Cybersecurity Control Standards & Implementation Guide

The Texas A&M University System

Revised September 4, 2021

Table of Contents

Revision History

Version	Updated By	Date	Change Description
1.0	N. McLarty	2020-08-18	Initial release
1.0.1	N. McLarty	2021-05-31	Change reference of controlled to internal use
1.1	N. McLarty	2021-06-18	Added IA-11
1.2	N. McLarty	2021-09-04	Moved DM-1 to RA-2, TR-1 to AC-8

About Texas A&M System Cybersecurity Control Standards

Texas A&M University System members publish a security control catalog to implement organizational information security controls in a format that aligns with the Texas Security Control Standards Catalog, prescribed by Title 1 Texas Administrative Code §202.76, *Security Control Standards Catalog* [1 TAC 202.76].

Texas A&M System Cybersecurity Control Standards provide system members with additional guidance that enhances State-level requirements for implementing security controls. These standards are prescribed by Texas A&M System Regulation 29.01.03, *Information Security* [TAMUS 29.01.03], paragraph 1.2(c).

This document is intended to be used as a supplement to *Texas Security Control Standards Catalog Version 1.3*, updated February 26, 2016 [TxDIR Catalog].

Cybersecurity Control Standards Lifecycle

The Texas A&M University System Office of Cybersecurity will review control standards each even-numbered year, following the Texas Department of Information Resources' publishing of new statewide security control standards.

Prior to publishing new or revised standards, the Office of Cybersecurity will solicit comments on new control standards from Chief Information Officers and (Chief) Information Security Officers at system members.

Cybersecurity Control Standards Sample Format

ID #	Control Title
IMPLEMENTATION	
	TEXAS A&M UNIVERSITY SYSTEM
	[System-level requirements for the implementation of information security controls]

Cybersecurity Control Standards

AC – Access Control

AC-1 Access Control Policy and Procedures

IMPLEMENTATION

TEXAS A&M UNIVERSITY SYSTEM

The System member ensures adequate processes are in place to positively establish the identity of (identity-proof) a user and determine the appropriate user role(s) before access is granted.

AC-2 Account Management

IMPLEMENTATION

TEXAS A&M UNIVERSITY SYSTEM

The System member implements role-based (e.g., students, employees, third parties, guests) access control or adopts an InCommon Federation assurance profile [InCommon], where possible.

AC-6 Least Privilege

IMPLEMENTATION

TEXAS A&M UNIVERSITY SYSTEM

The System member ensures users with privileged (also known as administrative or special access) accounts are aware of the extraordinary responsibilities associated with the use of privileged accounts.

AC-8 System Use Notification

IMPLEMENTATION

TEXAS A&M UNIVERSITY SYSTEM

The System member publishes a privacy notice on websites owned by the member which contains, at a minimum, the content contained on the Texas A&M University System website at https://www.tamus.edu/marcomm/reports/privacy.

AC-22 Publicly Accessible Content

IMPLEMENTATION

TEXAS A&M UNIVERSITY SYSTEM

The System member ensures organizational security controls are applied to official social media use by the member.

AT – Awareness and Training

No control standards exist for this control family.

AU – Audit and Accountability

No control standards exist for this control family.

CA – Security Assessment and Authorization

No control standards exist for this control family.

CM – Configuration Management

CM-2	**Baseline Configuration**
IMPLEMENTATION	
	TEXAS A&M UNIVERSITY SYSTEM
	The System member ensures all servers on System-owned or -managed networks conform to a baseline security configuration and are security-hardened based on risk.

CM-3 Configuration Change Control

IMPLEMENTATION

TEXAS A&M UNIVERSITY SYSTEM

The System member incorporates change management processes to ensure secure, reliable, and stable operations to which all offices that support information systems adhere. The change management process incorporates guidelines that address:

1. formally identifying, classifying, prioritizing, and requesting changes;

2. identifying and deploying emergency changes;

3. assessing potential impacts from changes;

4. authorizing changes and exceptions;

5. testing changes;

6. implementing changes and planning for back-outs, and

7. documenting and tracking changes.

