Carnegie Mellon

Guidelines for Data Protection

Document Information	
Status	Published
Published	01/31/2020
Last Reviewed	01/31/2020
Last Updated	01/31/2020
Version	2.0

Revision History

Version	Published	Author	Description
2.0	01/31/2020	Laura Raderman	Major changes from v1.0, reorganization, added controls to closer match regulations.

Table of Contents

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

These Guidelines are intended for all Data Stewards, Data Custodians, and Users to guide how to protect Institutional Data. Data must first be classified based on the Guidelines for Data Classification (https://www.cmu.edu/iso/governance/guidelines/data-classification.html). The classification will dictate what controls are necessary to protect that data. Public data is data that is intended for public release; however, the University is concerned about the integrity of the data (i.e. We would not like our main www.cmu.edu website defaced). All controls listed under "Public" in this document are for non-read only access to public data, and are intended to protect the integrity of that data.

Definitions

Applications – Programs that run on an Information System that provide functionality for users. Applications can be local or software as a service.

Console – Local access to a system, including through a KVM switch. If your system lost its network connection, where would you go to log into it. This is **usually**, but not always at the local keyboard and monitor for the system

Electronic Media - 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

Identifiers – How a system, user, or service is uniquely identified. For users, this is usually their username, for a system or service, it may be a hostname, a combination of host and port

Information System - 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 - any data that is owned or licensed by the University

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

Log content – The events and actions being logged. ISO publishes recommended log content at https://www.cmu.edu/iso/service/logging/index.html

Logs – Audit information regarding the activities occurring on the information system. Logs are used to monitor for unusual activity on the information system, and for forensic purposes if necessary.

Multi-factor Authentication - 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 Users – Users who can alter the configuration of the system, specifically, the security configuration. 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

Segregation of Duties – Fundamentally, the individual that implements a change is not the individual that approves the change. This allows for prevention and detection of fraud by one individual.

Services – Services are applications or groups of applications that provide a service to users or other systems, and are generally well-known services, such as DNS, SSH, etc.

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.

For the purpose of this Guideline, the Information Security Office has defined thirteen control areas. They are as follows:

Identifier	Control Area
AC	Access Controls
AL	Audit and Logging
DR	Business Continuity and Disaster Recovery
EN	Encryption and Key Management
ID	Identification and Authentication
IR	Incident Response
ME	Media Protection
NS	Network Security
PE	Personnel Security
PS	Physical Security
CM	Secure Configuration Management
AS	Security Assessment
TA	Training and Awareness

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 of data. 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.
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. If you would like assistance with this evaluation, contact the Information Security Office by email at iso@andrew.cmu.edu.

Access Controls

Access Controls are controls that are put in place to ensure that only approved individuals have access to data and information systems.

Control Number	Control Name	Public	Private	Restricted
AC-1	Access to Institutional Data and/or Information Systems is uniquely associated with an individual or system	Required	Required	Required
AC-2	Access to Institutional Data and/or Information Systems is authenticated	Required	Required	Required
AC-3	Access to Institutional Data and/or Information Systems is authorized by a Data Steward or a delegate prior to provisioning	Required	Required	Required
AC-4	Access to Institutional Data and/or Information Systems is authorized based on a business need	Required	Required	Required
AC-5	Access to Institutional Data and/or Information Systems is based on the principle of least privilege	Required	Required	Required
AC-6	Access to Institutional Data is reviewed and reauthorized by a Data Steward or a delegate on a periodic basis	Required	Required	Required
AC-7	Access is promptly revoked when it is no longer necessary to perform authorized job responsibilities	Required	Required	Required
AC-8	Active sessions require re-authentication after a period of inactivity	Recommended	Required	Required
AC-9	Segregate duties where possible	Recommended	Required	Required
AC-10	Do not use privileged accounts for non-privileged access	Recommended	Recommended	Required
AC-11	Prevent non-privileged users from accessing privileged functions	Recommended	Recommended	Required
AC-12	Individuals without normal access authorization must be supervised or escorted	Required	Required	Required
AC-13	Screen locking that hides the working screen after a period of inactivity (e.g. screensavers) is required	Recommended	Required	Required

Control Number	Control Name	Public	Private	Restricted
AC-14	Route remote access through defined access points	Recommended	Required	Required

Audit and Logging

Audit and Logging controls ensure that there is enough information to monitor systems and to conduct digital forensics should unauthorized access occur.

Control Number	Control Name	Public	Private	Restricted
AL-1	Log content is sufficient for monitoring, and later forensics to determine who accessed, modified, or removed content and when	Recommended	Required	Required
AL-2	Logging standard is reviewed at least annually	Recommended	Required	Required
AL-3	Alert if the audit process fails or is disabled	Recommended	Required	Required
AL-4	Logs are reviewed on a periodic basis for security events	Recommended	Recommended	Required
AL-5	Logs and logging tools are protected against unauthorized access, modification, and deletion	Recommended	Required	Required
AL-6	Logs are sent to a centralized system for analysis and review	Recommended	Recommended	Required
AL-7	Systems are synchronized to an authoritative time source	Required	Required	Required
AL-8	Monitor system security alerts and take appropriate action	Recommended	Required	Required

Business Continuity and Disaster Recovery

Availability is an important part of security. Business Continuity and Disaster Recovery ensures that data and business processes are available as needed.

