Clayton State University

Information Technology Services

Cyber Security Program Plan v1.0

Sensitive

July 2019

Revision and Sign-Off Sheet

Change Record:

Date	Author	Version	Change Reference
June 2019	LaMarcus Lawrence		Document creation;
July 24, 2019	LaMarcus Lawrence		Review and Update of Plan;

Reviewers:

Name	Version Approved	Position	Date
Bill Gruszka		CIO	7/30/19
Charles Read		VP	
Todd Birchfield		Director	
LaMarcus Lawrence	V 1.0	ISO	7/24/19

Distribution

Name	Location

Document Properties

Item	Details
Document Title	Cyber Security Program Plan
Document Type	Plan (Internal Use Only)
Author	LaMarcus Lawrence
Document Manager	LaMarcus Lawrence
Creation Date	June 2019
Last Updated	July 31,2019
Document Classification	Sensitive

Table of Contents

Executive Summary

The degree to which Clayton State University (CSU) has come to depend upon information systems to conduct routine, important, and critical missions and business functions means that the protection of the underlying systems and environments of operation is paramount to the success of the CSU. Understanding the overall effectiveness of implemented security and privacy controls is essential in determining the risk to CSU's operations and assets, to individuals, and other organizations resulting from the use of the systems.

Agility in our cyber security policies, guidance, and practices must be a goal for every process for CSU to maintain this competitive edge. Continuous improvement is mandated. The continuous improvement approach places great importance on harvesting and prioritizing ideas, rapid development and deployment of concepts and capabilities to enable constant preparation, shaping, and execution of our responses to the environment.

This Cyber Security Program Plan provides a broad overview of information security program elements to assist CSU in understanding how to establish and implement an information security program. Typically, CSU looks to the program for overall responsibility to ensure the selection and implementation of appropriate security controls and to demonstrate the effectiveness of satisfying their stated security requirements.

This document provides checklists of security activities and controls designed to help CSU improve the security posture of its organization and community. The checklists are drawn from industry implementations and standards to provide a mechanism to baseline existing security activities and controls against recommended best practices, identify gaps, capture the decision for risk acceptance or mitigation, and document an appropriate plan of action.

Transforming cyber security capabilities depends heavily on the ability to influence processes CSU uses to create, assess, test, and implement new ideas. Developing new approaches to problem solving depends on the synergy between each process, as an idea progresses from concept to reality. The focus of this Cyber Security Program Plan is to foster innovation, influence the planning, and acquisition processes to further the CSU cyber security mission.

Policy Statement

Each department will protect University resources by adopting and implementing, at a minimum, the security standards and procedures developed and approved by the Information Security Board of Review that can accessed from this Cyber Security Program Plan. Departments are encouraged to adopt standards that exceed the minimum requirements for the protection of University resources that are controlled exclusively within the Department. Individuals within the scope of this policy are responsible for complying with this policy and the Department's policy to ensure the security of University resources.

This Cyber Security Plan provides a set of procedures for assessing security controls and privacy controls employed within CSU information systems and organization. The assessment procedures are consistent with the security and privacy controls in University System of Georgia and the National Institute of Standards and Technology (NIST) Special Publications.

Purpose

The purpose of this policy is to ensure the protection of Clayton State University's information resources from accidental or intentional unauthorized access or damage while also preserving and nurturing the open, information-sharing requirements of its academic culture.

CSU's cyber security plan outlines our guidelines and provisions for preserving the security of our data and technology infrastructure. This plan will baseline existing cyber security related activities and controls at CSU.

These procedures are essential in conducting security control assessments and privacy control assessments that support CSU's risk management processes. This document provides guidance on how CSU, through the use of metrics, identifies the adequacy of in-place security controls, policies, and procedures. It provides an approach to help management decide where to invest in additional security protection resources or identify and evaluate non-productive controls.

