Office of Information Technology

IT Standard
THIRD PARTY SECURITY & ACCESSIBILITY REVIEW

Standard: IT06002
Original Effective Date: 10/15/2020
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

STANDARD

PURPOSE

Montgomery College ("College") information technology resources and digital business information are critical to the administrative business and academic success of its students. The task of protecting these resources in compliance with the Board of Trustees approved policy and applicable Federal and State laws and regulations is the responsibility of the Office of Information Technology (OIT).

This standard defines the manner in which Procurement, IT Security (ITSG), and the Accessible Technology groups ensure that new and existing applications, services, solutions or products meet the requirements to protect the College's Data and comply with regulations with regard to PCI DSS and technology accessibility.

SCOPE

This standard applies to all college vendors or potential vendors who provide technology resources or services in the form of software, hardware, electronic content, or support documentation and services as well as those vendors who host and/or process College Data in support of service offerings. The standard applies to Montgomery College employees who request new services, as well as those employees who are responsible for implementing and evaluating those services.

This standard also applies to vendors or potential vendors as described above for any services provided during trial or pilot periods prior to a formal purchase or procurement, as well as for any vendors or services that meet the above description that do not require a formal purchase or procurement.

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 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.
College Data	Per College Procedure 66002CP: All Data that is used by or belongs to the College, or that is created, processed, stored, maintained, transmitted, or copied using College or vendor provided IT Resources. For the purpose of this standard, the terms "data" and "information" are used interchangeably. They include any information kept electronically, whether stored onsite or offsite, kept as test data in a non-production system, or kept audio-visually, stored offsite, that meets any of the following criteria: 1. Created or updated via the use of the College's Systems of Record or used to update data in the Systems of Record; 2. Acquired or maintained by College employees in performance of official administrative or academic job duties;

	3. Relevant to planning, managing, operating, or auditing a major function at the College; 4. Included in official College administrative reports or official College records.
Data Trustees	Per College Procedure 66005CP: College officials who have responsibilities for major data management decisions within their academic and/or administrative area to include oversight of the implementation and verification of processes for Data privacy, protection, access, and accountability. Data Trustees may designate appropriate personnel to complete processes required under this Procedure.
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.
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.

STANDARD

A. Third Party Review

1. The third party review program focuses on three types of assessments: Security, PCI DSS compliance, and Web Accessibility.
2. Security assessments focus on the protection of College Data and PII, particularly for those vendors who store or process that Data outside of the College's systems and network.
3. PCI DSS compliance assessments ensure that credit card processing systems used by college offices comply with the payment card industry requirements.
4. ICT accessibility assessments identifies the level of compliance with accessibility standards.

B. Roles and Responsibilities

1. Procurement is responsible for:
   a. Ensuring that all new requests for applications, services, solutions or products are assessed prior to purchase.
   b. Ensuring that all currently owned and operated applications, services, solutions or products are reviewed at least annually to determine if there are any major changes that need to be addressed before continued use.
2. ITSG is responsible for:
   a. Conducting the Security assessment and sharing the results with Procurement.

b. Conducting the PCI DSS assessment, either separately or as part of a Security Assessment, and sharing the results with Procurement.

3. Accessible Technology is responsible for:
   a. Conducting the ICT Accessibility assessment and sharing the results with Procurement.
4. Business Owners/Requesters are responsible for:
   a. Ensuring any and all internal controls are managed appropriately to minimize risk.
   b. Complying with the recommendations provided by ITSG and Accessible Technology, or if they cannot comply, accepting the risk on behalf of the College as a result of non-compliance.
5. Data Trustees are responsible for:
   a. Ensuring compliance with the recommendations provided by ITSG (for data security), or consulting with the Business Owner/Requester on any risk acceptance decisions.
6. Director of ADA & Title IX Compliance is responsible for:
   a. Ensuring compliance with the recommendations provided by Accessible Technology (for accessibility), or consulting with the Business Owner/Requester on any risk acceptance decisions.
7. Unit Administrators are responsible for:
   a. Ensuring compliance with the recommendations provided by ITSG (for data security), and Accessible Technology (for accessibility), or consulting with the Business Owner/Requester on any risk acceptance decisions.
8. General Counsel is responsible for:
   a. Reviewing any and all contracts to ensure data protection and accessibility requirements are properly addressed.

C. Third Party Review Processes

The ITSG, in conjunction with Procurement and Accessible Technology establishes the processes that requesters must follow regarding assessing technology applications, services, solutions or products prior to purchase as well as on an ongoing basis. This process is defined in IT Process: Third Party Reviews, IT06002A.

RISK ACCEPTANCE

This standard is applicable as of its Effective Date. Exceptions to this standard and/or risk acceptance decisions must be escalated to the Business Owner/Requester's Unit Administrator in consultation with the Data Trustee (for data security) or the Director of ADA & Title IX Compliance (for accessibility), and documented through the IT Standard Exception and Risk Acceptance Process before any contracts or agreements are signed for a new vendor, or for the continued use of an existing vendor.

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. 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

- Montgomery College IT Standard Exception Request Form
- 66004 Electronic Information Technology Accessibility
- IT06002A: IT Process-Third Party Review Process

WEB SITE ADDRESS FOR THIS STANDARD

APPROVALS/REVISION HISTORY

Date	Version/Revision/Notes	Approver
10/15/2020	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 10:57:13 -04'00'