When the Rubber Meets the Road:
Moving from IT Policy Development to Implementation

CUMREC 2005

Jaime Galiano
Project Director

Georgia Institute of Technology
Office of Information Technology – Policy & Strategy

This work is the intellectual property of the author. Permission is granted for this material to be shared for non-commercial, educational purposes, provided that this copyright statement appears on the reproduced materials and notice is given that the copying is by permission of the author. To disseminate otherwise or to republish requires written permission from the author.

© Georgia Institute of Technology, 2005
• Public Research University, part of the University System of Georgia (USG)
• Atlanta campus: 400-acre city campus
• Enrollment: 16,000+ students
• Over 250 autonomous academic, research, and administrative units
• Decentralized IT support
• IT Policy Development function reporting to CIO / AVP
Policy Development & Review

Full lifecycle policy development, refreshment and retirement

Issue Identification & Scope Definition → Research & Analysis (SMEs) → Stakeholder Input → Policy Drafting

Distribution & Adoption → Policy Approval → Draft Policy Posting & Comment

Policy Review

Policy Retirement

© Georgia Institute of Technology, 2005
Policy Distribution & Adoption: the way things *typically* are...

- Signed, sealed, delivered and…
  - Promptly forgotten
  - Blindly and zealously enforced, or
  - Never even (properly) communicated
- Even with the best of intentions, distribution and adoption activities are mostly ineffective
- Rather than being seen as “living documents”, IT policies are typically seen as “dead documents”
  - a necessary evil
Why?
Policy Adoption Issues & Challenges

- **Upstream** issues
  - Policy approvals
    - Management concerns
    - Rank-and-file concerns

- **Downstream** issues
  - Communication & Awareness
  - Implementation
  - Training
  - Monitoring
• Execute the Communication Plan
• Define and implement communication channels as necessary
• Personalize and target the messages
• Use a combination of “Push” and “Pull” mechanisms
  – **Push measures**: Memo of Transmittal, policy “click-throughs”, portal announcements, etc.
  – **Pull measures**: FAQs, “What’s New?”, support groups/mailing lists, etc.
• Evaluate risk at the departmental or unit level
• Qualify & quantify the risks
• Accept, Mitigate or Transfer the risk
  – Understand the implications of each option
  – Trade-off analysis involved (tangibles and intangibles)
• Document the proposed (or adopted) solution and related tasks
GIT Data Protection Safeguards


[2] Safeguard Guidelines by Data Category: M = Mandatory safeguard, R = Recommended, S = Suggested

[3] Measures: Procedures, processes and/or mechanisms to meet Internal Controls

Any deviation from mandatory requirements must be documented and covered by adequate compensating control(s). The department of Internal Auditing is available to assist in reviewing compensating controls.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>System Admin Physical</td>
<td>I</td>
<td>II</td>
<td>III</td>
<td>IV</td>
<td>1-1</td>
</tr>
<tr>
<td></td>
<td>X</td>
<td>R</td>
<td>M</td>
<td>M</td>
<td>1-2</td>
</tr>
<tr>
<td></td>
<td>X</td>
<td>X</td>
<td>R</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td></td>
<td>X</td>
<td>X</td>
<td>M</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td></td>
<td>X</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td></td>
<td>X</td>
<td>R</td>
<td>M</td>
<td>1-6</td>
<td>Procedures must exist so all personnel can easily distinguish between employees and visitors, especially in areas where sensitive information is accessible.</td>
</tr>
<tr>
<td></td>
<td>X</td>
<td>X</td>
<td>R</td>
<td>M</td>
<td>1-7</td>
</tr>
</tbody>
</table>

© Georgia Institute of Technology, 2005
Unit-level Implementation Example

GT Health Services - HIPAA Security Standard - Risk Assessment
(as measured against Data Protection Safeguards)

<table>
<thead>
<tr>
<th>Safeguard</th>
<th>Data Category</th>
<th>Ref. Item</th>
<th>Measures</th>
<th>Internal Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>S A P I I I I I I I I I I</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliant</td>
<td>Risk</td>
<td>Impact</td>
<td>Level</td>
<td>Pol#</td>
</tr>
</tbody>
</table>

1 - Control Physical access to data

<table>
<thead>
<tr>
<th></th>
<th>Compliant</th>
<th>Risk</th>
<th>Impact</th>
<th>Level</th>
<th>Pol#</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X R M M</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>e.g. Security alarms, card readers, locks, etc.</td>
<td>Institute physical security controls for each computer room, data center and other physical areas with systems that process and store data.</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Video cameras with active 24/7 monitoring in Operating Centers</td>
<td>Constant monitoring is in place using video cameras in data centers to monitor storing/processing sensitive data. (Note: This is not mandatory for paper process and storage areas whose access is physically supervised or restricted when unmanned.)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X R M M</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consoles for systems that store and/or transmit sensitive data are “locked” to prevent unauthorized use. (Note: this refers to cabinet mounted servers with doors)</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Item</td>
<td>Measures</td>
<td>Internal Control</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>----------</td>
<td>------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-1</td>
<td>e.g., Security cameras, card readers, locks, etc.</td>
<td>Institute physical security controls for each computer room, data center, and other physical areas with systems that process and store data.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-2</td>
<td>CCTV cameras with active 24/7 monitoring in computing centers</td>
<td>Continual monitoring is in place using video cameras in data centers to monitor working computer systems. (Note: This is not mandatory for paper processes and storage areas whose access is physically supervised or restricted when unoccupied.)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-3</td>
<td>Control for systems that store or transmit sensitive data are &quot;locked&quot; to prevent unauthorized use. (Note: This refers to cabinet mounted servers with doors)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-4</td>
<td>Physical disconnection of unused jacks, connection access, authentication, etc.</td>
<td>Active UTP network jacks are only accessible to authorized users.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-5</td>
<td>Network access controls should be maintained, locked with access only to authorized personnel.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-6</td>
<td>Procedures must exist so all personnel can easily distinguish between employees and visitors, especially in areas where sensitive information is accessed.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-7</td>
<td>ID badges. Visitor ID badges do not provide access to physical areas that store mission data.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Best Practices: DAP Implementation Guidelines

• **Data Classification Guidelines**
  – Mapping of typical data to data categories

• **Quick-Reference Checklists**
  – Single-page “to-do” lists by roles

• **Comprehensive guidelines**
  – User Guidelines
  – Administrator Guidelines
  – Hardware/Machine Guidelines
• Formal training program and materials
  – Staff
  – Faculty
  – Students
• Offer training through multiple delivery methods
  – Formal classes, one-on-one, CBT, user support groups, etc.
  – Self-assessments
Best Practices: Monitoring & Support

- Collaborative effort
- Triage
  - Policy issue
  - Implementation issue
  - Information Security issue
- Appropriate representation in core support group
- Adequate support at the unit-level
- Issue escalation
DAP Rollout Anecdotes

• Successes
  – GT Health Services
  – Enterprise Information Systems (EIS) sensitive data scans

• Challenges
  – Student information handled by graduate Teaching Assistants
  – Laptop computers and encryption