Carnegie Mellon

Guidelines for Data Protection

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

Carnegie Mellon

Revision History

Version	Published	Author	Description
0.1	07/23/2008	Doug Markiewicz	Original draft
0.2	10/21/2008	Doug Markiewicz	Added Access Control and Encryption sections.
0.3	12/05/2008	Doug Markiewicz	Modified Access Control section and added Backup & Recovery section and Physical Security section.
0.4	01/14/2009	Doug Markiewicz	Reorganized controls.
0.5	04/16/2009	Doug Markiewicz	Added Approach section and made updates to all other sections with the exception of Purpose and Definitions.
0.6	04/20/2009	Doug Markiewicz	Corrected table numbering.
0.7	04/21/2009	Doug Markiewicz	Corrected error in Table 1 where Public was mapped to the Restricted definition and vice versa.
0.8	05/01/2009	Doug Markiewicz	Modified Access Controls to include access to information systems. Separated Auditing into its own section (previous part of Access Control). Added Information System Security. Inserted AC-10 and ES-7. Updated Approach section where appropriate.
0.9	05/15/2009	Doug Markiewicz	Updated all sections based on feedback provided by the Information Security Office. Renamed Backup and Recovery to Business Continuity and Disaster Planning. Merged Auditing with other sections.
0.10	06/01/2009	Doug Markiewicz	Inserted Application Security and Network Security.
0.11	06/23/2009	Doug Markiewicz	Updated based on additional feedback provided by the Information Security Office.
0.12	09/15/2009	Doug Markiewicz	See Summary of Changes.
0.13	09/23/2009	Doug Markiewicz	See Summary of Changes.
0.14	01/22/2010	Doug Markiewicz	Updated PS-1 and PS-3 and inserted supplemental guidance for each. See Summary of Changes for additional details.
0.15	01/14/2011	Doug Markiewicz	See Summary of Changes.
1.0	08/23/2011	Doug Markiewicz	Added section on Media Sanitization and Disposal. See Summary of Changes for more details.
1.0	09/15/2011	Doug Markiewicz	Removed DRAFT designation.

Carnegie Mellon

Table of Contents

Carnegie Mellon

Purpose

The purpose of these Guidelines is to define baseline security controls for protecting Institutional Data, in support of the University's Information Security Policy.

Applies To

This Policy applies to all faculty, staff and third-party Agents of the University as well as any other University affiliate who is authorized to access Institutional Data. In particular, this Guideline applies to those who are responsible for protecting Institutional Data, as defined by the Information Security Roles and Responsibilities.

Definitions

Electronic Media is defined as any media that records and/or stores data using an electronic process. This includes but is not limited to internal and external hard drives, CDs, DVDs, Floppy Disks, USB drives, ZIP disks, magnetic tapes and SD cards.

Information System is defined as any electronic system that can be used to store, process or transmit data. This includes but is not limited to servers, desktop computers, laptops, multi-function printers, PDAs, smart phones and tablet devices.

Institutional Data is defined as any data that is owned or licensed by the University.

Least Privilege is an information security principle whereby a user or service is provisioned the minimum amount of access necessary to perform a defined set of tasks.

Media is defined as any materials that can be used to record and/or store data. This includes but is not limited to electronic media (see definition above), paper-based media and other written media (e.g. whiteboards).

Multi-factor Authentication is the process by which more than one factor of authentication is used to verify the identity of a user requesting access to resources. There are three common factors of authentication: something you know (e.g. password, pin, etc.), something you have (e.g. smart card, digital certificate, etc.) and something you are (e.g. fingerprint, retinal pattern, etc.). Use of username and password combination is considered single-factor authentication, even if multiple passwords are required. Username and password used in conjunction with a smartcard is two-factor authentication. Multi-factor authentication represents the use of two or three factors.

Privileged Access is defined as a level of access above that of a normal user. This definition is intentionally vague to allow the flexibility to accommodate varying systems and authentication mechanisms. In a traditional Microsoft Windows environment, members of the Local Administrators, Domain Administrators and Enterprise Administrators groups would all be considered to have privileged access. In a traditional UNIX or Linux environment, users with root level access or the ability to sudo would be considered to have privileged access. In an application environment, users with 'super-user' or system administrator roles and responsibilities would be considered to have privileged access.