Control Number	Control Name	Public	Private	Restricted
DR-1	A disaster recovery strategy is implemented and tested periodically	Recommended	Required	Required
DR-2	A business continuity strategy is implemented and tested periodically	Recommended	Required	Required
DR-3	Backup copies are protected at least as well as primary data	Required	Required	Required

Encryption and Key Management

When Information systems use encryption, the keys used for that encryption must be managed securely.

Control Number	**Control Name**	Public	Private	Restricted
EN-1	Institutional Data transmitted over any network connection is encrypted	Recommended	Required	Required
EN-2	Institutional Data stored on Electronic Media is encrypted	Recommended	Recommended	Required
EN-3	Institutional Data stored on removable Electronic Media is encrypted	Recommended	Required	Required
EN-4	Data stored on a mobile computing device is encrypted	Recommended	Required	Required
EN-5	Remote administration of an Information System is performed over an encrypted network connection	Required	Required	Required
EN-6	Approved algorithms and key-lengths are used where encryption and/or digital signing are employed	Required	Required	Required
EN-7	Keys are changed periodically where encryption is employed	Required	Required	Required
EN-8	Keys are revoked and/or deleted when they are no longer needed to perform a business function	Required	Required	Required
EN-9	Keys are revoked or changed when compromised or individuals with access to the keys are no longer employed or transferred to another job role.	Required	Required	Required

Identification and Authentication

Identification and Authentication are the processes by which users, systems, and processes are identified and that identity is verified.

Control Number	Control Name	Public	Private	Restricted
ID-1	Administrative access to Institutional Data and/or Information Systems is authenticated using multi- factor authentication	Recommended	Required	Required
ID-2	Access to Institutional Data and/or Information Systems that traverses an unsecured network is authenticated using multi-factor authentication	Required	Required	Required
ID-3	Where username and password authentication is employed, passwords are managed according to the Guidelines for Password Management	Required	Required	Required
ID-4	Identifiers are never reused	Required	Required	Required
ID-5	Inactive identifiers are disabled after a defined period of time	Required	Required	Required
ID-6	Employ replay-resistant authentication mechanisms	Required	Required	Required
ID-7	Obscure feedback of authentication information	Required	Required	Required
ID-8	Authenticators (such as passwords) should always be cryptographically protected when electronically stored or transmitted	Required	Required	Required

Incident Response

Should unauthorized access occur, incident response is the business process that responds to that occurrence, and involves preparation, detection, containment, investigation, remediation, and recovery.

Control Number	Control Name	Public	Private	Restricted
IR-1	An incident response function supports the environment	Required	Required	Required
IR-2	The incident handling response is tested at least annually	Required	Required	Required
IR-3	The incident handling response reports to internal and external organizations as appropriate	Required	Required	Required

Media Protection

Media, both electronic and paper format, contains Institutional Data, and must be protected from unauthorized access.

Control Number	Control Name	Public	Private	Restricted
ME-1	Electronic Media is sanitized prior to reuse	Recommended	Required	Required
ME-2	Electronic and paper-based Media is destroyed prior to disposal	Optional	Required	Required
ME-3	Unencrypted media is protected from unauthorized access and accountability is maintained during transport	Optional	Required	Required
ME-4	Mark removable media with the data classification where it may be accessed outside of an authorized group of individuals	Optional	Recommended	Required

Network Security

Networks are used to protect Institutional Data and Information Systems from unauthorized access.

Control Number	Control Name	Public	Private	Restricted
NS-1	Networks that transmit Institutional Data are segmented according to access profile (i.e., public systems vs internal only systems)	Recommended	Required	Required
NS-2	Access to a network that transmits Institutional Data is authenticated	Recommended	Required	Required
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	Required	Required
NS-5	Changes to network access controls follow a documented change procedure	Required	Required	Required
NS-6	Network access controls are reviewed on a periodic basis for appropriateness	Required	Required	Required
NS-7	Controls are in place to protect the integrity of Institutional Data transmitted over a network connection	Required	Required	Required
NS-8	Network based intrusion detection and/or prevention technology is deployed and monitored at appropriate network boundaries	Recommended	Required	Required
NS-9	Network devices are configured to protect against network-based attacks	Required	Required	Required
NS-10	Connecting a remote endpoint to two networks at the same time is prohibited for administrative access (i.e., no split tunneling)	Recommended	Required	Required
NS-11	Network access controls (e.g. firewalls) must deny by default and permit by exception	Recommended	Required	Required

Personnel Security

Users and Administrators of Information Systems should possess the skills and background necessary for their access.