CM-6 Configuration Settings

IMPLEMENTATION

TEXAS A&M UNIVERSITY SYSTEM

The System member adopts baseline security configuration checklists that meet or exceed published industry best practice sources (e.g., Center for Internet Security Benchmarks [CIS Benchmarks], NIST National Checklist Program [NCP]) when available, or locally develops security configuration checklists otherwise, for all System-owned or -managed major and mission-critical information systems, and systems processing confidential information.

CM-10 Software Usage Restrictions

IMPLEMENTATION

TEXAS A&M UNIVERSITY SYSTEM

The System member ensures software installed on System-owned or -managed information systems is used in accordance with the applicable software license(s) and understands unauthorized or unlicensed use of software is regarded as a serious matter subject to disciplinary action.

CP – Contingency Planning

CP-1 Contingency Planning Policy and Procedures

IMPLEMENTATION

TEXAS A&M UNIVERSITY SYSTEM

The System member develops information resources contingency planning policy and procedures that align with the member's emergency management plan as required by Texas A&M System Regulation 34.07.01, *Emergency Management* [TAMUS 34.07.01].

CP-4 Contingency Plan Testing

IMPLEMENTATION

TEXAS A&M UNIVERSITY SYSTEM

The System member:

1. tests the contingency plan at least annually through a tabletop exercise;

2. tests the contingency plan at least every three years with a full interruption of mission-critical, on-premise services, and

3. includes information resources contingency plan testing in the member's emergency management plan testing and exercises.

CP-9 Information System Backup

IMPLEMENTATION

TEXAS A&M UNIVERSITY SYSTEM

The System member stores backup copies of information systems that process and/or store sensitive or mission-critical information offline or in a separate facility that is not collocated with the operational system.

IA – Identification and Authentication

No control standards exist for this control family.

IR – Incident Response

IR-6	Incident Reporting

IMPLEMENTATION

TEXAS A&M UNIVERSITY SYSTEM

The System member discloses incidents which compromise the confidentiality, integrity, or availability of major or mission-critical information systems, or systems processing confidential information, as quickly as possible upon the discovery or receipt of notification of the incident, using the notification matrix in Appendix C: Incident Notification Matrix, unless a law enforcement agency determines such a notification will impede a criminal investigation.

MA – Maintenance

No control standards exist for this control family.

MP – Media Protection

MP-3	Media Marking

IMPLEMENTATION

TEXAS A&M UNIVERSITY SYSTEM

The System member marks, physically or electronically, removable electronic media and information resources output containing sensitive personal information [TxBCC 521.002] by indicating the ownership, distribution limitations, handling caveats, and applicable data classifications.

PE – Physical and Environmental Protection

PE-6	Monitoring Physical Access

IMPLEMENTATION

TEXAS A&M UNIVERSITY SYSTEM

The System member ensures audio-visual surveillance technology used to monitor physical access to information systems is used responsibly and within the intended scope of the purpose for such deployment, and transparent processes and controls are implemented for the use of such technology and any resulting recorded material.

PL – Planning

PL-4	Rules of Behavior

IMPLEMENTATION

TEXAS A&M UNIVERSITY SYSTEM

The System member:

1. documents acceptable use guidelines;

2. ensures users formally acknowledge, agree to abide by, and adhere to prudent and responsible Internet use practices (including reasonable personal use) outlined in Texas A&M System Policy 33.04, *Use of System Resources* [TAMUS 33.04], and the member's acceptable use guidelines;

3. establishes a documented process for authorization to monitor member information resources, and

4. monitors information resources in accordance with Texas A&M System Policy 29.01, *Information Resources* [TAMUS 29.01].

PM – Program Management

PM-5	Information System Inventory

IMPLEMENTATION

TEXAS A&M UNIVERSITY SYSTEM

The System member:

1. designates a single system of record for inventory of all information systems [SP 800-171r2] and network-attached operational technology [SP 800-37r2] owned or managed by the member;

2. includes any cloud computing services [SP 800-145] operated by the member in its inventory of information systems, and

3. designates which data regarding an information system to record in the inventory of information systems. At a minimum, the data includes a unique identifier (e.g., serial number or system name), owner, custodian, description of the information system's function or major application, and highest level of data classification stored/processed on the information system.

PM-14	Testing, Training, and Monitoring

IMPLEMENTATION

TEXAS A&M UNIVERSITY SYSTEM

The System member ensures an IT organization is designated to provide security monitoring for all information systems, in both centralized and decentralized IT environments, owned or managed by the member.