Required Reporting

In 2008, Governor Sonny Perdue issued an Executive Order on Information Security. Each State agency is required to submit an annual Information Security Program Report. The USG - Office of Information Security will collect and compile the data into a comprehensive USG Information Security Program Report (ISPR), to be published by October 31st of each year. No USG institution or Georgia Public Library Service (GPLS) specific information will be reported.

The University System of Georgia (USG) has a compelling need to ensure confidentiality, integrity and availability of information technology (IT) systems and services as well as adequate protection from known and anticipated threats. As noted in Section 5.2.2 of the USG Information Technology Handbook, USG organizations are responsible for the designation of officials to fulfill key security functions and report on status of compliance with security policy, standards and procedures.

Authority and Approval

Clayton State University Information Technology Services has developed this document in furtherance of its statutory responsibilities under directives from the Board of Regents - University System of Georgia.

The approval of this plan, including any special memorandum language or other documentation required by CSU is by authority of

- University President, Dr. Tim Hynes
- Chief Information Officer, Bill Gruszka
- Information Security Officer, LaMarcus Lawrence

Applicability

This policy is applicable to all Clayton State University students, faculty and staff and to all others granted the use of Clayton State University information resources. Every user of any of CSU's information resources has some responsibility toward the protection of those assets. Some offices and individuals have very specific responsibilities.

This policy refers to all University information resources whether individually controlled or shared, stand-alone or networked. It applies to all computer and communication facilities owned, leased, operated, or contracted by the University.

This includes networking devices, personal digital assistants, telephones, wireless devices, personal computers, workstations, mainframes, minicomputers, and any associated peripherals and software, regardless of whether used for administration, research, teaching or other purposes.

Scope and Strategy

Clayton State University Information Technology Services (ITS) strategic approach

- Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements.
- Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

- Reviews the organization-wide information security program plan on an annual or ad-hoc basis.
- Updates the plan to address organizational changes and problems identified during plan implementation or security control assessments.
- Protects the information security program plan from unauthorized disclosure and modification.

This Cyber Security Plan is a living document; the vision, goals and objectives of this plan will be reviewed at least annually for relevancy and applicability. CSU's ability to successfully achieve the objectives in this plan requires the continued commitment and mandate from Senior Leadership and the cooperative support of all members of the CSU community.

Target Audience:

This policy applies to

- CSU faculty, staff, and users.
- CSU Security team, IT organization, leadership team.
- Contractors, volunteers, etc.
- Anyone who has permanent or temporary access to CSU systems and hardware.

Designated Contacts:

Lamarcus Lawrence
Information Security Officer
lamarcuslawrence@clayton.edu
678.466.4390

Glossary	
Internal risk	• Internal risk is an act leading to damage or loss stemming from human error, deliberate acts of sabotage, theft, or other malfeasance committed by employees and other insiders.
External risk	• External risks are outside the control of CSU ITS and CSU organization. Because of this, external risks are generally more difficult to predict and control.
Internal systems	• Computing Systems that reside within the infrastructure and management of the CSU.
External systems	• Computing Systems that reside outside the infrastructure and management of the CSU.
Third-Party or Service provider	• Any person or entity that maintains, processes, or otherwise is permitted access to CSU information through its provision of services directly to the University.
Information Systems	• An integrated set of components for collecting, storing, and processing data and for providing information, knowledge, and digital products. CSU information systems encompass all the hardware and software the University uses to access, collect, store, use, transmit, protect, or dispose of information.

Table 1: Glossary

Cyber Security Policy and Standards

Training faculty, staff and users to adopt security conscious behaviors and establishing policies for maintaining a secure environment go a long way toward improving CSU's overall security posture.

The Federal Trade Commission Safeguard Rules promulgated under Security Guidelines in section 501 and 505(b) of the Gramm-Leach-Bliley Act (GLBA) and Board of Regents requires CSU to implement an information security program that includes administrative, technical, and physical safeguards designed to achieve the following objectives

- Ensure the security and confidentiality of CSU information.
- Protect against any anticipated threats or hazards to the security or integrity of such information.
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to CSU.
- Ensure the proper disposal of CSU and student information.