Carnegie Mellon

Approach

The University's Information Security Policy states that all Institutional Data must be protected in a reasonable and appropriate manner based on the level of sensitivity, value and/or criticality that the data has to the University. This requirement acknowledges that different types of data require different sets of security controls. The University has defined three classifications of data for this purpose: Public, Private and Restricted. The following is a brief explanation of each. For more information, see the Guidelines for Data Classification.

Classification	Definition
Public	Data should be classified as Public when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to the University and its affiliates. Examples of Public data include press releases, course information and research publications. While little or no controls are required to protect the confidentiality of Public data, some level of control is required to prevent unauthorized modification or destruction of Public data.
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. By default, all Institutional Data that is not explicitly classified as Restricted or Public data should be treated as Private data. A reasonable level of security controls should be applied to Private data.
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. Examples of Restricted data include data protected by state and/or federal regulations and data protected by confidentiality agreements or other contractual obligations. The highest level of security controls should be applied to Restricted data.

This Guideline defines eight control areas. They are as follows:

Identifier	Control Area
AS	Application Security
DR	Disaster Recovery
EA	Electronic Access Control
EN	Encryption
IS	Information Systems Security
ME	Media Sanitization and Disposal
NS	Network Security
PS	Physical Security

Within each control area is a collection of security controls. Each security control is assigned a unique identifier consisting of two letters and a number. The letters represent the control area, as denoted above in the table, and the number simply provides uniqueness. Each security control is then assigned three control ratings, one for each classification of data, illustrating whether the control is appropriate. These control ratings are defined as follows.

Control Rating	Definition
Optional	The security control is optional for the designated classification. This does not imply that the control should not be implemented. Business units that would like to go above and beyond baseline requirements are encouraged to evaluate all controls for appropriateness.

Control Rating	Definition
Recommended	The security control is recommended for the designated classification of data but is not required due to limitations in available technology or because the control could potentially place an undue burden on a business unit to implement. Business units should document their justification for not implementing a 'Recommended' security control and whether or not a compensating control has been implemented.
Required	The security control is required for the designated classification of data. In situations where a 'Required' security control cannot be implemented, the Procedure for Policy Exception Handling should be followed. This process allows for a more formalized tracking and approval of security risks across the University.

This Guideline reflects a common set of controls that are appropriate across the entire University. It is important to note that additional or more specific security controls may be required based on individual business requirements (e.g. contractual and/or regulatory obligations). Many Industry business practices and regulatory requirements have been considered in the development of this Guideline; however, it may not be comprehensive in certain situations. Business units should consider mapping contractual and/or regulatory obligations to this Guideline to ensure there are no gaps in their own controls.

Carnegie Mellon

Application Security

The following tables define baseline application security controls for protecting institutional data, including secure development, vulnerability management and auditing. Security controls defined throughout the other portions of this document also play an important role in application security and should be reviewed prior to designing or implementing a new application. Special attention should be paid to the Electronic Access Control section and the Encryption and Key Management section.

In addition to the following controls, consideration should be given to the security impact of an application's architectural design. For example, the separation of application components (e.g. frontend, application service, database service, etc.) onto separate hosts can help reduce the risk of a compromise to one of the individual components. Similarly, placement of these components into network segments with appropriate degrees of security can also help protect the application as a whole. For example, it might be appropriate to place an application's database server on a more restrictive network segment than the application's frontend service. The type of institutional data involved and available resources will both play an important role in making architecture decisions.

