Policy for Cyber Data Security for Technology Procurements at the University of Massachusetts

Any Technology purchase that is used to collect, store or transmit personal information or used to process credit card transactions requires additional reviews and safeguards to ensure that the purchase is in compliance with all state, university and federal regulations.

Massachusetts General Law 93H (M.G.L. 93H) defines personal information as an individual’s first name or first initial, and last name in combination with one or more of the following:

- State-Identification Card Number
- Social Security Number
- Driver’s License Number
- Credit, Debit, or Financial Account Number (With or Without any Security Code, Access Code, Personally Identifiable Identification Number, or Password)

Personal information protections also extend to data about students and staff as defined by FERPA. A good tutorial on FERPA is available on the OIT website at [http://www.oit.umass.edu/sites/oit.umass.edu/files/2011/07/06/tutorial.pdf](http://www.oit.umass.edu/sites/oit.umass.edu/files/2011/07/06/tutorial.pdf)

Departments should carefully review software system contracts, software licenses and/or subscriptions to determine if the product collects, stores or transmits personal information (PII), FERPA information or processes credit/debit card for terms that relate to Data Security. This includes those contracts, licenses or subscriptions that may not require a purchase order. Contact a Buyer in Procurement with any questions and if needed the Buyer can provide you with a Data Security Amendment to be initialed by the department and vendor and then incorporated into the license agreement. The Data Security Amendment establishes the University’s Data Protection Controls and Breach Notification requirements.

Anytime a Department would like to accept credit cards, the Department must contact the campus eCommerce representatives in Administrative Systems for A&F to discuss options and requirements around Payment Card Industry Data Security Standards (PCI-DSS). PCI- DSS is an information security standard that relates to credit card cardholder information from debit, credit, and Point of Service (POS) cards. The standard was developed by the credit card industry and all banks, including the University’s bank,
require their customers to adhere to these standards to reduce fraud and protect cardholder personal information. It is the University’s policy that an eCommerce representative review and approve any activity involving credit cards to ensure that the system meets the PCI DSS standards, are certified as compliant, and the department is adhering to all PCI requirements. This additional review is critical since both the University and the other party are responsible for the security of the cardholder data. The eCommerce Manager will require the Data Security Amendment referenced above with additional PCI DSS security requirements be incorporated into the license or purchase agreement. As always please contact the Procurement Department if you have any questions.