Compendium:
CSU Office of Information Technology Services must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

The following checklist summarizes the various security best practices and controls that CSU incorporates into the dimensions of its cyber security policy and program.

Security Control	Rationale Associated
Assign responsibility for developing, implementing, and enforcing cyber security policy to a senior manager (the Information Security Officer). Ensure that the senior manager has the requisite authority across departments to enforce the policy.	• The development and implementation of effective security policies, plans, and procedures require the collaborative input and efforts of stakeholders in many departments of the CSU. Assigning a senior manager to organize and drive the efforts, with the authority to make and enforce decisions at each stage, raises the chances of success.

Identify Reasonably Foreseeable Internal and External Risks	• A risk assessment must be sufficient in scope to identify the reasonably foreseeable threats from within and outside CSU's operations that could result in unauthorized disclosure, misuse, alteration, or destruction of information or information systems, as well as the reasonably foreseeable threats due to the disposal of CSU data.
Identify security aspects to be governed by defined policies.	• In addition to identifying reasonably foreseeable threats to CSU information and University information systems and to CSU information that the University disposes, a risk assessment must evaluate the potential damage from these threats. • The Security Guidelines of GLBA allow broad latitude to determine the sensitivity of CSU information in the course of assessing the likelihood of, and potential damage from, the identified threats. • In the course of assessing the potential threats identified, CSU should consider its ability to identify unauthorized changes to records. In addition, it should take into consideration its ability to reconstruct the records from duplicate records or backup information systems.
Assess the Sufficiency of Policies and Procedures	• Evaluating the sufficiency of policies and procedures is a key element of CSU's risk assessment. The evaluation process includes identifying weaknesses or other deficiencies in existing security controls and assessing to what extent CSU information and information systems are at risk as a result of those weaknesses or to what extent CSU data is at risk as a result of improper methods of disposal.

Test Key Controls	• The Security Guidelines of GLBA recommend CSU test the key controls, systems, and procedures of its information security program. CSU's risk assessment should determine the scope, sequence, and frequency of testing.
Adjust the Cyber Security Program	• CSU should adjust its information security program to reflect the results of its ongoing risk assessment and the key controls it identifies as necessary to safeguard CSU information and ensure the proper disposal of CSU data. CSU should adjust the program to consider changes in technology, the sensitivity of University information, internal or external threats to information, and CSU's own changing business arrangement such as mergers, acquisitions, alliances and joint ventures, outsourcing arrangements, and changes in CSU information systems.
Responsibilities of and reporting to leadership.	• Under the Security Guidelines, CSU's leadership, or an appropriate committee of the University, must satisfy specific requirements designed to ensure that the CSU's information security program is developed, implemented, and maintained under the supervision of those who are ultimately responsible.

Table 2: Dimensions of Cyber Security Policy

Principles of Information Security

The purpose of information security is to protect the information resources of the University from unauthorized access or damage. The underlying principles that CSU ITS follows to achieve these objectives are:

- *Information Resource Availability*
  The information resources of the University, including the network, the hardware, the software, the facilities, the infrastructure, and any other such resources, are available to support the teaching, learning, research, or administrative roles for which they are designated.
- *Information Integrity*
  The information used in the pursuit of teaching, learning, research, or administration can be trusted to correctly reflect the reality it represents.
- *Information Confidentiality*
  The ability to access or modify information is provided only to authorized users for authorized purposes.
- *Support of Academic Pursuits*
  The requirement to safeguard information resources must be balanced with the need to support the pursuit of legitimate academic objectives.
- *Access to Information*
  The value of information as an institutional resource increases through its appropriate use; its value diminishes through misuse, misinterpretation, or unnecessary restrictions to its access.

Maturity/ Development model for CSU Cyber Security Program

At a high level, CSU's approach to the NIST Cyber Security Framework is composed of three parts:

- Core: The core is a set of cyber-security activities, desired outcomes, and relevant references common across CSU's critical infrastructure sectors.
- Implementation Tiers are a scaled ranking system (1-4) that describes the degree to which an organization exhibits the characteristics described in the NIST Cybersecurity Framework.
- Profiles: Framework Profiles enable CSU to create a roadmap for reducing cybersecurity risk. Essential it is a tool for CSU to identify opportunities for improvement in their cybersecurity posture.

