Third Party Security, Vendor Risk Management and Systems/Services Acquisition

`2021.1`

MiCT makes every effort to assure all third party organizations are compliant and do not compromise the integrity, security, and privacy of MiCT or MiCT Customer data. Third Parties include Vendors, Customers, Partners, Subcontractors, and Contracted Developers.

Policy Statements

MiCT policy requires that:

(a) A list of approved vendors/partners must be maintained and reviewed annually.

(b) Approval from management, procurement and security must be in place prior to onboarding any new vendor or contractor. Additionally, all changes to existing contract agreements must be reviewed and approved prior to implementation.

(c) For any technology solution that needs to be integrated with MiCT production environment or operations, a Vendor Technology Review must be performed by the security team to understand and approve the risk. Periodic compliance assessment and SLA review may be required.

(d) MiCT Customers or Partners should not be allowed access outside of their own environment, meaning they cannot access, modify, or delete any data belonging to other 3rd parties.

(e) Additional vendor agreements are obtained as required by applicable regulatory compliance requirements.

- A standard HIPAA Business Associate Agreement (BAA) is defined and includes the required security controls in accordance with the organization's security policies. Additionally, responsibility is assigned in these agreements. A BAA must be signed with any vendor that may have a business need to access, and/or unsupervised access to PHI or ePHI.

Controls and Procedures

Vendor Technology Risk Review

MiCT security policy requires a risk review of vendor technology, prior to any technology being integrated to MiCT operations and/or infrastructure. Employees are required to engage security team to conduct such review. The request may be submitted by email directly to the security team, or by opening a Github ticket through the MiCT internal service desk.

Security team is responsible to conduct the reviews via interviews and reviews of documentation, to ensure the vendor complies with regulatory requirements and follows security best practices to minimize risk to an acceptable level.

A vendor technology risk (VTR) assessment is conducted using Google VSAQ, in the following steps:

1. Reviewer sends questionnaire link(s) to vendor contact.
2. Vendor completes the questionnaire(s).
3. Vendor saves/exports answers to the assessment questionnaire(s).
4. Vendor contact sends the answers file back to reviewer.
5. Reviewer opens the same questionnaire(s) and loads the answers received from the vendor to complete the assessment.
6. Reviewer follows up with vendor contact as needed.
7. Reviewer facilities discussion with business owner to determine if the risk is acceptable. Vendor remediation may be required depending on the results.

A list of approved vendors / contractors is maintained by the Security and Operations teams.

Vendor Contractual Agreements

HIPAA. If the vendor needs access to PHI/ePHI, the vendor must be HIPAA compliant and a Business Associate Agreement (BAA) is required.

SLA for Service Providers. For network and infrastructure service providers that support production and/or critical operations at MiCT, a Service Level Agreement (SLA) is defined and included in the service contract.

As appropriate, the executed agreement(s) are linked or attached to the vendor on the approved vendors list.

Monitoring Vendor Risks

Vendor contracts are reviewed either annually or according to the signed contract duration.

Based on the risk level and the sensitivity/criticality of data the vendor has access to, the vendor review may include an updated risk analysis performed by the security team in addition to legal and business review of contract terms.

If the vendor is a service provider, the DevOps team monitors the service status of the provider according to its SLA. This is done by either manually reviewing the posted service status on the vendor's status pages at least quarterly, or by setting up alarms for service interruption using automation.

Software and Systems Acquisition Process

MiCT Security maintains a list of pre-approved business software and a list of approved vendors / contractors.

If additional commercial software, hardware system, or cloud services is needed, a request should be submitted through MiCT internal service desk. This will trigger the approval by manager/security and procurement process.

As applicable, MiCT security team may conduct a risk analysis on the software or system to ensure it complies with MiCT security, compliance and legal requirements and does not interfere with the security controls. If a risk is identified, additional controls should be identified and implemented (or planned) prior to acquisition. An alternative product may be considered as a result of the risk analysis.