Application Development

ID	Controls	Public	Private	Restricted
AS-1	Application development includes reviews for security vulnerabilities throughout the development lifecycle	Recommended	Recommended	Required
AS-2	Application change control procedures are documented and followed	Recommended	Recommended	Required
AS-3	Controls are in place to protect the integrity of application code	Recommended	Recommended	Required
AS-4	Application validates and restricts input, allowing only those data types that are known to be correct *	Required	Required	Required
AS-5	Application executes proper error handling so that error messages do not reveal potentially harmful information to unauthorized users (e.g. detailed system information, database structures, etc.)	Required	Required	Required
AS-6	Default and/or vendor supplied credentials are changed or disabled prior to implementation in a staging or production environment	Required	Required	Required
AS-7	Functionality that allows the bypass of security controls is removed or disabled prior to implementation in a staging or production environment	Required	Required	Required

Session Management

ID	Controls	Public	Private	Restricted
AS-8	Application sessions are uniquely associated with an individual or system	Recommended for READ access; Required for all other access	Required	Required
AS-9	Session identifiers are generated in a manner that makes them difficult to guess	Required	Required	Required
AS-10	Session identifiers are regenerated following a change in the access profile of a user or system *	Required	Required	Required
AS-11	Active sessions timeout after a period of inactivity	Recommended	Recommended	Required

Vulnerability Management

ID	Controls	Public	Private	Restricted
AS-12	Applications are periodically tested for security vulnerabilities (e.g. vulnerability scanning, penetration testing, etc.)	Recommended	Recommended	Required
AS-13	Application security patches are deployed in a timely manner	Required	Required	Required

Application Logging

ID	Controls	Public	Private	Restricted
AS-14	Successful attempts to access an application are logged	Required for privileged access; Recommended for all other access	Required for privileged access; Recommended for all other access	Required
AS-15	Failed attempts to access an application are logged	Required for privileged access; Recommended for all other access	Required for privileged access; Recommended for all other access	Required
AS-16	Attempts to execute an administrative command are logged *	Recommended	Recommended	Recommended
AS-17	Changes in access to an application are logged (e.g. adding, modifying or revoking access)	Required	Required	Required
AS-18	Application logs are reviewed on a periodic basis for security events	Recommended	Recommended	Required
AS-19	Application logs are protected against tampering	Required	Required	Required

Supplemental Guidance

AS-05: Input validation plays an important part in application security. For example, if a data entry field is asking for a phone number, the application should validate that the value entered matches a format similar to (###) ###-####. If a data entry field is asking for a date, the application should validate that the value entered matches a format similar to MM/DD/YYYY. If an application does not have controls in place to validate input, a malicious user may be able to enter data that results in unintended consequences, such as application failure or unauthorized access to potentially sensitive data.

AS-12: Not only should a session identifier (SID) be unique to an individual or system but it should also be unique to an individual's or system's access profile. For example, a user has a certain access profile prior to authenticating. This access profile may consist of limited functionality and access to a very limited subset of data. Once authenticated, a user may have access to increased functionality and a larger data set. A new SID should be generated and associated with this authenticated access. Similarly, a user may be able to enter a secondary set of credentials in order to gain access to administrative functionality. A new SID should be generated and associated with this administrative access. If a user has both a user session and an administrative session active, that user would have two different SIDs associated with two different sets of actions.

AS-17: Administrative commands are those commands that typically require some level of privileged access to execute. For example, adding and deleting users of an application, resetting a user's password and modifying how an application is configured are all examples of administrative commands that should be logged. Execution of administrative commands may occur through some type of command-line interface or they may occur through access to a graphical user interface. The full scope of administrative commands that should be logged may vary from application to application depending on the application's inherent functionality, the platform(s) it runs on top of or interacts with.

Carnegie Mellon

Disaster Recovery

The following tables define baseline controls for protecting the availability of Institutional Data and ensuring the continuity of business operations during an unplanned event. The extent to which business continuity and disaster planning controls are implemented should be based on an analysis of the business impact should a particular data set become unavailable. Available human and financial resources will also go into the decision making process. If there is little or no impact to the University should a particular data set become unavailable, the backup and recovery strategy may be to accept the risk of not having backups. The appropriate Data Steward should be involved in any decision to not backup Institutional Data. If such a strategy is approved, some of the controls below may not be applicable. It is also important to note that backup copies of institutional data should retain the same classification as their production copy.