CSU's core consists of five key functions

Figure 1: I.P.D.R.R

- ***Identify*:** What processes and assets need protection?
- ***Protect:*** What safeguards are available?
- ***Detect:*** What techniques can identify cyber-incidents?
- ***Respond:*** What techniques can contain the impact of a cyber-incident?
- ***Recover:*** What techniques can restore capabilities?

CSU's Steps for continual Improvement of the Cyber Security Program

The following steps illustrate how CSU plans to use the Cyber Security Framework to continually improve its existing program:

Step 1: Prioritize and Scope
CSU will identify its business/mission objectives and high-level organizational priorities. With this information, CSU will make strategic decisions regarding cybersecurity implementations and determines the scope of systems and assets that support the selected business line or process. CSU's Framework will be adapted to support the different business lines or processes within CSU, which may have different business needs and associated risk tolerance. Risk tolerances may be reflected in a target Implementation Tier.

Step 2: Orient
As the scope of the continual changes in the cybersecurity program are being determined for the business line or process, CSU will identify related systems and assets, regulatory requirements, and overall risk approach. CSU will then consult sources (internal or external) to identify threats and vulnerabilities applicable to those systems and assets.

Step 3: Create a Current Profile
CSU will continue working on developing a Current Profile by indicating which category and subcategory outcomes from the Cyber Security Framework Core are currently being achieved. If an outcome is partially achieved, noting this fact will help support subsequent steps by providing baseline information.

Step 4: Conduct a Risk Assessment
This assessment could be guided by the CSU's overall risk management process or previous risk assessment activities, through supported platforms from the USG. CSU will analyze the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on CSU. It is important that CSU identifies emerging risks and uses cyber threat information from internal and external sources to gain a better understanding of the likelihood and impact of cybersecurity events.

Step 5: Create a Target Profile
CSU will create a Target Profile that focuses on the NIST Assessment of the Cyber Security Framework Categories and Subcategories which will fortify CSU's desired cybersecurity outcomes. CSU may develop their own additional Categories and Subcategories to account for unique organizational risks. CSU may also consider influences and requirements of external stakeholders such as sector entities, customers, and business partners when creating a Target Profile. The Target Profile should appropriately reflect criteria within the target Implementation Tier.

Step 6: Determine, Analyze, and Prioritize Gaps
CSU will compare the Current Profile and the Target Profile to determine gaps. Next, CSU will create a prioritized action plan to address gaps–reflecting mission drivers, costs and benefits, and risks–to achieve the outcomes in the Target Profile. CSU will then determine resources, including funding and workforce, necessary to address the gaps. Using Profiles in this manner encourages CSU to make informed decisions about cybersecurity activities, supports risk management, and enables the organization to perform cost-effective, targeted improvements.

Step 7: Implement Action Plan
CSU will determine which actions to take to address the gaps, if any, identified in the previous step and then adjusts its current cybersecurity practices in order to achieve the Target Profile. For further guidance, the NIST Cyber Security Framework identifies example Information References regarding the Categories and Subcategories, but CSU will determine which standards, guidelines, and practices, including those that are sector specific, that work best for CSU needs.

CSU will repeat the steps as needed to continuously assess and improve its cybersecurity.

Plan of Action and Milestone (POA&M)

The plan of action and milestones (POA&M) is a key document in CSU information security program and is subject to federal reporting requirements established by the University System of Georgia and Office of Management and Budget.

With the increasing emphasis on organization-wide risk management across all three tiers in the risk management hierarchy (organization, mission/business process, and information system), CSU views plans of action and milestones from an organizational perspective, prioritizing risk response actions and ensuring consistency with the goals and objectives of Clayton State University.

CSU's plan of action and milestones updates are based on findings from security control assessments and continuous monitoring activities.

