Office of Information Technology

IT Process
THIRD PARTY SECURITY & ACCESSIBILITY REVIEW

Standard: IT06002A
Original Effective Date: 11/13/2020
Last Revised:

Last Reviewed: 5/04/2022
Next Scheduled Review Date: 5/04/2023
Version No.: 1.01
Administrative Owner: Director of Information Security Services

PURPOSE

The purpose of this document is to outline the overall Third Party Security & Accessibility Review Process. This Process will analyze, identify, assess and provide recommendations and possible mitigation actions for vulnerabilities and threats or other compliance issues that may be associated with an application, service, solution or product to be acquired by the College and to monitor those services already in the College's portfolio of products on an ongoing basis.

SCOPE

The Procurement Office, IT Security Group (ITSG) and the Accessible Technology Group (ATG) coordinate the review and assessment of applications, services, solutions or products that includes cloud/offsite storage or processing of College data, contains transactions subject to PCI DSS or is an Information Communication Technology (ICT) intended for the general public or widely used internally at the College.

DEFINITIONS

Term	Definition
Business Owner/ Requester	A member of the College community with a need to acquire or maintain a product, software or service offered by a vendor/third party.
Vendor/Third Party	An external business entity contracted by Montgomery College for a set period for providing a service or delivering a product.
PII, Personally Identifiable Information	Data that can be used, in part or in combination with other Data to distinguish or trace an individual's identity, such as name, social security number, date of birth, student/staff M number; and any other information that is linked or linkable to an individual, such as medical, educational, financial, or employment information.
PCI DSS	Payment Card Industry Data Security Standard (PCI DSS) is an industry-based regulation developed by major credit card companies and serves as a set of technological and procedural requirements for better securing credit card processing and cardholder information.
SOC 2	A SOC 2 is an independent audit report based on AICPA's existing Trust Services principles and criteria. The purpose of the SOC 2 report is to evaluate an organization's information systems relevant to security, availability, processing integrity, and confidentiality or privacy.
AoC	PCI DSS Attestation of Compliance (AoC)is a document that serves as a declaration of the merchant's compliance status with the PCI DSS. The AoC must be completed by a Qualified Security Assessor (QSA) or the merchant if the merchant's internal audit performs validation.

ICT	Information and communication technology (ICT) is an electronic system or equipment and content contained therein, used to create, develop, maintain, duplicate, convert, store, or display information. ICT includes software, hardware, electronic content, or support documentation and services
ICT Accessibility	The practice of incorporating accessibility in the development, procurement, maintenance, or use of ICT for the purpose of ensuring that the quality of a product or service is one which can be used by all its intended users regardless of differing capabilities.
VPAT	A Voluntary Product Accessibility Template (VPAT™) is a document that explains how information and communication technology (ICT) meet (conform to) the Revised 508 Standards for IT accessibility. Vendors may self-disclose how the features and functional characteristics of the product meets Revised 508 Standards.

PROCESS

A. New Purchase/Acquisition

1. Initiation

The Third Party Security & Accessibility Review Process starts with a necessity of a unit or department to acquire services, software, hardware, electronic content or support documentation and services offered by a third party. The Procurement Office addresses this necessity by identifying the different options and vendors in the market. As data protection and web accessibility are critical to fulfill Montgomery College's policies, the Procurement Office must initiate this Process since they are often the first (and sometimes the last) to encounter a request for these offerings. Therefore, the Procurement Office must ask the business requester to complete the Third Party Pre-Engagement Checklist. If the requester contacts the IT Resource Management (ITRM) group prior to contacting Procurement, ITRM will send the Third Party Pre-Engagement Checklist as part of OIT's Software Request Form to the requester. ITSG and the ATG will review the completed checklist and determine the level of security assessment or web compliance review required from the vendor before a purchase is approved.

If it is determined that no assessment is required, ITSG and ATG, will sign the Third Party Pre-Engagement Checklist or Software Request Form and return to ITRM or Procurement indicating as such.

