Carnegie Mellon

Guidelines for Data Protection

Doug Markiewicz
Policy and Compliance Coordinator

Information Security Office
www.cmu.edu/iso

Background

Carnegie Mellon

- 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

Background

Carnegie Mellon

- 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 Policy Roadmap

Carnegie Mellon

- 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

Carnegie Mellon

- 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

Carnegie Mellon

Role	Responsibilities
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

Carnegie Mellon

Public

Data should be classified as Public when the unauthorized disclosure, alteration or destruction of that data would results 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

Carnegie Mellon

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

Carnegie Mellon

- 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

Guidelines for Data Protection

Carnegie Mellon

Identifier	Control Area
AS	Application Security (19)
DR	Disaster Recovery Planning (9)
EA	Electronic Access Control (16)
EN	Encryption (10)
IS	Information System Security (23)
NS	Network Security (11)
PS	Physical Security (7)

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

ID	Control	Public	Private	Restricted
EA-1	Electronic access to Institutional Data and/or Information Systems is uniquely associated with an individual or system	Optional for READ access to data. Required for all other access.	Required	Required
EA-2	Electronic access to Institutional Data and/or Information Systems is authenticated	Optional for READ access to data. Required for all other access.	Required	Required
EA-3	Electronic access to Institutional Data and/or Information Systems is authenticated using multi-factor authentication	Optional	Recommended	Recommended

Encryption Controls

ID	Control	Public	Private	Restricted
EN-1	Institutional Data transmitted over a network connection is encrypted	Optional	Recommended	Required
EN-2	Institutional Data stored on Electronic Storage Media is encrypted	Optional	Recommended	Recommended
EN-3	Institutional Data stored on portable Electronic Storage Media is encrypted	Optional	Recommended	Required

Information Systems Security Controls

ID	Control	Public	Private	Restricted
IS-1	Controls are deployed to protect against unauthorized connections to services (e.g. firewalls, proxies, access control lists, etc.)	Required	Required	Required
IS-2	Controls are deployed to protected against malicious code execution (e.g. antivirus, antispyware, etc.)	Required	Required	Required
IS-3	Controls deployed to protected against malicious code execution are kept up to date	Required	Required	Required

Next Steps

Carnegie Mellon

- 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

Carnegie Mellon

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

Information Security Policy Roadmap
http://www.cmu.edu/iso/governance/policies/docs/InformationSecurityPolicyRoadmap.xls

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
http://www.cmu.edu/iso/governance/guidelines/data-protection/self-assessment.html

Questions?