, the public, and/or employees
- Reputation Risks: Risks associated with vendors violating laws and/or regulations that lead to public enforcement actions
- Operational Risks: Risks related to failed processes, system outages, or data losses that result in privacy issues, business or service interruptions, etc.

Scope

This policy applies to all employees at MSDH, and the standards within this policy regulate all existing and new third-party vendors partnerships MSDH has formed or will form.

Policy

MSDH effectively manages the lifecycle of all vendor relationships to responsibly administer resources and minimize the inherent risk associated with third-party services.

MSDH's vendor management program consists of the following:

1. Vendor Risk Assessment
2. Vendor Monitoring
3. Vendor Due Diligence and Remediation
4. Vendor Offboarding

1. Vendor Risk Assessment

MSDH evaluates all potential vendors by conducting an initial risk analysis. This risk analysis should utilize MSDH's Vendor Matrix to assign each vendor to one of four risk tiers (Critical-1, High-2, Medium-3, or Low-4). Vendors receive risk tiers based on the highest risk level attributable to that vendor.

Monitoring & Risk Management

- Risk personnel must monitor all third-party vendors using UpGuard VendorRisk
- Risk personnel must enable automated notifications to alert MSDH if a vendor's risk score drops below 600 (Tier 4), 650 (Tier 3), 700 (Tier 2), or 800 (Tier 1) depending on vendor Tier Rank.
- If a Tier 1, 2, or 3 vendor drops below the acceptable threshold, risk personnel must conduct a risk assessment and note it on the risk register
- The Vendor must provide a technical or security point of contact and agree to remediate or submit a risk waiver for risks detected by UpGuard's scanning alerts.
- Risk personnel will send Tier 1 and 2 vendors annual risk assessments.
- Significant changes in score need to be recorded on the risk register and discussed at the monthly Information Security Management Council (ISMC) meeting.

Labels

All vendors in VendorRisk must have labels that reflect the following information:

- Vendor internal owner(s)
- Department(s) or Program Area(s) using the vendor
- Level of risk
- Data types they process - Business Data, Customer Data, Personal Data, PII, ePHI, etc.
- Whether they have Network, API, or Physical Access to MSDH systems
- Payment terms and renewal date of the contract

Vendor Records

All vendors should contain the following information:

- Contract
- Vendor risk assessment (where applicable)
- Vendor Account Management Contact
- Vendor Security or Technical Contact

Organization Considerations

- Personnel should leverage vendor portfolios to streamline vendor intake. MSDH maintains portfolios for "Evaluating Vendors" that can help personnel separate considered vendors from the rest of the vendor pool
- Colleagues who could benefit from seeing vendor data but aren't directly involved in vendor evaluations should receive "read-only" access to relevant vendor portfolios. Employees can use the existing Access Request Form to request "read-only" access to UpGuard

Table 1: Vendor Tiering Matrix			
Tier	Description	Definition	Acceptable Score
1	Critical	• High Operational (IT Availability), AND Financial, AND Reputational (IT Integrity), AND Regulatory (IT Confidentiality) Risk. OR • Loss of vendor services/resources for greater than 12 business hours will significantly inhibit the agencies mission. OR • Lack of supply chain resiliency limits MSDH actions upon breach (Sole Source Contract, Limited Alternative Vendors). OR • Loss of service provided can reasonably be expected to impact public health and may lead to unnecessary injury or death. OR • Any system required for MSDH's COOP/DR or defined by the SHO as a critical system. • Generally assessed annually and monitored continually.	>800

2	High	• High Operational (IT Availability), OR Financial, OR Reputational (IT Integrity), OR Regulatory (IT Confidentiality) Risk. AND
		  • Loss of vendor services/resources for greater than 48 business hours may significantly inhibit the agencies mission. AND
		  • Vendor has 2-4 competitors in the space able to support MSDH. OR
		  • Loss of service provided may impact public health and may lead to unnecessary injury or death.
		• Generally assessed annually and monitored periodically.
			>700

3	Medium	• Some Operational (IT Availability), AND Financial, AND Reputational (IT Integrity), AND Regulatory (IT Confidentiality) Risk. OR • Loss of vendor services/resources for greater than 5 business days will inhibit a program area's mission. AND • MSDH has alternative sources which can be readily leveraged. • Generally assessed every two years.	>650
4	Low	• Some Operational (IT Availability), OR Financial, OR Reputational (IT Integrity), OR Regulatory (IT Confidentiality) Risk. OR • Loss of vendor services/resources for greater than 5 business days will inhibit a program area's mission. AND MSDH has alternative sources which can be readily leveraged. Generally monitored but not assessed on a consistent cadence.	>600

*MSDH does not consider this an exhaustive list of factors for determining the risk tier of a vendor. Therefore, MSDH may consider other key factors that could cause a vendor to be placed within a particular Tier. Other key factors may include, but are not limited to, the vendor's involvement with State Health Officer declarations, MSDH's emergency responses, Continuity of Operations Plans (COOP), or Disaster Recovery (DR).