Clayton State University Information Technology Services Department implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems are developed and maintained. CSU ITS will continue to review plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

Layered Approach to Cybersecurity

A layered approach to cyber security, or what is also known as 'Defense in Depth,' refers to the practice of combining multiple security controls to slow and eventually thwart a security attack. By combining a myriad of hardware, software, policy and assessment tools, CSU will significantly decrease its risk exposure.

CSU's layered approach

- **Data** - This is the sensitive information CSU houses like SSNs, DOBS, financial records, patents, trade secrets, contact lists and more.

  Relevant questions: Where is my data in space and time? On what specific drives? Utilizing what database technologies? Accessible remotely by what tools and people?

- **Application Security** - These are the controls within CSU's line-of-business applications like People Soft, Banner, D2L, document management, and so on.

  Relevant questions: Has CSU setup security profiles, access rights, permissions, ethical walls and passwords? Do we have or need dual-factor authentication? How is CSU sharing important documents and emails with clients?

- **IT Infrastructure Security** - These are the actual hardware and software assets CSU employs for security like end-point protection, antispam, firewall, content filtering, patch & vulnerability management, encryption, physical security and more.

Relevant questions: Am I proactively managing security? Is CSU testing for new vulnerabilities on an ongoing basis? Does CSU have encryption for data at rest?

- **Education & Policy Enforcement** - The creation of CSU's policies and plans that constitute the CSU's Cyber security implementations, such as written security policies, incident response plan, disaster recovery plan and more.

  Relevant questions: Are CSU faculty and users trained on proper security? Do they know how to identify a malicious email or how to respond if they believe a virus has infected their PC? Are CSU policies adequate, written, updated and enforced?

- **Continual Assessment & Improvement** - Finally, CSU needs an ongoing process for the testing of new attack vectors, the effectiveness of the CSU Framework, and testing for weaknesses in the approach.

  Relevant questions: Have new threats emerged? Do recent close-calls warrant a review of CSU's practices? In spite of our efforts and security spend, are users really knowledgeable and therefore safe? Have any of the new programs or services CSU purchased this year compromised our security posture?

Data Lifecycle Management

Data lifecycle management (DLM) is a policy-based approach to managing the flow of an information system's data throughout its life cycle: from creation and initial storage to the time when it becomes obsolete and is deleted.

CSU uses the DLM model to establish benchmarks, set future goals, and measure progress toward targets aimed at identifying duplicate student records, managing data migration, matching criteria and processes. CSU ITS will foster methods to design road maps to determine how to manage the complete data supply chain – "what comes first?" and sequences the University must take to get there.

CSU ITS understands the first step, creating an enterprise architecture to align visions, goals and objectives, putting together a direction for the strategy, creating principals and models and frameworks, and designing a multi-generation plan. CSU ITS' second step is the continual design of data object architecture to align the business, standards, data governance, organization model, and management of change.

With the right data lifecycle management practices in place, CSU can mitigate the risk of data loss, deletion and breaches, as well as the fines, penalties, downtime and reputation management struggles

that go hand in hand with these occurrences. CSU ITS will continue to incorporate these data lifecycle management practices into their short- and long-term goals of security implementations.

CSU data lifecycle management practices

- ***Define your data types***
  CSU handles many different types of documents and files. In order to outline an internal data management policy, CSU will need to distinguish the types of data being managed. Graduate or Undergraduate data will need to be handled differently than accounting data. Each data type may have its own retention length minimums, archive policies, and safe destruction methods. Identifying the types of data CSU stores and utilizes is the starting point for outlining how to manage each kind.

- ***Create a file naming process***
  Losing data because it's unsearchable is an easily preventable data lifecycle management failure. CSU implements a simple, yet thorough file naming structure that will allow anyone within the organization to find the data they need in seconds.

- ***Implement a strong data backup plan***
  When a file is created, its vulnerability is immediate. Any file that lives on a physical storage device or computer is vulnerable to loss and deletion. While loss and deletion can occur due to physical damage, natural disaster, virus and many other threats, some of the most common data loss scenarios boil down to human error. It takes seconds to make an accidental, irreparable file change, or to accidentally delete an important document — and it can take days to get that data back, if it can be saved at all.

