Meeting Minutes from PIR group meeting on October 23, 2006

Two attachments were shown and discussed:
“PII List 102306.xls” (spreadsheet containing known applications at Loyola that contain PII)
“PII 102306.ppt” (presentation outlining privacy policies at peer institutions, and the similarities/differences between those policies)

Should the policy be centralized or de-centralized?
- Policy should be University-wide (centralized), not done on a department-by-department basis (decentralized)

What regulations should we comply with in this policy?
- Policy should satisfy all regulatory compliance issues required of Loyola (FERPA, HIPAA, GLB, Illinois’ FOIA, Illinois’ PIPA, PCI DSS)

How should we classify data at Loyola? Covered & not covered, or protected, sensitive, and public?
- Consensus was to have 3 classes of data. These would be data covered by regulations (protected), data that is not covered by regulations but that Loyola would want to keep private (sensitive), and data that is not covered by regulations that Loyola does not need to keep private (public).
- Terms should be clearly identified as Loyola-centric terms. One possibility would be to use “Loyola protected”, “Loyola sensitive”, and “Loyola public” as terms to describe data.
- Data that is “Loyola protected” can be identified by a series of rules. Examples should be provided of types of data that are “Loyola sensitive”, along with guidelines for how the data should be handled (be careful about saving and printing it, how to properly dispose of paper copies of that information, etc)

There should be an annual review of systems housing “Loyola protected” data and the users who have access to that data. This will ensure that the system is being properly maintained, and that the only users who have access to “Loyola protected” data are those that need to have access to it.

The Office of the General Counsel has standard clauses to add to contracts concerning the handling of certain types of protected data. If they are assisting you with a contract, be sure to highlight your
regulatory compliance needs to confirm that they have inserted those clauses into the contract.

Physical security concerns around “Loyola protected” and possibly for “Loyola sensitive” information
- Best if the information is kept behind a locked / badged door – not publicly accessible.
- Paper shredders should be available. Loyola does have a licensed and bonded service for destroying paper documents.
- “Electronic shredding” is available from ITS to ensure that data on disk drives is completely erased.
- Cleaning staff can come during regular business hours instead of during evening hours. Registration & Records currently does this.
- Fax machines can also contain "Loyola protected" information. There is a method to pull faxes into GroupWise. ITS is working to put together documentation around this solution. If your department is interested in this, please contact Joe Bazeley after the meeting.