Agenda

• Cellular Contracts and Support - Update
  – D. Vonder Heide

• **Personally Identifiable Information Policies**
  – L. Lauger

• System Proposal - ePortfolio & Assessment
  – C. Scheidenhelm, P. Green

• Recruitment CRM - System Replacement Update
  – P. Roberts, T. Heuer
PIP Policy Agenda

• Overview of PII on Workstations
• Risk Management Considerations
• Solutions
• ISAC Recommendations
• Proposed Policy Revisions
• Next Steps
Where is the PII now?

2009 = 25% of workstations contained PII
2010 = 9.7% of workstations contained PII
2011 = goal is for <5% of computers to have PII

<table>
<thead>
<tr>
<th>PII 2011 Status</th>
<th>2011</th>
<th>2010</th>
<th>2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Stewards Reporting</td>
<td>5</td>
<td>7.6%</td>
<td>67</td>
</tr>
<tr>
<td>Computers Scanned</td>
<td>192</td>
<td>7.7%</td>
<td>2483</td>
</tr>
<tr>
<td>Computers Encrypted</td>
<td>112</td>
<td>58.3%</td>
<td>1534</td>
</tr>
<tr>
<td>PII Found</td>
<td>25</td>
<td>13.0%</td>
<td>569</td>
</tr>
<tr>
<td>PII Left on Device</td>
<td>10</td>
<td>5.2%</td>
<td>242</td>
</tr>
</tbody>
</table>

Currently there are approximately 240 workstations containing PII.
Risk Management

• In 2010:
  – 690 known viruses/malware found on workstations
  – 3 system compromises
  – 3 account compromises
  – 5 thefts

• Encryption manages the risk for theft
  – However, malware and viruses introduce the risk that data can be stolen while the user is logged on to the computer

• Malware cannot be eliminated from the environment completely despite additional controls such as:
  – Antivirus software
  – Intrusion Prevention Systems
  – Security Awareness and Education Programs
How to address the risk?

• Do we want to revise the policies to prohibit PII on workstations?
• Can we enforce this? Does it matter if it is strictly enforced or monitored?
• Alternatively, do we recommend but not require not keeping PII on workstations?
The Information Security Advisory Council (ISAC) is recommending policy changes strictly prohibiting all PII on desktops.

- Risks outweigh the benefits of having the data locally
- Loyola has enterprise systems (e.g. Locus, ECM) and network storage for maintaining this data - no need to keep it on local workstations
- Reluctance to exempt Student Data
# ISAC Members

**Chair:** Leilani Lauger, *University Information Security Office*

<table>
<thead>
<tr>
<th>Department/Area</th>
<th>Primary</th>
<th>Alternate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Academic Affairs</td>
<td>Francesca Pirovano</td>
<td></td>
</tr>
<tr>
<td>Advancement</td>
<td>Ron Iwanski</td>
<td></td>
</tr>
<tr>
<td>Finance</td>
<td>Cory O’Brien</td>
<td></td>
</tr>
<tr>
<td>Financial Assistance</td>
<td>Tad Verdun</td>
<td>Eric Weems</td>
</tr>
<tr>
<td>Human Resources</td>
<td>Carol Mc Cormack</td>
<td>Mike Capulong</td>
</tr>
<tr>
<td>ITS - Infrastructure</td>
<td>Dave Wieczorek</td>
<td>Jeff Apa</td>
</tr>
<tr>
<td>ITS - Applications</td>
<td>Cheryl Heckel</td>
<td>Charlotte Pullen</td>
</tr>
<tr>
<td>Registration &amp; Records</td>
<td>Diane Hullinger</td>
<td>Eric Pittenger</td>
</tr>
<tr>
<td>Risk Management</td>
<td>Regina Ruffin</td>
<td>Sue Bodin</td>
</tr>
<tr>
<td>Student/Judicial Affairs</td>
<td>Dana Broadnax</td>
<td>Jeremy Inabinet</td>
</tr>
<tr>
<td>Ex-Officio</td>
<td>Jim Sibenaller</td>
<td></td>
</tr>
</tbody>
</table>
Proposed PII Policy Changes

• Summary of proposed policy revisions
  – No Loyola Protected Data may be stored on workstations or personal devices
    • Including thumb drives and mobile devices
    • Protected Data may be stored only on ITS-managed information resources such as file servers, application server or databases.
  – The physical transfer of Loyola Protected Data (e.g., via CD, USB drive, or other portable medium) is not allowed.
Next Steps

• Any changes made to the PIP policies go through the following approval steps, per the governance policy:
  1. Working Group
  2. ITS Directors
  3. Executive or Leadership Sponsor
  4. IT Executive Steering Committee
  5. General Counsel
  6. University Coordinating Committee
  7. President’s Cabinet