Guidelines for Data Protection

Doug Markiewicz
Policy and Compliance Coordinator

Information Security Office
www.cmu.edu/iso
• Information Security Policy
  – Published in December 2008
  – Motivations
    • Replace previous policy, which was published in 1990
    • Expand the scope of who and what the policy applies to
    • Accommodate a heterogeneous computing environment
    • Accommodate expanding regulatory requirements
    • Separate technical standards and administrative procedures from actual policy
• Information Security Policy

1. Throughout its lifecycle, all Institutional Data shall be protected in a manner that is considered reasonable and appropriate, as defined in documentation approved by the ESCC and maintained by the Information Security Office, given the level of sensitivity, value and criticality that the Institutional Data has to the University.

2. Any Information System that stores, processes or transmits Institutional Data shall be secured in a manner that is considered reasonable and appropriate, as defined in documentation approved by the ESCC and maintained by the Information Security Office, given the level of sensitivity, value and criticality that the Institutional Data has to the University.

3. Individuals who are authorized to access Institutional Data shall adhere to the appropriate Roles and Responsibilities, as defined in documentation approved by the ESCC and maintained by the Information Security Office.
• Information Security Roles & Responsibilities
• Guidelines for Data Classification
• Guidelines for Data Protection
• Guidelines for Data Disposal
• Guidelines for Data Retention
• Guidelines for Data Handling
• Procedure for Responding to a Security Breach
Information Security Policy Roadmap

- Information Security Roles & Responsibilities
- Guidelines for Data Classification
- Guidelines for Data Protection
  - Guidelines for Data Disposal
  - Guidelines for Data Retention
  - Guidelines for Data Handling
  - Procedure for Responding to a Security Breach
# Roles and Responsibilities

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibilities</th>
</tr>
</thead>
</table>
| **Director of Information Security** | • Develop an information security program  
• Coordinate IT security training and awareness  
• Respond to actual or suspected IT security threats |
| **Data Steward**              | • Determine appropriate criteria for access to data  
• Delegate responsibility for data to a “Data Custodians”  
• Oversee implementation of security controls  
• Approve operational policies and procedures  
• Approve how data is stored & used  
• Accept or reject risk related to security threats  
• Understand contractual and regulatory obligations |
| **Data Custodian**            | • Implement physical and technical security controls  
• Document administrative and operational procedures  
• Provision and deprovision access to data  
• Understand how data is stored and used  
• Understand IT security risks in greater detail |
| **User**                      | • Adhere to policies and procedures  
• Report actual or suspected IT security breaches |
Data Classification

Public

Data should be classified as Public when the unauthorized disclosure, alteration or destruction of that data would result in **limited risk** to the University and its affiliates.

Private

Data should be classified as Private when the unauthorized disclosure, alteration or destruction of that data could result in a **moderate level of risk** to the University or its affiliates.

Restricted

Data should be classified as Restricted when the unauthorized disclosure, alteration or destruction of that data could cause a **significant level of risk** to the University or its affiliates.
Data Classification

Public
Examples:
• Press release
• Course information
• Public web content
• Published research

Private
Examples:
• Interdepartmental documents
• Email communications
• Unpublished research

Restricted
Examples:
• Authentication verifiers
• Credit card numbers
• Federal tax information
• Financial account numbers
• Health information
• Passwords
• PII (e.g. SSN)
• Protected health information
Guidelines for Data Protection

• Purpose

“…to define baseline security controls for protecting Institutional Data, in support of the University’s Information Security Policy.”