Disaster Recovery Planning

ID	Controls	Public	Private	Restricted
DR-1	A disaster recovery plan is documented	Recommended	Recommended	Required
DR-2	Disaster recovery plans are periodically tested	Recommended	Recommended	Required

Backup and Recovery Controls

ID	Controls	Public	Private	Restricted
DR-3	A backup and recovery strategy for Institutional Data is documented	Required	Required	Required
DR-4	Backup and recovery procedures are documented and followed	Required	Required	Required
DR-5	Backup and recovery procedures are periodically tested	Recommended	Recommended	Recommended
DR-6	Backup copies of data are accurately inventoried	Required	Required	Required
DR-7	Content and physical location of removable backup media is tracked	Required	Required	Required
DR-8	Removable backup media is periodically validated	Recommended	Recommended	Recommended
DR-9	Backup copies of data are stored in a secondary location that is not in close proximity to the primary location (e.g. secondary datacenter, third-party storage site, etc.)	Recommended	Recommended	Recommended

Carnegie Mellon

Electronic Access Controls

The following tables define baseline security controls for authentication, authorization and auditing of electronic access to Institutional Data and/or Information Systems that store, process or transmit Institutional Data. Controls in this section apply to user access as well as system and/or service access.

Authentication

ID	Controls	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
EA-4	Electronic access to Institutional Data and/or Information Systems that traverses the Internet is authenticated using multi-factor authentication	Optional for READ access to data. Recommended for all other access.	Recommended	Required
EA-5	Electronic access to Institutional Data and/or Information Systems is re-authenticated after a period of inactivity	Optional for READ access to data. Recommended for all other access.	Recommended	Required
EA-6	Where username and password authentication is employed, passwords are managed according to the Guidelines for Password Management	Recommended	Recommended	Required

Authorization

ID	Controls	Public	Private	Restricted
EA-7	Electronic access to Institutional Data and/or Information Systems is authorized by a Data Steward or a delegate prior to provisioning	Optional for READ access. Required for all other access.	Required	Required
EA-8	Electronic access to Institutional Data and/or Information Systems is authorized based on a business need	Optional for READ access. Recommended for all other access.	Recommended	Required

ID	Controls	Public	Private	Restricted
EA-9	Electronic access to Institutional Data and/or Information Systems is based on the principle of least privilege	Optional for READ access. Recommended for all other access.	Recommended	Required
EA-10	Electronic access to Institutional Data is reviewed and reauthorized by a Data Steward or a delegate on a periodic basis	Optional for READ access. Recommended for all other access.	Recommended	Required
EA-11	Electronic access is promptly revoked when it is no longer necessary to perform authorized job responsibilities	Optional for READ access. Required for all other access.	Required	Required

Access Logging

ID	Controls	Public	Private	Restricted
EA-12	Successful attempts to access Institutional Data in electronic form are logged *	Optional for READ access. Recommended for all other access.	Optional for READ access. Recommended for all other access.	Optional for READ access. Recommended for all other access.
EA-13	Failed attempts to access Institutional Data in electronic form are logged *	Optional for READ access. Recommended for all other access.	Optional for READ access. Recommended for all other access.	Required
EA-14	Changes in access to Institutional Data in electronic form are logged *	Required	Required	Required
EA-15	Electronic access logs are reviewed on a periodic basis for security events *	Recommended	Recommended	Required
EA-16	Electronic access logs are protected against tampering *	Required	Required	Required

Supplemental Guidance

EA-12 thru EA-16: Auditing access to Institutional Data occurs at various levels. As a result, similar requirements exist in the Application Security and the Information Systems Security sections. In some situations, the same set of controls may fulfill all three sets of requirements. For example, EA-12 is similar to AS-14 and IS-16. While all three deal with logging of successful access attempts, each deals with a unique type of access. The Electronic Access Controls section deals with direct access to Institutional Data. It is also important to note that audit logs should be classified and protected just like any other data set. The type of data that exists in a log will help determine the appropriate classification for that log. For example, if a log file contains passwords, security controls should be implemented consistent with the Restricted classification since Appendix A of the Guidelines for Data Classification defines Authentication Verifiers as Restricted information.

Carnegie Mellon

Encryption

The following tables define baseline encryption and key management controls for protecting Institutional Data.