2. Types of Assessments

i. Security Assessment

If use of proposed solution includes the cloud or off-site storage or processing of College data, the vendor will be required to submit its latest SOC 2 Type 2 report and complete a security assessment questionnaire designated by ITSG (assessment may be facilitated by a third party engaged by the College). The College reserves the right to disqualify any vendor that fails to provide a satisfactory SOC 2 Type 2 report and/or to satisfactorily complete the requested assessment questionnaire.

The SOC 2 report and the security assessment are the main documents ITSG uses to evaluate if the security controls provided by the vendor are appropriate based on best business practices and the Montgomery College Confidential Data Management and Security Policy, 66002.

ii. PCI DSS Assessment

If use of proposed solution includes transactions subject to PCI DSS, ITSG will review the handling of credit card processing within the context of the security assessment or separately if warranted. The vendor will be required to submit its PCI Attestation of Compliance (AoC). The College reserves the right to disqualify any vendor that fails to provide a satisfactory AoC.

iii. Web Accessibility Assessment

If the proposed solution contains a public web presence or user interface intended for the public or widely used internally at the College, the ATG will conduct an assessment to determine the level of compliance with accessibility standards.

3. Assessment Process

i. Security Assessments

ITSG and/or its designated third party assessor will reach out to the vendor directly for additional information, requesting its SOC 2 report, and initiating the completion of a security questionnaire. Once the questionnaire and/or SOC 2 report is completed and returned, ITSG will perform the required analysis and provide the requester and Procurement with a recommendation. The assessment will be processed only if it meets the following requirements:

- The vendor provides a copy of the SOC2 report, if available.
- The vendor fully cooperates with ITSG and its designated third party assessor.
- The vendor provides any additional documentation considered relevant to complete the assessment.

ii. ICT Accessibility Assessments

ATG will review the VPAT, and may request a demonstration environment to complete the compliance assessment using available tools. ATG will perform the required analysis and provide the requester and Procurement with a recommendation. The assessment will be processed only if it meets the following requirements:

- The VPAT must be fully completed by the vendor.
- The vendor fully cooperates with the Accessibility Technology group.
- The vendor provides any additional documentation or access to a demonstration environment considered relevant to complete the assessment.

iii. Assessment Compliance

If the security or accessibility assessments cannot be completed due to non-compliance by the requester or the vendor, the Procurement Office cannot continue with the purchasing process. The requester will need to resubmit the request to restart the assessment process.

4. Review Time

If the vendor meets the above requirements and ITSG or ATG raises no questions, a final response will be sent to the requester within fifteen (15) business days from the date of receiving the required documentation and/or demo environment. If necessary, meetings

or conference calls will be scheduled with the appropriate parties to gather additional information and/or clarify responses.

NOTE: The fifteen (15) business days is in addition to the time it takes (up to 30 days) for the vendor to complete its requirements (submit documentation, complete security questionnaire, provide authorizations to ITSG to review its materials, etc. Business Owners/Requesters must build this additional time into their timelines.

5. *Determine Compliance*
For each area that is not in compliance with the applicable regulation, College policy or security best practices, the ITSG or the ATG will identify potential remediation options, if feasible.

6. *Assessment Report*

ITSG and/or the Accessible Technology team will prepare an Assessment Report with the recommendations/remediation plans based upon the identified risks associated to the review. The Assessment Report will be sent via e-mail to the Requester, ITRM and/or the Procurement Analyst in charge of the request. The report will include the following sections:

- Executive Summary
- Information Security Assessment
- Conclusion and Recommendations, which may include:
    - Risks Identified
    - Remediation Actions
    - Additional recommendations

NOTE: ITSG and the ATG may not be able to recommend moving forward with the vendor, either because there are no appropriate mitigations available or because the vendor is not inclined to implement the requirements necessary to reduce or eliminate the risk to the College, or the vendor simply refused to comply with the assessment process. In that case, Procurement may not proceed with the purchase of the requested solution.

7. *Follow Up*

It is the responsibility of the Requester or the Business Process Owner to implement and periodically communicate the status of any agreed upon remediations noted in the report.

ITSG or the ATG are available to provide guidance on remediation steps on an as needed basis.

