Carnegie Mellon

Guidelines for Data Protection
Summary of Changes

Document Information	
Status	DRAFT
Published	09/15/2009
Last Updated	09/15/2011
Current Version	1.0

Revision History

Version	Published	Author	Description
0.12	09/15/2009	Doug Markiewicz	Updated with summary of changes for version 0.12.
0.13	09/23/2009	Doug Markiewicz	Updated with summary of changes for version 0.13.
0.14	01/22/2010	Doug Markiewicz	Updated with summary of changes for version 0.14.
1.0	09/15/2011	Doug Markiewicz	Updated with summary of changes for version 1.0.

Table of Contents

Version 0.12

The following provides a comprehensive listing of changes made to the Guidelines for Data Protection moving from version 0.11 to 0.12. Also provided is a list of issues that have been deferred to a future release of the guidelines as well as some noteworthy comments that were provided that did not warrant change or further investigation.

Summary of Changes

Approach

1. Made the following changes in the identifiers table to reflect sections that were renamed. See additional information is respective sections.
    - Changed “Business Continuity and Disaster Recovery Planning” to “Disaster Recovery Planning”
    - Removed “, Signing” from the name of the Encryption and Key Management section

2. Made the following changes in the identifiers table to better align identifiers with their section names
    - Changed “BC” to “DR”
    - Changed “AC” to “EA”
    - Changed “ES” to “EN”

Application Security

3. Appended the introductory paragraph with a portion of the content that was previously in the Supplemental Guidance subsection in order to increase its visibility.

4. Removed “A software development lifecycle is documented and followed” (previously AS-1) as a control in the Application Development subsection. This control extends beyond the scope of this document and the intent is largely encapsulated in AS-1 (previously AS-2). Renumbered subsequent controls.

5. Replaced “Application development includes review for design, logic and implementation related security vulnerabilities prior to implementation in a production environment” with “Application development includes review for security vulnerabilities throughout the development lifecycle” as control AS-1 (previously AS-2).

6. Replaced “…those types of input that are…” with “…those data types that are…” in AS-4 (previously AS-5) to improve clarity. Added supplemental guidance related to control.

7. Replaced “Application sessions are uniquely identified” with “Application sessions are uniquely associated with an individual or system” in AS-8 (previously AS-9) in order to provide consistency in language with EA-1 (previously AC-1).

8. Replaced “…following client authentication” with “…following a change in the access profile of a user or system” in AS-10 (previously AS-11) to alleviate some confusion. Inserted supplemental guidance to further explain this requirement.

9. Removed “Session identifiers are regenerated following a change in access privileges” (previously AS-12) because it is encapsulated in the updated language for AS-10 (previously AS-11). Renumbered subsequent controls.

10. Changed the ratings for Public and Private data in AS-14 (previously AS-16) from “Required” to “Required for privileged access; Recommended for all other access” in order to make the control more scalable.

11. Replaced "All attempts to execute a command that requires privileged access to an application are logged" with "Attempts to execute and administrative command are logged" for AS-16 (previously AS-18) to improve clarity. Inserted supplemental guidance to further explain this requirement.

Disaster Recovery Planning

12. Appended the introductory paragraph with the content that was previously in the Supplemental Guidance subsection in order to increase its visibility. Removed the Supplemental Guidance subsection.

13. Renamed the "Business Continuity and Disaster Planning" section to "Disaster Recovery Planning" due to comments that business continuity was beyond the scope of this document and that the focus should be on disaster recovery planning only. Renamed the "Business Continuity Planning" subsection to "Disaster Recovery Planning" to reflect this same change in scope. Changed the "BC" identifier to "DR" to align with the name change.

14. Changed "Business continuity" to "Disaster recovery" in DR-1 and DR-2 (previously BC-1 and BC-2) to reflect the change in scope of this section.

15. Removed "formally" from DR-4 (previously BC-4) for brevity and clarity.

Electronic Access Control

16. Appended the introductory paragraph with a portion of the content that was previously in the Supplemental Guidance subsection in order to increase its visibility.

17. Changed the identifier for each control from "AC" to "EA" to better reflect the name of the section.

18. Replaced "Remote access to Institutional Data and/or Information Systems is…" with "Electronic access to Institutional Data and/or Information Systems that traverses the Internet is…" in EA-4 (previously AC-4). This change was made to improve the clarity of the control.

19. In EA-9 (previously AC-9), changed the control rating for Public data from "Required for all other access." To "Recommended for all other access." in order to make it consistent with the control rating for Private.

20. Appended EA-12 thru EA-16 (previously AC-12 thru AC-16) with a * indicating that supplemental guidance exists for these controls.

21. Labeled supplemental guidance with the relevant control identifiers.

Encryption and Key Management

22. Changed the identifier for each control from "ES" to "EN" to better reflect the name of the section.

23. Renumbered controls EN-3 through EN-10 (previously ES-3 through ES-10) to EN-2 through EN-9 due to a typographical error that left out EN-2 (previously ES-2) as a control identifier.

