PIRG Meeting Minutes 03/26/07

<table>
<thead>
<tr>
<th>Identification</th>
<th>Personal Information Risk Group</th>
<th>Phase: 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Name:</td>
<td>Personal Information Risk Group</td>
<td></td>
</tr>
<tr>
<td>Project ID #:</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Project Sponsor:</td>
<td>Susan Malisch</td>
<td></td>
</tr>
<tr>
<td>Date / Time:</td>
<td>03/26/07</td>
<td></td>
</tr>
<tr>
<td>Topic:</td>
<td>Discussion of draft policies</td>
<td></td>
</tr>
<tr>
<td>Attendees:</td>
<td>Larry Adams, Joe Bazeley, Laura Bulgarelli, Becky Gomez, Benjie Loanzon, Cory O’Brien, Tim O’Connell, Eric Pittenger, Jim Sibenaller, Kathleen Steinfels, Rob Thoma</td>
<td></td>
</tr>
<tr>
<td>Non-Attendees:</td>
<td>Diane Asaro, John Campbell, Stacey Hughes, Sue Kilby, Clare Korinek, Susan Malisch, Christine Marciasini, Carol McCormack, Tim McGuriman, Brian Slavinskas, Carolyn Wright</td>
<td></td>
</tr>
</tbody>
</table>

**Discussion Points**

_Briefly describe the points / issues / topics that were discussed._

- **PII Identification policy**
  - Two additions discussed at previous meeting were approved. Under Frequency, “All departments need to maintain a schedule of when they plan to perform their scans” was added. Under Measurement & Reporting, “ITS will provide a summary report to the Information Technology Executive Steering Committee” was added.
  - Policy approved by PIRG.

- **Encryption policy**
  - Loyola’s standard contractor terms and conditions does contain elements relating to maintaining the privacy of Loyola information.
  - Two items were discussed that will be forwarded to the General Counsel for consideration regarding this T&C document. The first item is to explicitly state that any costs associated with a data breach caused by a contractor will be the contractor’s responsibility. The second item is to state that the contractor is required to promptly fix/resolve the issue.
  - Policy approved by PIRG.

- **Compliance Review for PIRG policies**
  - Modifications were made to the policy from suggestions at the previous meeting.
  - The responsibility for designating a compliance lead was moved from the division or department to the division or department head.
  - Wording was added to have both a primary and alternate compliance lead for each department.
  - Wording was added to have each department send ITS the names of their compliance leads.
  - Modifications were discussed for the checklist. These include:
    - Changing the third point to reference the Encryption policy and Electronic Security policy
    - Changing the sixth point to reference the Access Control policy (referred to as the “Key policy” during discussion) and password standards. The referenced Key policy is an existing Campus Safety policy located at [http://www.luc.edu/safety/keypolicy.shtml](http://www.luc.edu/safety/keypolicy.shtml).
    - Changing the seventh point to reference the Disposal of Loyola Protected / Sensitive Data policy
    - Changing the twelfth point to clarify the clean desk policies are being followed where they exist
Keeping the reference to the key policy was discussed. Certain areas do require that paper documents with personally identifiable information are kept locked up when not in use. The group decided to keep the reference to the key policy in this document.

The printer / fax item was discussed. A proposal was made to change the wording to convey the idea that only printers / faxes that received / produced personally identifiable information were covered. The group decided not to change the wording “limited access area”. This was purposely left to interpretation by the department and is considered a discretionary item.

When the document is published, links to other referenced documents will be included.

The group approved the policy, with the right to make modifications to the policy if the wording did not accurately reflect the conversations at this meeting. The group has until 4/9/07 to adjust any wording.

Data Breach Response policy

- The email address will be changed to DataSecurity@luc.edu. This address will be an alias that points to Security@luc.edu. There was discussion around the Security@AnyDomain. A question came up about what the email address was for Campus Safety is – it is AskSafety@luc.edu.
- The need for an anonymous method of reporting a data breach was identified. ITS will create a solution/web page for anonymous reporting. The policy will be updated to reflect this option.
- The composition of the response team for a confirmed breach of protected / sensitive data was discussed. An appendix will be added indicating that if the data has credit card numbers or bank account numbers then the Director of Cash Management and/or the Assistant Treasurer must be included on the team, and if the data has social security numbers then a human resources representative must be included on the team.
- The 4 hour response time was discussed. There was a desire to indicate that the process would start as quickly as possible, and to remove the 4 hour deadline to protect ourselves if our best efforts required longer than 4 hours. The policy was updated to reflect this.
- The group approved the policy, with the right until 4/9/07 to make modifications to the policy if the wording did not accurately reflect the conversations at this meeting.

Email forwarding

- A list of concerns around allowing email forwarding will be brought up to the CIO and ITESC. If anyone has any additional concerns, please provide them to Joe Bazeley by 4/9/07.