PS – Personnel Security

No control standards exist for this control family.

RA – Risk Assessment

RA-2	Security Categorization

IMPLEMENTATION

TEXAS A&M UNIVERSITY SYSTEM

The System member:

1. categorizes information and information systems owned or managed by the member using a data classification structure that incorporates the guidance provided in Appendix D: Data Classification, at a minimum.

2. reduces, and eliminates where possible, the collection and/or use of sensitive personal information [TxBCC 521.002] in information resources under the control of the member.

SA – System and Services Acquisition

SA-3	System Development Life Cycle

IMPLEMENTATION

TEXAS A&M UNIVERSITY SYSTEM

The System member Information Security Officer (ISO) reviews the data security requirements and specifications of any new information systems or services that process and/or store sensitive or mission-critical information.

SA-4	Acquisition Process

IMPLEMENTATION

TEXAS A&M UNIVERSITY SYSTEM

The System member Information Security Officer (ISO):

1. reviews and approves the security requirements in acquisition contracts of any new information system that processes and/or stores sensitive or mission-critical information prior to the member procuring the system or service, and

2. ensures acquisition contracts for information systems, system components, or information system services address information security, backup, and privacy requirements.

a. Such contracts should include right-to-audit and other provisions to provide appropriate assurance that applications and information are adequately protected.

b. Vendors and third parties adhere to all state and Federal laws and System policies pertaining to the protection of information resources and privacy of sensitive information.

SC – System and Communications Protection

SC-13	Cryptographic Protection

IMPLEMENTATION

TEXAS A&M UNIVERSITY SYSTEM

The System member ensures that information systems owned or operated by the member implement FIPS-validated cryptography [FIPS 140-2].

SI – System and Information Integrity

SI-3	Malicious Code Protection

IMPLEMENTATION

TEXAS A&M UNIVERSITY SYSTEM

The System member:

1. ensures all System-owned or -managed information systems that connect to a member network employ endpoint protection software and any other protective measures required by applicable policies or guidelines, and

2. ensures personally owned devices that connect to networks within the same boundary as confidential or mission-critical information systems employ endpoint protection software or suitable compensating controls, based on assessed risk.

SI-4	Information System Monitoring

IMPLEMENTATION

TEXAS A&M UNIVERSITY SYSTEM

The System member ensures the security of information systems through monitoring network traffic and use of information resources.

References

General References

[1 TAC 202.76] Title 1 Texas Administrative Code §202.76, *Security Control Standards Catalog*, Link to https://texreg.sos.state.tx.us.

[CIS Benchmarks] "CIS Benchmarks™," *Center for Internet Security*, https://www.cisecurity.org/cis-benchmarks.

[InCommon] "InCommon Assurance Program," *InCommon*, https://www.incommon.org/federation/incommon-assurance-program.

[NCP] *NCP - National Checklist Program Repository*, https://nvd.nist.gov/ncp/repository.

[TxBCC 521.002] Texas Business and Commerce Code §521.002, *Unauthorized Use of Identifying Information: Definitions*, https://statutes.capitol.texas.gov/Docs/BC/htm/BC.521.htm.

[TxDIR Catalog] Texas Security Control Standards Catalog, Version 1.3, February 2016, http://publishingext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Security%20Control%20Standards%20Catalog.pdf.

[TAMUS 29.01] Texas A&M System Policy 29.01, *Information Resources*, April 2018, https://policies.tamus.edu/29-01.pdf.

[TAMUS 29.01.03] Texas A&M System Regulation 29.01.03, *Information Security*, February 2018, https://policies.tamus.edu/29-01-03.pdf.

[TAMUS 33.04] Texas A&M System Policy 33.04, *Use of System Resources*, September 2016, https://policies.tamus.edu/33-04.pdf.

[TAMUS 34.07.01] Texas A&M System Regulation 34.07.01, *Emergency Management Plans*, August 2018, https://policies.tamus.edu/34-07.pdf.

NIST Special Publications

[SP 800-37r2] NIST Special Publication 800-37 Rev 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, December 2018, https://doi.org/10.6028/NIST.SP.800-37r2.

[SP 800-39] NIST Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011, https://doi.org/10.6028/NIST.SP.800-39.