Table 2: Risk Matrix

Risk Area	High Severity	Medium Severity	Low Severity
Operational Risk (Outage) **IT Availability**	This can include a significant system outage of the service that may not be back online within 12 business hours.	This can include a significant system outage of the service that may not be back online within 48 business hours.	This can include a significant system outage of the service that may not be back online within 5 business days.
Financial Risk Occurs when the actions of the vendor may place the organization at financial risk. Suppose the product or service is not provided as expected. In that case, this risk might manifest as lost revenue or paying for rework, litigation, or regulatory fines.	Financial Risk Greater than $1,000,000	Financial Risk Greater than $100,000 but less than $1,000,000	Financial Risk Less than $100,000
Reputational Risk **IT Integrity** The public makes no distinction between your company and your third-party vendors. It may have been the vendor's fault, but it is your reputation on the line.	Legislative/Executive Intervention Likely, Organizational Extinction Event, Consumer Legal Action Likely (Class Action Lawsuit)	Legislative/Executive Intervention Possible, Consumer Legal Action Possible	Legislative/Executive Intervention Unlikely, Consumer Legal Action Unlikely
Regulatory Risk **IT Confidentiality** This risk relates to industry specific laws and rules that may be broken if there are issues with the product or service. For example, a customer service agent who provides false or misleading information to your customer would make your company responsible for a direct regulatory violation. These direct violations almost always have a material adverse impact.	MSDH Internally Hosted or Developed System with ePHI subject to HIPAA Rule	Vendor Hosted or Developed System with ePHI subject to HIPAA Rule with MSDH owned data, or SSO with MSDH users	Vendor Hosted or Developed System with non-MSDH owned data. MSDH is a passthrough or bill payer

2. Vendor Monitoring

Risk personnel will monitor all third-party vendors using UpGuard VendorRisk to ensure MSDH's risk posture and hygiene remain healthy. Personnel will evaluate Tier 1 and 2 vendors monthly to monitor changes in risk posture. Tier 4 vendors may be removed from UpGuard VendorRisk to free up space for higher-tier vendors, this will not impact their annual assessments if applicable.

Personnel should document new risks (primarily when associated with a Tier 1 or 2 vendor) or changes in a vendor's risk score that result in a score below the acceptable threshold on the Risk Register per the Risk Management Policy Table 1. Personnel should also note all relevant actions and complete a third-party risk assessment.

3. Vendor Due Diligence

Due diligence requires personnel to complete a reasonable inquiry into a vendor's ability to ensure they can meet the requirements of the proposed service. The degree of due diligence required when selecting a vendor depends on the vendor's risk tier.

The due diligence needed to assess low-risk vendors may be nominal, while critical vendors will require a more thorough assessment consistently. Tier 1 vendors will receive security questionnaires annually and/or supply a copy of their SOC-2/ISO 27001/HITRUST/HIPAA or equivalent report, regardless of their score.

Vendor Intake Workflow

Step 1

Send vendor relationship questionnaires to relevant business owners via UpGuard.

Step 2

Review answers while evaluating vendors that provide IT hardware, software solutions, and/or IT infrastructure services with greater scrutiny.

Step 3

Implement initial Questionnaire-Based Vendor Tiering per Table 1 and Table 2.

Step 4

Implement initial Vendor Assessment (Vendor Onboarding):

Tier 1 Vendors:

- Will receive questionnaires annually and supply a copy of their SOC-2/ISO 27001/HITRUST/HIPAA or equivalent report (if available), regardless of their security score.
- Risk personnel will use default CyberRisk, short form, or custom MSDH security questionnaires to comprehensively evaluate the vendor's attack surface in tandem with their risk profile.
- Personnel will develop extensive risk assessments to highlight relevant risks, remediation plans, vendor risk justification, and all anticipated risks.
- Risk personnel will reassess Tier 1 vendors annually.

Tier 2-3 Vendors (A Range: 801-950)

- Intake questionnaire responses will define internal parameters for sending security questionnaires.
    - For example, if the vendor answered YES to the IT hardware question, then personnel should send an infrastructure security questionnaire to evaluate that aspect of their security posture.
    - Personnel can also utilize short, custom security questionnaires to evaluate vendors in this range.
- Develop an annual cadence for sending/receiving standard risk assessments and security questionnaires.