Concerns & Comments

- There is no way to validate that a student has received/opened an email they were sent. This includes both emails from faculty and administrative emails such as eBill notices.
- Forwarding may lead to attachments being sent outside of the University without the sender's knowledge. This may include documents that should not be forwarded outside of the University due to the types of information they contain.
- Official communications from all departments should be sent to @luc.edu addresses.
- Should faculty and staff be allowed to use email forwarding? They are more likely to receive documents containing sensitive information that should not leave Loyola.
- Should we include boilerplate legal language at the bottom of all email messages indicating that the contents are confidential, intended only for recipient, etc?
- If we include this boilerplate, would it attach to all messages? Or only to messages that leave the Loyola network? Would it apply to student messages? Does it apply to student workers? Senders responsibility or automatic insertion?
- There are multiple ways to forward messages. The standard way is to use Novell's IUAdmin tool (called PAM at Loyola - http://www.luc.edu/its/pam_reroute.shtml). Users can also configure rules within GroupWise to automatically forward messages to an outside account.
- Certain departments recommend that students use external providers, and have instructions for doing so on their departmental web site.
PIRG Meeting Minutes 03/26/07

- **Policy Routing/Approval**
  - All policies have been approved by PIRG (with the option to revisit the wording on Compliance Review policy and Data Breach action plan until 4/9/07).
  - They will next go to SMART for 3rd party review, then to the ITESC and General Counsel, then to the UCC. Jim Sibenaller and Susan Malisch will shepherd the documents through this process.

- **Rollout / Awareness**
  - Discussion around whether a subcommittee should be formed to address how to roll out these policies and build awareness once they are approved. The group decided to discuss this topic at the next meeting.
  - Recommendation to include Jorene Richards and a UMC representative.

- **PIRG Future**
  - PIRG was initially created as a temporary group to address a specific issue. Additional security issues will most likely need to be addressed, but the current makeup of PIRG may not be ideal to address them. A similar committee may be formed once PIRG completes its tasks, and it may contain some of the same individuals who are part of PIRG. It was mentioned that having an information security group would be viewed favorably by underwriters.

- **PII Identification policy approved.**
- **Encryption policy approved.**
- **Joe Bazeley will send two items to General Counsel for consideration in regards to the contractor terms and conditions.**
- **Compliance review policy approved. Changes discussed at the meeting will be added to the document. The document will be circulated so that changes can be entered prior to 4/9/07 if an item from the meeting was incorrectly captured in the document.**
- **Data breach response action plan approved. Changes discussed at the meeting will be added to the document. The document will be circulated so that changes can be entered prior to 4/9/07 if an item from the meeting was incorrectly captured in the document.**
- **Initial list of email forwarding concerns created. Additional concerns should be sent to Joe Bazeley prior to 4/9/07. The final list will be sent to Susan Malisch to present at the ITESC.**
- **Rollout / Awareness will be discussed at the next meeting.**

### Decisions / Recommendations / Confirmations

- PII Identification policy approved.
- Encryption policy approved.
- Joe Bazeley will send two items to General Counsel for consideration in regards to the contractor terms and conditions.
- Compliance review policy approved. Changes discussed at the meeting will be added to the document.
  - The document will be circulated so that changes can be entered prior to 4/9/07 if an item from the meeting was incorrectly captured in the document.
- Data breach response action plan approved. Changes discussed at the meeting will be added to the document.
  - The document will be circulated so that changes can be entered prior to 4/9/07 if an item from the meeting was incorrectly captured in the document.
- Initial list of email forwarding concerns created. Additional concerns should be sent to Joe Bazeley prior to 4/9/07.
- Rollout / Awareness will be discussed at the next meeting.

### Next Steps / Follow-ups

<table>
<thead>
<tr>
<th>Task</th>
<th>Owner</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Send contractor T&amp;C considerations to</td>
<td>Joe Bazeley</td>
<td>4/2/07</td>
</tr>
<tr>
<td>General Counsel</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 Send any modifications to the Compliance</td>
<td>PIRG</td>
<td>4/9/07</td>
</tr>
<tr>
<td>Review policy to Joe Bazeley by 4/9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 Send any modifications to the Data</td>
<td>PIRG</td>
<td>4/9/07</td>
</tr>
<tr>
<td>Breach Response action plan to Joe</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bazeley by 4/9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4 Send any additions to the email</td>
<td>PIRG</td>
<td>4/9/07</td>
</tr>
<tr>
<td>forwarding concern list to Joe Bazeley</td>
<td></td>
<td></td>
</tr>
<tr>
<td>by 4/9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5 Provide PIRG with access to shared</td>
<td>Joe Bazeley</td>
<td>4/2/07</td>
</tr>
<tr>
<td>folder containing PIRG policies</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6 Determine method for anonymous breach</td>
<td>Joe Bazeley</td>
<td>4/30/07</td>
</tr>
<tr>
<td>submission</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>