[SP 800-145] NIST Special Publication 800-145, *The NIST Definition of Cloud Computing*, September 2011, https://doi.org/10.6028/NIST.SP.800-145.

[SP 800-171r2] NIST Special Publication 800-171 Rev 2, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, February 2020, https://doi.org/10.6028/NIST.SP.800-171r2.

Federal Information Processing Standards

[FIPS 140-2] Federal Information Processing Standard Publication 140-2, *Security Requirements for Cryptographic Modules*, December 2002, https://doi.org/10.6028/NIST.FIPS.140-2.

[FIPS 199] Federal Information Processing Standard Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004, https://doi.org/10.6028/NIST.FIPS.199.

Appendix A: Legacy Security Standard Crosswalk

Configuration Management Standard

- CM-3 Configuration Change Control
- CM-8 Information System Component Inventory
- PM-5 Information System Inventory

Contingency Planning Standard

- CP-1 Contingency Planning Policy and Procedures
- CP-2 Contingency Plan
- CP-4 Contingency Plan Testing

Data Classification Standard

- RA-2 Security Categorization
- Appendix D Data Classification

Electronic Media Protection Standard

- MP-3 Media Marking

Electronic Signature Standard

- [Removed from Cybersecurity Control Standards]

Identity Management Standard

- AC-1 Access Control Policy and Procedures
- AC-2 Account Management

Incident Management Standard

- IR-6 Incident Reporting

Information Integrity Standard

- CM-2 Baseline Configuration

CM-10 Software Usage Restrictions

PL-4 Rules of Behavior

SI-3 Malicious Code Protection

Information Resources Access Standard

AC-2 Account Management

PL-4 Rules of Behavior

Information System Monitoring Standard

PM-14 Testing, Training, and Monitoring

SI-4 Information System Monitoring

Notification Matrix

Appendix C Incident Notification Matrix

Online Privacy Standard

TR-1 Privacy Policy

Physical and Environmental Protection Standard

DM-1 Minimization of Personally Identifiable Information

PE-6 Monitoring Physical Access

PL-4 Rules of Behavior

Preservation Holds Standard

[Removed from Cybersecurity Control Standards]

System Development and Acquisition Standard

SA-3 System Development Life Cycle

SA-4 Acquisition Process

Appendix B: Identity Role Examples and Definitions

a) Active Students – students who are enrolled and attending in learning activities at system institutions.

b) Alumni – non-personnel who are either former students, graduates or former employees (in good standing) who may be granted some limited access to information resources.

c) Faculty – personnel who act as instructors or assistants to instructors at system institutions.

d) Financial Staff – personnel whose work role is to perform financial activities, such as accounting, bursar, budgeting, procurement, invoicing and disbursement activities.

e) Guest – non-personnel who may or may not be affiliated with system institutions who have temporary and limited access to system information resources.

f) HIPAA-access – this role is a sub-role that is usually combined with other roles which further define related attributes and is not a healthcare professional but has access to HIPAA-related information.

g) Healthcare professional – personnel who have access to HIPAA-related information in accordance with health-related work or research activities.

h) Human Resources – personnel whose work activities include the ability to view or update personnel records, coordinate performance reviews, perform compensation management and view or manage HIPAA-related or insurance-related information related to personnel.

i) Inactive Students – students who are not enrolled and are not attending in learning activities at a system institution.

j) IT Security – personnel who perform cybersecurity activities for system institutions.

k) IT Staff – information technology professionals and help desk or technical support staff who operate or support IT infrastructure or applications. This also includes programming and database activities.

l) Law Enforcement – personnel who are a part of the system's university police departments.

m) Partner (Research) – non-personnel who are affiliated with system institutions or activities but are not employees. They may be granted specific but limited access to system-related information resources and must be closely monitored.

n) Physical Security – personnel whose work activities include the physical protection and monitoring of system facilities.

o) Research Professional – personnel who work in officially sanctioned and recognized system research activities.

p) Staff/Administrative/Service – personnel who participate in general administrative duties at system institutions.

q) Student Workers – students who are enrolled and attending learning activities and are also performing officially recognized and sanctioned work activities on behalf of a system institution.

r) Vendor/Service Provider – non-personnel who perform some service to system institutions that require access to specific and limited information resources for specified activities. Their activities must be closely monitored.

s) Visiting Professor – a person who is employed as a professor or instructor at another university institution that has been officially invited by the system to act as a professor and participate in teaching activities for some defined time. The visiting professor may be granted specific but limited access to system-related information resources and must be closely monitored.

t) Visiting Research Professional – personnel who are not system employees, faculty or researchers, but who have an official system research sponsor who is either doing direct or assistive work with system research.