Control Number	Control Name	Public	Private	Restricted
PE-1	All individuals are screened prior to accessing institutional systems	Recommended	Recommended	Required

Physical Security

Institutional Data must be protected physically as well as logically.

Control Number	Control Name	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	Recommended	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	Required	Required
PS-3	Physical access to Institutional Data in written or paper form is secured in a manner that prevents unauthorized access	Recommended	Required	Required
PS-4	Procedures for obtaining physical access to datacenter facilities are formally documented and followed	Recommended	Required	Required
PS-5	Physical access to datacenter facilities is logged and monitored	Required	Required	Required
PS-6	Alternate worksites have a similar physical security profile to the primary site	Required	Required	Required
PS-7	All mobile devices are protected as one would protect their money, ID or credit cards	Recommended	Required	Required
PS-8	Support Infrastructure for datacenter facilities are protected from unauthorized access	Recommended	Required	Required

Secure Configuration Management

Secure Configuration Management is concerned with ensuring that an Information System is configured securely initially, that it remains in that known configuration, and any changes to that configuration does not reduce the protections of that Information System.

Control Number	Control Name	Public	Private	Restricted
CM-1	Controls are deployed to protect against unauthorized connections to services (e.g. firewalls, proxies, access control lists, etc.)	Required	Required	Required
CM-2	Controls are deployed to protect against malicious code execution (e.g. antivirus, antispyware, etc.)	Required	Required	Required
CM-3	Controls deployed to protect against malicious code scan files or objects on-read or on-access	Required	Required	Required
CM-4	Controls deployed to protect against malicious code scan the entire system periodically	Required	Required	Required
CM-5	Controls deployed to protect against malicious code execution are kept up to date (e.g. software version, signatures, etc.)	Required	Required	Required
CM-6	Local accounts that are not being utilized are disabled or removed	Required	Required	Required
CM-7	Limit Unsuccessful login attempts	Recommended	Required	Required
CM-8	Default or vendor supplied credentials (e.g. username and password or encryption keys) are changed prior to implementation	Required	Required	Required
CM-9	Services that are not being utilized are disabled or removed	Required	Required	Required
CM-10	Applications that are not being utilized are removed	Required	Required	Required
CM-11	Auto-run for removable electronic storage media (e.g. CDs, DVDs, USB drives, etc.) and network drives is disabled	Required	Required	Required
CM-12	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.)	Required	Required	Required
CM-13	Operating system and software security patches are deployed in a timely manner	Required	Required	Required

Control Number	Control Name	Public	Private	Restricted
CM-14	Mitigating controls are deployed for known security vulnerabilities in situations where a vendor security patch is not available	Required	Required	Required
CM-15	Changes to critical system files (e.g. configuration files, executables, etc.) are logged	Recommended	Required	Required
CM-16	Provide warnings/banners/notices upon login to notify users of the classification of the data contained in that system where the user has access to more than their own personal data	Recommended	Required	Required
CM-17	Baseline configurations for each system, device, application, and use are documented and used	Recommended	Required	Required
CM-18	Prevent the unauthorized use of external and removeable media devices	Recommended	Required	Required
CM-19	All Information Systems must document how they meet these requirements, and where they do not, a business justification or a plan of remediation with estimated timelines must be documented	Recommended	Required	Required
CM-20	Track, review, and approve/disapprove of all changes to system configurations	Recommended	Required	Required
CM-21	Review all configuration changes for security impacts	Recommended	Required	Required

Security Assessment

Security Assessment ensures that Data Stewards and Data Custodians are aware of changing threats to Institutional Data, and that the controls implemented for a particular Information System are in place and appropriate for that System or Data.

Control Number	Control Name	Public	Private	Restricted
AS-1	Procedures for monitoring for new security vulnerabilities are documented and followed	Required	Required	Required
AS-2	System is periodically tested for security vulnerabilities (e.g. vulnerability scanning, penetration testing, etc.)	Required	Required	Required
AS-3	Periodically audit systems for adherence to controls	Recommended	Recommended	Required
AS-4	Monitor threats, and risks to ensure that controls remain appropriate	Required	Required	Required
AS-5	Monitor system controls for effectiveness	Recommended	Required	Required

Training and Awareness

Training and awareness includes controls that ensure that users are trained properly and are aware of their responsibilities as it pertains to information security and these guidelines.

Control Number	Control Name	Public	Private	Restricted
TA-1	All users, including privileged users have completed security awareness training prior to accessing Institutional Data and at least annually	Required	Required	Required
TA-2	All privileged users have completed additional security training in relation to their job duties	Recommended	Required	Required
TA-3	Training includes how to spot and report potential insider threats	Recommended	Required	Required
TA-4	Training must include safety of portable devices	Recommended	Required	Required

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 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
  https://www.cmu.edu/policies/information-technology/information-security-policy.html

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