The Procurement Office will provide standard contract language in any agreement to ensure that the vendor maintain the agreed upon security and/or accessibility levels throughout the lifecycle of the product and its use at the College.

8. *Documentation*

All documentation received and reports issued as part of the operation of this Process are stored in the Montgomery College document storage repository.

9. *Workflow of the Process*

This process is depicted in the workflow diagram file Third Party Security Review Process Workflow Diagram.

B. Current Vendors

1. *Annual Reviews*

i. Security Reviews

Procurement will require that vendors provide a current SOC 2 report on an annual basis as part of the renewal process. In addition, ITSG and/or its designated third-party assessor will conduct an annual security review to ensure the vendor is maintaining the level of security that meets the College's requirements.

ITSG will provide a summary response indicating its recommendations, similar to the initial assessment report.

ii. PCI DSS Reviews

The ITSG will reassess the existing product on at least on an annual basis to ensure continued PCI compliance.

iii. ICT Accessibility Reviews

The Accessible Technology group will reassess the existing product at least on an annual basis to ensure continued compliance and maintaining contractual agreements.

NOTE: ITSG and the ATG may not be able to recommend continuing with the vendor, either because the vendor's security or accessibility posture has changed and there are no appropriate mitigations available or because the vendor is not inclined to implement the requirements necessary to reduce or eliminate the risk to the College, or the vendor simply refused to comply with the renewal assessment process. In that case, Procurement may not proceed with the renewal of the requested solution, or upon agreement of all parties, Procurement may proceed with a one-time renewal, while the requester identifies an alternative solution that meets the College's security and accessibility requirements before the next renewal.

C. Roles and Responsibilities

Table 3 describes the roles and responsibilities of the groups involved in the Third Party Review process.

Table 1: Roles and Responsibilities

Role	Responsibilities
Procurement Office	- Initiates this process for all potential vendors before the procurement is completed. - Incorporate recommendations and/or remediation language/steps into any contracts to ensure compliance.

	- Communicate any issues of concern and/or non-compliance to the vendor on behalf of the College. Communication to vendors will be based on feedback/guidance from ITSG and ATG.
IT Resource Management	- Initiates this process for all potential vendors before the procurement is completed, if the request is received prior to engaging with Procurement. - Communicates any findings by ITSG or ATG to the Procurement Office.
IT Security Group	- Evaluate the Third Party Pre-Engagement Checklist - Conduct Security Assessments - Provide assessment report to the requester and the Procurement Office.
Accessible Technology Group	- Evaluate the Third Party Pre-Engagement Checklist - Conduct ICT Accessibility Assessments - Provide assessment report to the requester and the Procurement Office.
Director of Information Security Services	- Review exception requests - Approve exceptions

EXCEPTIONS

Exceptions to this process will be considered on a case by case basis in accordance with the IT Exception Request Process.

COMPLIANCE AND RECOURSE FOR NON-COMPLIANCE

Montgomery College has established College Policies/Procedures and the OIT has established IT Standards and Processes and associated guiding documents to provide appropriate protection of technology resources, to assure protection of personally identifiable and sensitive information and to promote privacy and to assure accessibility for all students and employees. Any faculty, staff, contractor, or vendor found to have violated any part of College Policies, Procedures or IT Standards or Processes may be subject to disciplinary action and/or legal action.

RELATED DOCUMENTS

- 66002 Confidential Data Management and Security Policy
- 66005 Data Asset Management and Security Policy
- Montgomery College IT Standard Exception Request Form
- IT06002: Third Party Security and Accessibility Standard
- 66004 Electronic Information Technology Accessibility

WEB SITE ADDRESS FOR THIS STANDARD

APPROVALS/REVISION HISTORY

Date	Version/Revision/Notes	Approver
11/13/2020	Initial Version: 1.0	Nell Feldman, Interim Director of Information Security Services/CISO/IT Policy Administrator
5/4/2022	Minor modifications after review;	Nell Feldman, Interim Director of Information Security Services/CISO/IT Policy Administrator

Nell Feldman Digitally signed by Nell Feldman
Date: 2022.05.05 10:56:35 -04'00'