Assessment Procedure for Software Purchases

Office of Information Technology

Miami Dade College

While using a commercial off-the-shelf or third party hosted software application has many advantages over internal developed solutions, there are security concerns must be considered prior to entering a purchase and/or use agreement. The following procedure applies to all third party software applications that are used by the departments to collect, transmit, process, or store college data. The software application can be administrated remotely by an application service provider and made available to the College community via an Internet-accessible service. The software application can also be an off-the-shelf solution and administrated internally by college IT staff or department personnel.

The decision to incur business expenses for third party services must be evaluated from a cost/benefit perspective. Department heads should consider other viable options such as internal development or maintenance prior to pursuing of third party services. A review of both the necessity and cost shall be conducted annually by the department heads to ensure the effective use of college resources.

1. Security Assessment

The following table shows the scenarios where security assessment is required prior to entering a purchase or use agreement. The guideline is based on the type of institutional data involved. Miami Dade College classifies institutional data into four categories: Restricted, Confidential, Internal, and Public. See *Data Classification Standards* for more information.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Scenario | Restricted | Confidential | Internal | Public |
| A commercial off-the-shelf application that runs on College desktop/laptop or academic/administrative department server | Not permitted. | Not permitted. | No action required. | No action required. |
| A commercial off-the-shelf application that runs on a server housed in College data center and supported by IT. | Security & operation assessments by IT prior to purchase or adoption is required. | Security & operation assessments by IT prior to purchase or adoption is required. | Security & operation assessments by IT prior to purchase or adoption is required. | Security & operation assessments by IT prior to purchase or adoption is required. |
| The application is installed in a remote facility that is administrated by a 3rd party vendor. Access to the application/data transmission occurs over the Internet. | * Security requirements in RFP/RFI required. * Security assessment by IT prior to purchase or adoption. * Data must reside on a college approved system. * Contract required. | * Security requirements in RFP/RFI required. * Security assessment by IT prior to purchase or adoption. * Data must reside on a college approved system. * Contract required. | Security assessment by IT prior to purchase or adoption is required. | Security assessment by IT prior to purchase is recommended but not required. |

1. Compliance with College Policies

Prior to entering into the purchase or use agreement, the department heads must also adhere to the guidelines, criteria, and conditions stated in the following policies:

* MDC Information Security Policy

Certain types of data require the college to comply with external mandates. All data management processes must conform to all applicable mandates. Such mandates include but are not limited to:

* Federal Educational Rights and Privacy Act (FERPA)
* Gramm-Leach-Bliley Act (GLBA)
* Health Insurance Portability and Accountability Act (HIPAA)
* Payment Card Industry Standards Supporting Documents (PCI)

The department heads must also receive approvals from the appropriate data stewards.

1. Invitation to Negotiate (ITN), Request for Proposal (RFP)

The Office of Information Technology will assist department in drafting ITN or RFP to include security requirements. IT will also assist departments in evaluating responses from the vendors. All ITN or RFP that involves third party vendor handling restricted or confidential data must include information security requirements.

1. Review of Contract Details

The Purchasing Office may require specific language in a contract to protect college interests. Any contract with a third party vendor that involves restricted or confidential data must be reviewed and approved by the Purchasing Office. Questions regarding policy interpretation or compliance should be directed to Office of Information Technology.