Encryption

ID	Controls	Public	Private	Restricted
EN-1	Institutional Data transmitted over a network connection is encrypted	Optional	Recommended	Required
EN-2	Institutional Data stored on Electronic Media is encrypted	Optional	Recommended	Recommended
EN-3	Institutional Data stored on portable Electronic Media is encrypted	Optional	Recommended	Required
EN-4	Data stored on a mobile computing device is encrypted	Optional	Recommended	Required
EN-5	Remote administration of an Information System is performed over an encrypted network connection	Required	Required	Required

Key Management

ID	Controls	Public	Private	Restricted
EN-6	Industry accepted algorithms are used where encryption and/or digital signing are employed	Recommended	Required	Required
EN-7	Key sizes of 128-bits or greater are used where symmetric key encryption is employed *	Recommended	Required	Required
EN-8	Key sizes of 1024-bit or greater are used where asymmetric key encryption is employed *	Recommended	Required	Required
ENS-9	Keys are changed periodically where encryption is employed	Recommended	Required	Required
EN-10	Keys are revoked and/or deleted when they are no longer needed to perform a business function	Recommended	Required	Required

Supplemental Guidance

ES-7 / ES-8: These controls establish baseline key sizes for symmetric key encryption (e.g. AES and 3DES) and asymmetric encryption (e.g. RSA and Diffie-Hellman). However industry trends illustrate a gradual movement toward larger key sizes. For example, the National Institute of Standards and Technology now requires 256-bit and 2048-bit keys for certain aspects of personal identity verification when dealing with federal information systems (see Special Publication 800-78). Data Custodians should evaluate any contractual obligations that might exist when selecting an appropriate key size.

Carnegie Mellon

Information System Security

The following tables define baseline security controls for protecting Information Systems that store, process or transmit Institutional Data. By definition, an Information System is any electronic system that stores, processes or transmits Institutional Data. This may include workstations, servers, mobile devices (e.g. smart phones, PDAs, etc.) or network devices (e.g. firewalls, routers, etc.). Controls defined in other portions of this document (e.g. Electronic Access Controls, Encryption and Key Management, etc.) also impact the security of Information Systems and should be reviewed to ensure comprehensive implementation of controls.

System Hardening

ID	Controls	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 protect against malicious code execution (e.g. antivirus, antispyware, etc.)	Required	Required	Required
IS-3	Controls deployed to protect against malicious code execution are kept up to date (e.g. software version, signatures, etc.)	Required	Required	Required
IS-4	Host-based intrusion detection and/or prevention software is deployed and monitored	Recommended	Recommended	Recommended
IS-5	Local accounts that are not being utilized are disabled or removed	Required	Required	Required
IS-6	Default or vendor supplied credentials (e.g. username and password) are changed prior to implementation	Required	Required	Required
IS-7	Services that are not being utilized are disabled or removed	Required	Required	Required
IS-8	Applications that are not being utilized are removed	Recommended	Recommended	Recommended
IS-9	Auto-run for removable Electronic Media (e.g. CDs, DVDs, USB drives, etc.) and network drives is disabled	Required	Required	Required
IS-10	Active sessions are locked after a period of inactivity	Required	Required	Required
IS-11	Native security mechanisms are enabled to protect against buffer overflows and other memory based attacks (e.g. address space layout randomization, executable space protection, etc.)	Recommended	Recommended	Recommended

Vulnerability Management

ID	Controls	Public	Private	Restricted
IS-12	Procedures for monitoring for new security vulnerabilities are documented and followed	Required	Required	Required
IS-13	Operating system and software security patches are deployed in a timely manner	Required	Required	Required
IS-14	Mitigating controls are deployed for known security vulnerabilities in situations where a vendor security patch is not available	Required	Required	Required
IS-15	System is periodically tested for security vulnerabilities (e.g. vulnerability scanning, penetration testing, etc.)	Recommended	Recommended	Required

System Logging

ID	Controls	Public	Private	Restricted
IS-16	Successful attempts to access Information Systems are logged	Required	Required	Required
IS-17	Failed attempts to access Information Systems are logged	Required for privileged access. Recommended for all other access.	Required for privileged access. Recommended for all other access.	Required
IS-18	Attempts to execute an administrative command are logged *	Recommended	Recommended	Required
IS-19	Changes in access to an Information System are logged	Required	Required	Required
IS-20	Changes to critical system files (e.g. configuration files, executables, etc.) are logged	Recommended	Recommended	Required
IS-21	Process accounting is enabled, where available	Recommended	Recommended	Recommended
IS-22	System logs are reviewed on a periodic basis for security events	Recommended	Recommended	Required
IS-23	System logs are protected against tampering	Required	Required	Required