• Roles & Responsibilities

  – Data Stewards: Oversee implementation of security controls
  – Data Custodians: Implement security controls

November 9, 2009
### Guidelines for Data Protection

#### Identifier Control Area

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Control Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS</td>
<td>Application Security (19)</td>
</tr>
<tr>
<td>DR</td>
<td>Disaster Recovery Planning (9)</td>
</tr>
<tr>
<td>EA</td>
<td>Electronic Access Control (16)</td>
</tr>
<tr>
<td>EN</td>
<td>Encryption (10)</td>
</tr>
<tr>
<td>IS</td>
<td>Information System Security (23)</td>
</tr>
<tr>
<td>NS</td>
<td>Network Security (11)</td>
</tr>
<tr>
<td>PS</td>
<td>Physical Security (7)</td>
</tr>
</tbody>
</table>

**Total = 95 Controls**

**Note:** These controls reflect a baseline set of requirements for Carnegie Mellon based on our current understanding of business need. While they are representative of industry standards, they are less numerous and onerous.
# Electronic Access Controls

<table>
<thead>
<tr>
<th>ID</th>
<th>Control</th>
<th>Public</th>
<th>Private</th>
<th>Restricted</th>
</tr>
</thead>
<tbody>
<tr>
<td>EA-1</td>
<td>Electronic access to Institutional Data and/or Information Systems is uniquely associated with an individual or system</td>
<td>Optional for READ access to data. Required for all other access.</td>
<td>Required</td>
<td>Required</td>
</tr>
<tr>
<td>EA-2</td>
<td>Electronic access to Institutional Data and/or Information Systems is authenticated</td>
<td>Optional for READ access to data. Required for all other access.</td>
<td>Required</td>
<td>Required</td>
</tr>
<tr>
<td>EA-3</td>
<td>Electronic access to Institutional Data and/or Information Systems is authenticated using multi-factor authentication</td>
<td>Optional</td>
<td>Recommended</td>
<td>Recommended</td>
</tr>
</tbody>
</table>
### Encryption Controls

<table>
<thead>
<tr>
<th>ID</th>
<th>Control</th>
<th>Public</th>
<th>Private</th>
<th>Restricted</th>
</tr>
</thead>
<tbody>
<tr>
<td>EN-1</td>
<td>Institutional Data transmitted over a network connection is encrypted</td>
<td>Optional</td>
<td>Recommended</td>
<td>Required</td>
</tr>
<tr>
<td>EN-2</td>
<td>Institutional Data stored on Electronic Storage Media is encrypted</td>
<td>Optional</td>
<td>Recommended</td>
<td>Recommended</td>
</tr>
<tr>
<td>EN-3</td>
<td>Institutional Data stored on portable Electronic Storage Media is encrypted</td>
<td>Optional</td>
<td>Recommended</td>
<td>Required</td>
</tr>
</tbody>
</table>
## Information Systems Security Controls

<table>
<thead>
<tr>
<th>ID</th>
<th>Control</th>
<th>Public</th>
<th>Private</th>
<th>Restricted</th>
</tr>
</thead>
<tbody>
<tr>
<td>IS-1</td>
<td>Controls are deployed to protect against unauthorized connections to services (e.g. firewalls, proxies, access control lists, etc.)</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
</tr>
<tr>
<td>IS-2</td>
<td>Controls are deployed to protect against malicious code execution (e.g. antivirus, antispyware, etc.)</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
</tr>
<tr>
<td>IS-3</td>
<td>Controls deployed to protect against malicious code execution are kept up to date</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
</tr>
</tbody>
</table>
Next Steps

- Ongoing vetting thru 05/2010 (Feedback to doug@cmu.edu)
- Benchmarking against industry standards
  - ISO 27002, NIST, PCI DSS, etc.
- Benchmarking against regulatory requirements
  - FISMA, GLBA, HIPAA, ITAR/EAR, etc.
- Real word testing
- Supporting documentation and tools
Links

Information Security Policy
http://www.cmu.edu/iso/governance/policies/information-security.html

Information Security Policy Roadmap

Information Security Roles & Responsibilities
http://www.cmu.edu/iso/governance/policies/information-security-roles.html

Guidelines for Data Classification
http://www.cmu.edu/iso/governance/guidelines/data-classification.html

Guidelines for Data Protection
http://www.cmu.edu/iso/governance/guidelines/data-protection/index.html

Data Protection Self Assessment Worksheet
Questions?