- ***Create a data archive policy that works for your business***
  Creating a detailed archive policy will help CSU and its employees decide how to manage data that is no longer in use but needs to be retained. CSU's archive strategy will vary depending on the type of data involved. Developing a complete archive policy will provide CSU with guidelines that will empower them to make decisions about which files to archive and which files to delete. Additionally, CSU ITS will continue to develop instructions on where to archive data and how to archive data safely to avoid data breach.

- ***Archive seldom used data***
  In the process of distinguishing between the types of data CSU owns and setting guidelines for each, CSU may notice that some of the data and files haven't been updated or accessed for long periods of time. Depending on the type of data involved, CSU may elect to move this infrequently used data to a storage archive. Moving seldom used data into an archive can clear

up storage space on the devices you use daily and accelerate processing speeds to make the University run faster.

- ***Set data deletion guidelines***
  CSU ITS' continual development of archives and data deletion processes will help the University determine archiving best practices per data type placing CSU in compliance with industry regulations and ensures the data cannot find itself in the wrong hands once it leaves the University System.

- ***Create a complete data management policy***
  Training and awareness of guidelines is paramount in getting the University community on board and participating in the data lifecycle management structure. CSU ITS will define processes for handling data storage, backup, management, archiving, and deletion, through campus and Board of Regent policies.

By implementing these best practices, CSU can check off a highly important step in building its internal data lifecycle management practices.

Cyber Security Plan Controls and Requirements

The security requirements described in this Cyber Security Program Plan have been developed based on three fundamental assumptions

- Statutory and regulatory requirements for the protection of CSU data are consistent, whether such information resides within internal or external systems including the environments in which those systems operate.
- Safeguards implemented to protect CSU data are consistent in both internal or external systems and organizations.
- The confidentiality impact value for CSU is in accordance with Federal Information Processing Standards (FIPS) Publication 199.15 and Gramm-Leach-Bliley Act (GLBA).

Notifying the University System Office

CSU Computer Incident Response Team and management will promptly investigate incidents involving loss, damage, misuse of information assets, or improper dissemination of information. USG organizations are required to report cybersecurity incidents consistent with the security reporting requirements of the USG Information Technology Handbook. Reports must be submitted to USG Cybersecurity per the Reporting Requirements noted in Section 5.10 of the USG Information Technology Handbook.

In addition, CSU will submit an incident follow-up report that includes the application of lessons learned from incidents, together with the development and implementation of appropriate corrective actions directed to preventing or mitigating the risk of similar occurrences in the future. Reports must be submitted to USG Cybersecurity using the ticketing system.

In the event of a cybersecurity event or incident concerning sensitive organizational or personal data, immediately report the event or incident by calling the ITS Helpdesk at 706-583-2001, or 1-888-875-3697 (Toll free within Georgia) or by emailing the Helpdesk at helpdesk@usg.edu. The ITS Helpdesk is available 24 hours a day, seven days a week.

Classification of Information

All University information is classified into one of four levels based on sensitivity and risk. These classifications take into account legal protections, contractual agreements, ethical considerations, privacy issues, and strategic or proprietary worth. The classification level determines the security protections and access authorization mechanisms which must be used for the information. Security policies can be found in the Clayton State University Privacy and Controlled Unclassified Information CUI) Policy. The information classifications are as follows:

- *Prohibited Information:*
  Information is classified as "Prohibited" if protection of the information is required by law or government regulation, *or* CSU is required either to provide notice to the individual if information is inappropriately accessed or to report unauthorized access to the governing body.
- *Restricted Information:*
  Information is classified as "Restricted" if it would otherwise qualify as "Prohibited" but it has been determined by the Data Governance Board that prohibiting information storage on computing equipment would significantly reduce faculty, staff, or student effectiveness when acting in support of CSU's mission.
- *Confidential Information:*
  Information is classified as "Confidential" if it is not considered to be prohibited or restricted and is not generally available to the public, or it is listed as confidential in the Classification of Common Data Elements.
- *Public Information*
  All information which does not fall into one of these categories is considered to be "public."

