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

LOYOLA
UNIVERSITY CHICAGO

Preparing people to lead extraordinary lives

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

PII 2011 Status	2011		2010		2009	
Data Stewards Reporting	5	7.6%	67	100.0%		
Computers Scanned	192	7.7%	2483	106.9%	2322	
Computers Encrypted	112	58.3%	1534	61.8%	1302	56%
PII Found	25	13.0%	569	22.9%	573	25%
PII Left on Device	10	5.2%	242	9.7%		

Currently there are approximately 240 workstations containing PII.

Preparing people to lead extraordinary lives

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?

Perspective

- 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*

Department/Area	Primary	Alternate
Academic Affairs	Francesca Pirovano	
Advancement	Ron Iwanski	
Finance	Cory O'Brien	
Financial Assistance	Tad Verdun	Eric Weems
Human Resources	Carol Mc Cormack	Mike Capulong
ITS - Infrastructure	Dave Wieczorek	Jeff Apa
ITS - Applications	Cheryl Heckel	Charlotte Pullen
Registration & Records	Diane Hullinger	Eric Pittenger
Risk Management	Regina Ruffin	Sue Bodin
Student/Judicial Affairs	Dana Broadnax	Jeremy Inabinet
Ex-Officio	Jim Sibenaller	

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.

LOYOLA UNIVERSITY CHICAGO

Preparing people to lead extraordinary lives

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

LOYOLA
UNIVERSITY CHICAGO

Preparing people to lead extraordinary lives