Supplemental Guidance

IS-18: Administrative commands are those commands that typically require some level of privileged access to execute. For example, adding and deleting users of a system, starting and stopping services and rebooting a system are all examples of administrative commands. Execution of these commands may occur through some type of command-line interface or they may occur through access to a graphical user interface. The full scope of administrative commands that should be logged may vary from one system to the next. As a general rule of thumb, a command that requires the use of sudo on a UNIX or Linux platform would be considered an administrative command. On a Windows platform, a command that requires a typical user to "Run as administrator" would constitute an administrative command.

Carnegie Mellon

Media Sanitization and Disposal

Media sanitization is a process by which data is irreversibly removed from media or the media is permanently destroyed. The following table defines baseline controls for sanitization and disposal of media that records and/or stores Institutional Data.

ID	Controls	Public	Private	Restricted
ME-1	Electronic Media is sanitized prior to reuse *	Recommended	Required	Required
ME-2	Electronic Media is destroyed prior to disposal *	Recommended	Required	Required
ME-3	Paper-based and/or written Media is destroyed prior to disposal *	Optional	Recommended	Required

Supplemental Guidance

ME-1: A single pass overwrite of magnetic or solid state media is recommended. While multiple overwrites can be performed, this does not provide any additional assurance that data has been irreversibly removed. It is important to note that a range of factors can impact the effectiveness and completeness of an overwrite operation. Reuse of electronic media outside of the organization is not recommended unless sanitization can be fully validated. If available, a firmware-based Secure Erase is recommended over a software-based overwrite. In situations where a third-party warranty or repair contract prohibits sanitization, a confidentiality and non-disclosure agreement should be put into place prior to making the electronic media available to the third-party.

ME-2: Media destruction should be performed in a manner that is consistent with techniques recommended by the National Institute of Standards and Technology (see Appendix A of Special Publication 800-88). Shredding and incineration are effective destruction techniques for most types of electronic media. The Information Security Office recommends destroying electronic media through Carnegie Mellon's Computer Recycling Program, which is managed by the Environmental Health and Safety department. In situations where a third-party warranty or repair contract prohibits destruction, a confidentiality and non-disclosure agreement should be put into place prior to making the Electronic Media available to the third-party.

ME-3: Common techniques for destroying Institutional Data in written or printed form include cross shredding or incineration. In situations where cross shredding or incineration are either not feasible or impractical, use of a third-party data destruction service may be appropriate. Reasonable effort should be made to track and inventory data sent to a third-party for destruction and evidence of destruction should be retained (e.g. Certificate of Destruction). In situations where documents are destroyed in large quantities or are collected and sent to a third-party for destruction, a secure trash receptacle should be leveraged to mitigate the risk of unauthorized access during the collection period.

Carnegie Mellon

Network Security

The following table defines baseline network security controls for University owned and/or operated networks that transmit Institutional Data. For the purpose of this Guideline, network devices are considered Information Systems and, as a result, appropriate Information Systems Security controls should be implemented to protect these devices.

ID	Controls	Public	Private	Restricted
NS-1	Networks that transmit Institutional Data are segmented according to access profile *	Recommended	Recommended	Required
NS-2	Access to a network that transmits Institutional Data is authenticated	Optional	Recommended	Recommended
NS-3	Controls are in place to prevent unauthorized inbound access to a network that transmits Institutional Data (e.g. firewalls, proxies, access control lists, etc.)	Recommended	Required	Required
NS-4	Controls are in place to prevent unauthorized outbound access from a network that transmits Institutional Data (e.g. firewalls, proxies, access control lists, etc.)	Recommended	Recommended	Required
NS-5	Changes to network access controls follow a documented change procedure	Recommended	Recommended	Required
NS-6	Network access controls are reviewed on a periodic basis for appropriateness	Recommended	Recommended	Required
NS-7	Controls are in place to protect the integrity of Institutional Data transmitted over a network connection *	Optional	Recommended	Required
NS-8	Network based intrusion detection and/or prevention technology is deployed and monitored	Recommended	Recommended	Required
NS-9	Network devices are configured to protect against network-based attacks *	Recommended	Required	Required
NS-10	Successful attempts to establish a network connection are logged	Required	Required	Required
NS-11	Failed attempts to establish a network connection are logged	Required	Required	Required