Appendix C: Incident Notification Matrix

The Texas A&M University System
Notification Matrix

Type of Information	Regulated			Confidential			Controlled			Notes
The Texas A&M University System maintains a data classification standard that is reflected here to assist readers of their responsibilities in notifying the correct personnel in the case of a breach of information as defined by the type of information breached.	Focuses on information that is regulated by federal statute or third-party agreements such as research. Examples include classified research, HIPAA data, FERPA data, and covenant-controlled or third-party research.			Information that must be protected from unauthorized disclosure or public release based on state or federal law. Examples include credit card numbers, personally identifiable information (PII), Social Security Numbers, computer vulnerability reports that include network and security information. This may also include some controlled unclassified information as defined by Executive Order 13556.			Information that is not generally created for or made available for public consumption, but that may not be subject to public disclosure. Examples include controlled but unclassified research, operational records, budgets, employee salaries and expenditures.			Notes that modify or clarify notification and communication with parties involved or affected. Affected member leadership is responsible for communicating initially to system-level SCIO and SCISO personnel who will then notify other responsible parties on the notification matrix.
Notified parties/Time line	24 hrs	48 hrs	72 hrs	24 hrs	48 hrs	72 hrs	24 hrs	48 hrs	72 hrs	
Chancellors' Office	X					X			X	Notification of the Chancellor's representative
SCIO	X				X			X		
SCISO	X			X				X		
Security Operations Center (Part 26)	X			X				X	X	Notify if applicable to research and DoD/research partners
Facility Security Officer	X			X						
Agency/University President/Provost	X			X				X		
Agency/University CIO	X			X				X		
Agency/University ISO/CISO	X			X				X		
Agency/University Department head	X			X				X	X	
Office of General Counsel	X				X	X				
Vendors, Partners Affected		X				X				
Affected people (students, employees)			X			X				
SO Marcom	X				X				X	
Internal Audit	X				X				X	
Compliance	X				X				X	
Department of Information Resources		X				X			X	SCISO to be copied on all communications to DIR for incidents
Law Enforcement		X			X					Only as needed. OGC would determine need to inform and involve
Office of Civil Rights	X									HIPAA-only data breach of 500 records or more. SCISO to determine.

Information Gathering and Evidence for Incident Response:

		Potential Impact Related to Information Breach		
When notifying, have the following info:		Low	Moderate	High
Who	Who was impacted?	The unauthorized disclosure of information would be expected to have no or only a slight adverse affect on the organization's operations, assets or on individuals. This could include network probes or system scans, isolated virus infections and acceptable use violations.	The unauthorized disclosure of information would be expected to have a limited adverse effect on organizational operations, assets and individuals. This would affect a small number of (less than 500) individuals. This would also include small-scale Denial-of-Service (DoS) attacks, website compromises and unauthorized access against FTP, ssh and other protocols.	The unauthorized disclosure of information would be expected to have severe or catastrophic adverse effect on organizational operations, assets or individuals. This would be classed as information that would impact multiple organizations, including external partners, vendors and affiliates. This could also include large-spread compromises of sensitive data and malware code attacks.
What	What was breached, exposed, stolen or destroyed?			
When	When did it happen? What's the timeline? Can you determine when it was breached?			
Where/Source	Where did it happen? Are there other parties affected, such as a vendors?			
Why	Is there a reason why or is it known why the incident occurred?			
How	How did it happen? Is it known or should internal and external investigations be initiated?			
Status	What's the status of the incident? Have we halted the incident or at least prevented additional information from being exposed, stolen or destroyed?			
Containment/Remediation	What's the plan for remediation? How quickly can we move on containment and remediation and eliminating the threat if it is ongoing?			
Recovery	Once the root cause has been identified and completed after remediation, how quickly can we recover to normal operation? What's the timeline to recover?			
Lessons Learned	Have we preserved evidence for analysis to perform a lessons learned? Do we need to involve outside parties, such as forensics investigators, to perform an analysis to complete the lessons learned? Do we need to adjust our security posture and policies to prevent this incident from reoccurrence?			