Tier 2-3 Vendors (High B Range: 701 - 800)

- Intake questionnaire responses will define internal parameters for sending security questionnaires.
    - For example, if the vendor answered YES to the IT hardware question, then personnel should send an infrastructure security questionnaire to evaluate that aspect of their security posture.
    - Personnel can also utilize short, custom security questionnaires to evaluate vendors in this range.
- Develop an annual cadence for sending/receiving detailed risk assessments and security questionnaires.
- Develop remediation plans (if needed).

Tier 2-3 Vendors (Low B to High C Range: 401 - 700)

- Risk personnel will use default CyberRisk, short form, or custom MSDH security questionnaires to comprehensively evaluate the vendor's attack surface in tandem with their risk profile.
- Personnel will develop extensive risk assessments to highlight relevant risks, mandatory remediation plans, vendor risk justifications, and all anticipated risks.
- Tier 2 vendors in this range: one additional assessment on an agreed-upon cadence before the standard annual reassessment date.

Tier 2-3 Vendors (D & F Range: 0 - 400)

- Risk personnel should strongly consider rejecting this vendor, establishing concrete action items the vendor can use to improve their score, or installing financial implications into the vendor's contract.
    - i.e., "As part of this agreement, you are committing to remediating [risks] by [date] before onboarding with MSDH".
- Risk personnel will use default CyberRisk, short form, or custom MSDH security questionnaires to comprehensively evaluate the vendor's attack surface in tandem with their risk profile.
- Personnel will develop extensive risk assessments to highlight relevant risks, mandatory remediation plans, vendor risk justification, and all anticipated risks.
- Tier 2 vendors in this range: one additional assessment on an agreed-upon cadence before the standard annual reassessment date.

Step 5

Ongoing Assessments (Tier 1-3 vendors)

Tier 1 Vendors

- Tier 1 Vendors will, at minimum, go through an annual assessment process, including filling out a security questionnaire and collecting any updated reports (SOC-2, ISO audit, HITRUST, HIPAA, etc.)
- If a Tier 1 vendor falls below the "Acceptable Score" as indicated in the above matrix, then personnel should take the following actions:
    - Adjust the frequency of the questionnaire as needed (i.e., perform an assessment every six months to ensure security controls are in place and/ or improvements are underway).
    - Create "remediations" within UpGuard to develop a posture improvement plan with the vendor by an agreed-upon due date.

Tier 2 Vendors

- Tier 2 Vendors will, at minimum, undergo an annual assessment process. The depth of the assessment process will be based on their overall risk score and will follow the same assessment steps as during onboarding (listed above).
- If a Tier 2 vendor falls below the "Acceptable Score" as indicated in the above matrix, then personnel should take the following actions:
    - Adjust the frequency of the questionnaire as needed (i.e., perform an assessment every six months to ensure security controls are in place and/ or being improved on).
    - Create "remediations" within UpGuard to develop a posture improvement plan with the vendor by an agreed-upon due date.

Tier 3 Vendors

- Tier 3 Vendors will, at minimum, undergo an assessment process every two years. The depth of the assessment process will be based on their overall risk score and will follow the same assessment steps as during onboarding (listed above).
- If a Tier 3 vendor falls below the "Acceptable Score" as indicated in the above matrix, then personnel should take the following actions:
    - Adjust the frequency of the questionnaire as needed (i.e., perform an assessment every 12 months to ensure security controls are in place and/ or being improved on).
    - Create "remediations" within UpGuard to develop a posture improvement plan with the vendor by an agreed-upon due date.

4. Vendor Offboarding

Whether a vendor relationship ends naturally after contract fulfillment or due to performance or non-compliance issues, MSDH must offboard vendors efficiently to eliminate risks and lower exposure.

Risk personnel should take the following actions to disengage vendors from MSDH systems and ensure they no longer have access to sensitive information:

- Maintain communication with vendors to ensure they complete tasks promptly and personnel resolve vendor questions efficiently and accurately.
- Perform a final review of the vendor contract to ensure termination terms and conditions.
- Issue a termination notice that provides detailed reasons and causes for termination.
- Settle outstanding invoices or contract terms with vendors.
- Revoke vendors' access to IT systems, sensitive data, IP information, and any physical buildings or workspaces (if applicable).
- Ensure vendor termination procedures align with all data regulations.
- Update MSDH’s vendor database with UpGuard Vendor Risk to reflect vendor termination.