24. Replaced "Data at rest or in storage is encrypted" with "Institutional Data stored on Electronic Storage Media I encryption" in EN-3 (previously ES-4). This change was made to improve clarity and align with previously defined terminology.

25. Replaced “Data stored on removable storage media is encrypted” with “Institutional Data stored on portable Electronic Storage Media is encryption” in EN-4 (previously ES-5). This change was made to improve clarity and align with previously defined terminology.

Information System Security

26. Appended the introductory paragraph with the content that was previously in the Supplemental Guidance subsection in order to increase its visibility. Removed the Supplemental Guidance subsection.

27. Replaced “All attempts to execute a command that requires privileged access to an application are logged” with “Attempts to execute and administrative command are logged” for IS-18 (previously AS-18) to improve clarity. Inserted supplemental guidance to further explain this requirement.

Network Security

28. Appended the introductory paragraph with a portion of the content that was previously in the Supplemental Guidance subsection in order to increase its visibility.

29. Appended NS-1, NS-7 and NS-9 with a * indicating that supplemental guidance exists for these controls.

30. Inserted supplemental guidance on NS-7.

31. Labeled existing supplemental guidance with relevant control identifiers (NS-1 and NS-9).

Additional Information

32. Removed “and Categorization” from the reference to the Guidelines for Data Classification. This document was previously entitled Guidelines for Data Classification and Categorization but was shorted for brevity and clarity.

Deferred Issues

The following is a list of issues that have been deferred to a future version of this Guideline.

1. Numerous comments were received related to whether or not ratings were appropriate for a given control. With the exception of a few areas where changes were made to clear up inconsistencies in the Guidelines, these comments have been deferred to a future release. This decision was made to allow sufficient time to complete real world testing of the Guidelines and to complete a mapping of the Guidelines to both industry practices and regulatory obligations. Following completion of this work, ratings will be re-evaluated and a revision will be published.

2. Several comments were received pointing out that having logging controls in multiple sections and structuring them in a manner that creates the potential for overlap may lead to confusion. This issue has been deferred to allow more time to test the current format in real-world scenarios and to investigate viable alternatives.

3. One comment was received pointing out that there are no controls defined to address the security of institutional data communicated vocally (e.g. sound proof walls). This issue has been deferred to allow time to more fully understand industry practices and any potential legal obligations.

4. Several comments were received requesting a clear definition of the terms “periodic”, “periodically” and “timely” as it is used throughout the Guideline. This issue has been deferred to allow additional time to

investigate industry practices and any potential legal obligations. Initial investigations show that existing structure is consistent with industry practice. This is in recognition of the fact that the unique circumstances of a given business unit will play an important role in defining these terms. At a minimum, the Information Security Office will look to provide some examples of industry practice.

Additional Comments

The following is a list of additional comments that did not warrant a change or additional investigation.

1. One comment was received pointing out that the Guidelines do not address the use of production data in a test environment. Appropriate use of institutional data is beyond the scope of this document. Regardless of whether an environment is considered test or production, security controls should be implemented in a manner that is consistent with the appropriate data classification.

2. Several comments were received pointing out that the Guidelines are not clear on roles and responsibilities. The Information Security Roles and Responsibilities point out that Data Custodians are responsible for implementing security controls. Data Stewards are responsible for assigning this responsibility to one or more Data Custodians and then overseeing implementation.

3. Several comments were received pointing out that the Guidelines would be difficult for a typical end user to interpret despite the fact that a typical end user may carry some responsibility for protecting data related to his or her own computer. The Information Security Office plans to publish supplemental guidance that specifically targets a typical end user and his or her role in protecting institutional data.

4. One comment was received requesting guidance on retention of logs. The Information Security Office plans to publish Guidelines for Data Retention to address this issue.

5. Numerous comments were received indicating a desire for real-world examples of how to implement each security control. The Information Security Office is planning several real-world tests of these Guidelines that would result in a case study report; however, comprehensive documentation on how to implement each control is currently beyond the scope of planned activities. The Information Security Office will continue to evaluate opportunities to provide supplemental guidance both within the Guidelines for Data Protection and in other supporting documentation.

Version 0.13

The following provides a comprehensive listing of changes made to the Guidelines for Data Protection moving from version 0.12 to 0.13.

Summary of Changes

Approach

1. Modified language preceding the control areas table for brevity and to improve flow.

2. Removed "If you would like assistance with this evaluation, contact the Information Security Office by email at iso@andrew.cmu.edu." Similar information is already included in the Additional Information section.

Application Security

3. In the second paragraph, replaced "…placement of these components into network segments with varying degrees of security…" with "…placement of these components into network segments with appropriate degrees of security…" to improve clarity.

