## Identification

<table>
<thead>
<tr>
<th>Project Name:</th>
<th>Personal Information Risk Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project ID #:</td>
<td>N/A</td>
</tr>
<tr>
<td>Project Sponsor:</td>
<td>Susan Malisch</td>
</tr>
<tr>
<td>Topic:</td>
<td>Discussion of draft policies</td>
</tr>
</tbody>
</table>

| Phase: | 1 |
| Date / Time: | 02/06/07 |
| Project Manager: | Joe Bazeley |

## Attendees:
- Remote - Laura Bulgarelli, John Campbell, Stacey Hughes, Kathleen Steinfels

## Non-Attendees:
- Clare Korinek, Benjie Loanzon, Carolyn Wright

## Discussion Points

**Briefly describe the points / issues / topics that were discussed.**

- **PII Identification policy**
  - Is 6 months an appropriate time frame? Consensus was yes.
  - Should it be every 6 months or every 6 months with a defined/specifed timeframe for all departments (Mar/Sep)? Consensus was every 6 months so that departments could flex the audit away from busy times.
  - Text should be added to Frequency section stating that all departments need to maintain a log/schedule of when they are scheduling/planning to do their audits.
  - Discussion around the possibility of having a list of all removable devices in a department. Consensus was that this would not be feasible.
  - Text should be included in Measurement & Reporting stating that ITS will provide a summary of the results to the IT Executive Steering Committee.
  - Training will be created by ITS & HR. Jorene Richards from HR can assist in creating the training.
  - Discussion around the value of scanning machines that are known to contain Protected data. The tool is intended to validate that machines that are believed to not hold any Protected data actually do not hold any Protected data.

- **Encryption policy**
  - Subcommittee expanded scope from Full Disk Encryption to all forms of Encryption.
  - What happens if a disaster situation (i.e. bird flu) forces us to move to a virtual campus? How will individuals be able to access and save files necessary to do their work? An improved remote files access method is being investigated by ITS.
  - How to best handle contractors and 3rd parties? Contractual obligation is the best way. Joe is checking with General Counsel to see if this is part of our boilerplate contract language.

- **Compliance Review for PIRG policies**
  - Subcommittee changed wording from Audit Practices to Compliance Review because it is not a true audit.
PIRG Meeting Minutes 02/06/07

- Semi-annual basis will be switched to 6 months to coincide with the PII Identification. The person identified to coordinate the scanning for PII will also be responsible for the Compliance reviews.
- Text “individual will rotate” changed to “individual may be rotated”.
- Third policy paragraph changed from “ensuring encryption” to “ensuring compliance with all items listed in the Compliance Review form”.
- Departmental compliance person will send results to ITS.
- A number of items from Compliance Review form will be addressed at the next meeting to ensure that they are in scope with existing policies. These items include #3 (LUC approved programs...), #4 (Staff members are...), #6 (Key and password... - add “physical” before key), #8 (Print and Fax... - add in Document imaging), #12 (Clean desk policy...)
- Definitions of user types discussion also postponed to the next meeting - regular, special, and excluded users.

**Email forwarding**
- Concerns brought up around email forwarding will be listed at the next meeting. This list of concerns will then be brought up at an IT Executive Steering Committee meeting

**Decisions / Recommendations / Confirmations**

- Identification policy needs minor modifications before approval.
- Encryption policy may need modification depending on General Counsel’s response.
- Subcommittee will be formed to draft Data Breach policy. Subcommittee will include Carol, Joe, Diane, someone from Risk, and someone from UMC.

**Next Steps / Follow-ups**

Briefly describe any identified follow-up Tasks.

<table>
<thead>
<tr>
<th>#</th>
<th>Task</th>
<th>Owner</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Update PII Identification policy with recommended changes</td>
<td>Joe Bazeley</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Follow-up with General Counsel regarding contract language around 3rd parties handling sensitive data</td>
<td>Joe Bazeley</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Draft data breach response policy</td>
<td>Data breach subcommittee</td>
<td></td>
</tr>
</tbody>
</table>