Appendix D: Data Classification

Texas A&M University System (A&M System) data classification consists of a minimum of three specific classifications based on access restrictions and risk. These classifications apply to all members. While the classification applicable to specific information may change based on circumstances, the intent of this document is to define the appropriate classification for different types of information. These three classifications are:

Classification	Description	Examples	Comments
Confidential Information	Information that must be protected from unauthorized disclosure or public release based on state or federal law or other legal agreement (1 TAC §202.1)	• Patient billing information and protected health information as protected by HIPAA. • Student education records protected by FERPA. • Information or Information System security plans, reports and related information • Credit/debit card numbers, bank account numbers • Personal financial information • Social security numbers • A&M System intellectual property and research information having commercial potential Confidential Information requiring breach notifications or having stricter access requirements may include SPI as defined by Texas Business and Commerce Code § 521.002(a)(2);	This classification may not be absolute; context is an essential element. Owners of confidential information must ensure such information is correctly classified. Custodians of confidential information must implement appropriate controls. HIPAA, FTI or PCI information is covered in this category. This classification may include agreements or contracts for research work that require higher levels of security and/or procedural elements for handling of information. Consult the Office of General Counsel regarding confidential information requested through open records, subpoena, or other legal process.

Classification	Description	Examples	Comments
		credit card numbers covered by PCI DSS v3.1. Classified National Security Information under Executive Order 13526, and Controlled Unclassified Information under Executive Order 13556, shall be protected as prescribed by System Regulations 15.05.01 and 15.05.02, respectively, and the System Facility Security Officer (FSO).	
Internal Use	Information that is not generally created for or made available for public consumption but that may or may not be subject to public disclosure through the Texas Public Information Act or similar laws.	This information includes institutional budgetary, financial and operational records such as expenditures, statistics, contracting information, non-confidential personnel information. It may also include non-confidential internal communications.	Consult the Office of General Counsel regarding controlled information requested through open records, subpoena, or other legal process.
Public Information	Public information includes all information made available to the public through posting to public websites, distribution through email, or social media, print publications or other media. This classification also includes information for which public disclosure is intended or required.	Published system and system member policy documents, organizational charts, Statistical reports, Fast Facts, unrestricted directory information, employee salaries, and educational content available to the public at no cost.	Information can migrate from one classification to another based on information lifecycle. For example, a draft policy document would fit the criteria of "Internal Use" until being published upon which it would become "Public Information".

1. Each member will use this classification criteria as their baseline standard. If a member requires a more restrictive classification for a class of data due to state, federal or other agreements, the more restrictive classification will apply.

2. This classification criteria will be used to assess information access and security requirements for information to be stored or processed within member shared information centers.

3. When determining security controls to use for a given set of information, Information Owners and Custodians should also assess whether special requirements exist regarding importance of information availability and integrity and rate the need as LOW, MODERATE, or HIGH for both integrity and availability. The needs regarding availability and integrity may impact security control decisions but are not used for purposes of assigning a classification label of Confidential, Internal Use, or Public.

4. Some classes of information may have attributes, such as “mission critical” or “business critical”. Information attributes do not supplant these classifications but should be used to clarify their importance to the institution.

State of Texas Requirement

“State institutions of higher education are responsible for defining all information classification categories except the Confidential Information category, which is defined in Subchapter A of this chapter, and establishing the controls for each” *(1 Tex. Admin. Code § 202.74(b)(1))*.

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restriction on information access and disclosure including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Using the table above, any set of information can be assigned three security ratings: one for Confidentiality (LOW, MODERATE or HIGH), another for Integrity (LOW, MODERATE or HIGH), and a third for Availability (LOW, MODERATE or HIGH). This is useful for defining security controls in cases where, for example, a set of information may have a low need for confidentiality (LOW impact) but require HIGH availability. In this example, encryption may not be appropriate, but redundancy may be a requirement.

Most breaches that cause HIGH impact are a result of unauthorized access to Confidential information. Therefore, this document and System member assignment of classification places prime importance on the level of Confidentiality required of the information.