Supplemental Guidance

NS-1: Network segmentation is a complex topic and strategies will vary depending on the circumstances of a given scenario. It may be appropriate to segment a network based on access profiles. For example, a database server that requires no direct user access could be placed on a network with more restrictive access controls than a web

server that requires direct user access. It may also be appropriate to segment a network based on the type of data residing on that network. For example, a collection of servers that store Restricted data could be placed on a network with more restrictive controls than a collection of servers that store Public data. Available financial resources will also likely play a role in the decision making process.

NS-7: Integrity related security controls should be implemented to protect Institutional Data from unauthorized modification during transmission over a network. Message signing is one of the more common methods of ensuring the integrity of a data transmission. Message signing often goes hand-in-hand with encryption controls. For example, both the Transport Layer Security ("TLS") protocol and the IP Security ("IPSec") protocol offer messaging signing and encryption.

NS-9: Network devices should be configured to protect against denial of service, eavesdropping, impersonation and other network based attacks. ARP spoofing and MAC flooding are two examples of such attacks. Network devices can be configured in a variety of ways to protect against these attacks. For example, on a Cisco network device, DHCP snooping and dynamic ARP inspection can be configured to help prevent ARP spoofing attacks and port security can be enabled to help prevent MAC flooding.

Carnegie Mellon

Physical Security

The following table defines baseline physical security controls for protecting Institutional Data.

Physical Access Control

ID	Controls	Public	Private	Restricted
PS-1	Physical access to Institutional Data and/or Information Systems is authorized by an appropriate Data Steward or a delegate prior to provisioning *	Required	Required	Required
PS-2	Physical access to information systems that store, process or transmit Institutional Data is secured in a manner that prevents unauthorized access	Recommended	Recommended	Required
PS-3	Physical access to Institutional Data in written or paper form is secured in a manner that prevents unauthorized access *	Optional	Recommended	Required

Datacenter Security

ID	Controls	Public	Private	Restricted
PS-4	Procedures for obtaining physical access to datacenter facilities are formally documented and followed	Required	Required	Required
PS-5	Physical access to datacenter facilities is logged and monitored	Required	Required	Required
PS-6	Physical access to datacenter facilities is reviewed and reauthorized by a Data Steward or delegate on a periodic basis	Required	Required	Required
PS-7	Physical access to datacenter facilities is promptly revoked when it is no longer necessary to perform authorized job responsibilities	Required	Required	Required

Supplemental Guidance

PS-1: In addition to authorizing access to users of Institutional Data and/or Information Systems, physical access of janitorial, maintenance, police and delivery/courier personnel should also be authorized by an appropriate Data Steward or delegate.

PS-3: Institutional Data in printed or written form includes, but is not limited to, hard copies of electronic documents, hand written documents or notes and writing on a whiteboard. Physical access to workspaces, printers, fax machines and trash receptacles should all be taken into consideration. Common techniques for

securing physical access include storing data in a locked office or a locked filing cabinet, installing whiteboards in a manner that obscures visual inspection from outside an office or laboratory and shredding documents prior to disposal. In certain situations, it may also be appropriate to procure dedicated printers and fax machines for processing sensitive data.

Carnegie Mellon

Additional Information

If you have any questions or comments related to these Guidelines, please send email to the University's Information Security Office at iso@andrew.cmu.edu.

Additional information can also be found using the following resources:

- Guidelines for Appropriate Use of Administrator Access
  http://www.cmu.edu/iso/governance/guidelines/appropriate-use-admin-access.html

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

- Guidelines for Password Management
  http://www.cmu.edu/iso/governance/guidelines/password-management.html

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

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