4. In the second paragraph, removed "The Information Security Office is available to assist business units in reviewing the security implications of an application's architectural design." Similar information is already included in the Additional Information section.

5. In AS-16, changed the control rating from Required to Recommended for Restricted data. This change was made based upon a reevaluation of its reasonableness.

6. Corrected grammatical error in supplemental guidance for AS-12 by replacing "they" with "it" in the first sentence.

Disaster Recovery

7. Changed all identifiers from "BC" to "DR" to accurately reflect the name of the section.

8. Replaced "…below controls…" with "…controls below…" in the introductory paragraph to improve the flow of the sentence.

9. Removed "formally" from controls DR-1 and DR-3 (previously BC-1 and BC-3) to alleviate any potential confusion in terms of what constitutes "formal" documentation. Both controls simply require documentation. Business units should determine an appropriate level of documentation for their own unique circumstances.

10. In DR-5, DR-8 and DR-9 (previously BC-5, BC-8 and BC-9), changed the control rating from Required to Recommended for Restricted data. An analysis of business impact should ultimately determine whether or not these controls are implemented.

Electronic Access Controls

11. Replaced “This section deals with direct access to Institutional Data” with “The Electronic Access Controls section deals with direct access to Institutional Data” to clear up confusion about which section this sentence was referring to in the supplemental guidance for EA-12 thru EA-16.

Information System Security

12. Corrected a typographical error in IS-1 by replacing “protection” with “protect.”

13. Corrected two typographical errors in supplemental guidance for IS-18 by replacing “them” with “thumb” and making “require” plural in the second to last sentence.

Network Security

14. In the supplemental guidance for NS-1, removed “The Information Security Office can assist with reviewing the security implications of a network’s architectural design.” Similar information is already included in the Additional Information section.

15. Corrected a typographical error in supplemental guidance for NS-7 by replacing “Messaging signing…” with “Message signing…” in the third sentence.

16. In the supplemental guidance for NS-9, removed “The Information Security Office can provide further assistance with evaluating and selecting appropriate controls for prevent network-based attacks.” Similar information is already included in the Additional Information section.

Version 0.14

The following provides a comprehensive listing of changes made to the Guidelines for Data Protection moving from version 0.13 to 0.14.

Summary of Changes

Physical Security

1. Reversed the order of PS-1 and PS-2 to provide for more logical flow.

2. In PS-1 (previously PS-2), replaced “Physical access to Information Systems that store, process or transmit Institutional Data is authorized by an appropriate Data Steward or a delegate” with “Physical access to Institutional Data and/or Information Systems is authorized by an appropriate Data Steward or a delegate prior to provisioning” in order to align the control more closely with EA-7 and to ensure protection of both data and systems.

3. In PS-3, replaced “paper” with “written or printed” in order to improve clarity and removed examples.

4. Inserted supplemental guidance for PS-1 (previously PS-2).

5. Inserted supplemental guidance for PS-3.

Version 1.0

The following provides a comprehensive listing of changes made to the Guidelines for Data Protection moving from DRAFT version 0.14 to version 1.0. In addition to these changes, the status of this document will be changed from DRAFT to FINAL.

Date of Publication

Version 1.0 of the Guidelines for Data Protection was published on 09/15/2011.

Summary of Changes

Definitions

1. Inserted the definition of "Media" in support of the new Media Sanitization and Disposal section.

2. Replaced "Electronic Storage Media" with "Electronic Media" and updated definition in order to eliminate redundancy with the definition of Media.

3. Updated definition of "Information System" to site specific examples, including desktop computers, laptops, multi-function printers, PDAs, smart phones, servers and tablet devices.

Approach

4. Updated total number of control areas from 7 to 8.

5. Updated Identifier table to reflect a new Media Sanitization and Disposal section.

Encryption

6. Replaced "The following tables define baseline encryption, signing and key management controls for protecting Institutional Data at rest or in transmission." with "The following tables define baseline encryption and key management controls for protecting Institutional Data."

7. Replaced "Electronic Storage Media" with "Electronic Media" in EN-2 and EN-3 to reflect a change in terminology.

Information System Security

8. Replaced "electronic storage media" with "electronic media" in IS-9 to reflect a change in terminology.

Media Sanitization and Disposal

9. Inserted a new section titled Media Sanitization and Disposal. This section replaces the Guidelines for Data Sanitization and Disposal document.

Physical Security

10. Replaced "printed" with "paper" in PS-3 to better align with the definition of Media.

Additional Information

11. Removed reference to the Guidelines for Data Retention. This reference was included in previous versions in anticipation of a draft document. Since the Guidelines for Data Retention have not been drafted, the reference is being removed.

12. Removed reference to the Guidelines for Data Sanitization and Disposal. This guidance is being replaced with the Media Sanitization and Disposal section of the Guidelines for Data Protection.