Requirement Control Families

The Security Guidelines require CSU to design an information security program to control the risks identified through its assessment, commensurate with the sensitivity of the information and the complexity and scope of its activities. Thus, CSU must consider a variety of policies, procedures, and technical controls and adopt those measures that it determines can appropriately address the identified risks. Below are the developments and implementations that CSU utilizes to control risks.

Access Controls (AC)

Adequate security of information and information systems is a fundamental management responsibility. Nearly all applications that deal with financial, privacy, safety, or academics include some form of access (authorization) control. Access control is concerned with determining the allowed activities of legitimate users, mediating every attempt by a user to access a resource in the system.

CSU access control systems are made up of three abstractions, access control policies, models, and mechanisms. Access control policies are high-level requirements that specify how access is managed and who may access information under what circumstances. At a high level, CSU access control policies are enforced through a mechanism that translates a user's access request, often in terms of a structure that a system provides. A model is a formal presentation of the security policy enforced by the system and is useful for proving theoretical limitations of a system. Access control models are of general interest to both users and vendors, bridging the rather wide gap in abstraction between policy and mechanism.

Compendium
CSU Office of Information Technology Services must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

Awareness and Training (AT)

CSU determines the content and frequency of security awareness training and security awareness techniques based on the specific organizational requirements and the systems to which personnel have authorized access.

CSU's approach includes a concrete understanding of the need for information security in conjunction with user actions to maintain security and to respond to suspected security incidents. CSU's approach also addresses awareness for operational security. Security awareness techniques can include formal training, offering supplies inscribed with security reminders, generating email advisories or notices from CSU organizational officials, displaying logon screen messages, displaying posters, and conducting information security-awareness events. CSU recognizes and will align all efforts with the expanded requirements under the new GLBA Safeguards Rule.

Compendium
CSU Office of Information Technology Services must: (i) ensure that faculty, staff and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of CSU information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information-security-related duties and responsibilities.

CSU Annual Awareness and Training Plan and Agenda

Training Goals

- Provide training on use of CSU information and computing resources in a protective, efficient, ethical, and lawful manner.
- Ensure that all CSU employees (internal, external, and contractors) agree to the Rules of Behavior regarding the use of CSU equipment, accounts, and information only for authorized purposes.
- Test employees understanding of the material.

Agenda

- Applicability
- General computer and information use
- Responsibility and Accountability
- Using a CSU Computer – Limited Personal Use
- Employee Access and Protection
- Password Management
- Using Email
- Local Administrator Accounts
- Portable and Removable Media
- Cell Phone and Camera Security
- Protecting sensitive information and PII & new requirements
- Social Engineering and Phishing
- Identity Theft
- Malware
- Rules of Behavior and Acceptable Use Policy

Recommended Tools and Materials

- USG organizational learning management system (LMS).
- USG organizationally developed LMS.
- Awareness training module delivered via electronic presentation.
- Document-based awareness training module.

Audit and Accountability (AU)

The goal of the Audit and Accountability (AU) objective is to ensure there are enough controls in place to provide auditable evidence for CSU system transactions and that key records are available for a sufficient amount of time. If the system crashes, is hacked, or there is human error on an entry, CSU will have ways to recover data and trace back or rollback changes. This control addresses the establishment of policy and procedures for the effective implementation of the selected security controls (i.e. risk management, media protection, contingency planning) and their control enhancements. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.

Compendium
CSU Office of Information Technology Services must create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity and ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

Configuration Management (CM)

CSU approaches the necessity of Configuration Management in a disciplined manner to ensure the integrity and availability of IT assets in support CSU's mission.

Configuration Management (CM) is a discipline to ensure that the configuration items are known and documented, and that all subsequent changes to it are controlled and tracked. Configuration items are the information system items (hardware, software, firmware, and documentation) to be managed. The goals of using CM are to ensure the integrity of CSU data and to make its evolution more manageable. Effective CM imposes control over the activities that require the updating and usage of multiple versions of data artifacts in CSU assets.

Compendium
CSU Office of Information Technology Services must establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles and establish and enforce security configuration settings for information technology products employed in CSU organizational information systems.

Identification and Authentication (IA)

An Identity and Access Authentication system's purpose is to control the framework and facilitate electronic identities, specifically procedures of identity management. Identity and Authentication Management technology are used to ensure that services are managed, authorized, and audited properly within CSU.

CSU's security measures establish the policy for managing user identification and authentication in order to access information and information systems supporting Clayton State University**.**

Compendium
CSU Office of Information Technology Services must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to CSU organizational information systems.

Implementing Identification and Authentication (IA):

Organizational users include employees or individuals that CSU deems to have equivalent status of employees (e.g., contractors, guest researchers). CSU applies this control accesses that occur through authorized use of group authenticators without individual authentication. CSU may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity. CSU employs passwords or tokens to authenticate user identities, or in the case multifactor authentication, or some combination thereof.

Access to organizational CSU systems is defined as either local access or network access. Local access is any access to organizational information systems by users (or processes acting on behalf of users) where

such access is obtained by direct connections without the use of networks. Network access is access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks (e.g., the Internet). Internal networks include local area networks and wide area networks. In addition, the use of encrypted virtual private networks (VPNs) for network connections between organization-controlled endpoints and non-organization controlled endpoints may be treated as internal networks from the perspective of protecting the confidentiality and integrity of information traversing the network.

CSU Requires:

- CSU systems implements multifactor authentication for network access to privileged and non-privileged accounts.
- CSU systems implement multifactor authentication for local access to privileged and non-privileged accounts.
- CSU systems implement multifactor authentication for network access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets CSU BYOD Requirements.
- CSU systems implement replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts. (i.e. protocols that use nonce or challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators.)
- CSU system implement multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets CSU BYOD policy and requirements.
- CSU Physical Access systems verify identifiable credentials
- CSU systems implements out-of-band authentication where specified and recommended. Explained: Out-of-band authentication (OOBA) refers to the use of two separate communication paths to identify and authenticate users or devices to an information system. The first path (i.e., the in-band path), is used to identify and authenticate users or devices, and generally is the path through which information flows. The second path (i.e., the out-of-band path) is used to independently verify the authentication and/or requested action. For example, a user authenticates via a notebook computer to a remote server to which the user desires access, and requests some action of the server via that communication path. Subsequently, the server contacts the user via the user's cell phone to verify that the requested action originated from the user. The user may either confirm the intended action to an individual on the telephone or provide an authentication code via the telephone. This type of authentication can be employed by organizations to mitigate actual or suspected man-in the-middle attacks. The conditions for activation can include, for example, suspicious activities, new threat indicators or elevated threat levels, or the impact level or classification level of information in requested transactions.

Incident Response (IR)

It is vital to the CSU community that computer security incidents that threaten the security or privacy of confidential information are properly identified, contained, investigated, and remedied. CSU's design and implementation standards for the Incident Response Plan can be referenced in the CSU Incident Response Plan.

The purpose of this Cyber Security Plan is to provide the basis of appropriate response to incidents that threaten the confidentiality, integrity, and availability of university digital assets, information systems, and the networks that deliver the information.

The Incident Response Policy provides a process for documentation, appropriate reporting internally and externally, and communication to the community as part of an ongoing educational effort. Finally, the policy establishes responsibility and accountability for all steps in the process of addressing computer security incidents.

Compendium
CSU Office of Information Technology Services must establish an operational-incident-handling capability for CSU information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities, while assuring that all breaches are report to University System of Georgia and track, document, and report incidents to appropriate organizational officials and/or authorities.

Maintenance (MA)

Compendium
CSU Office of Information Technology Services must perform periodic and timely maintenance on organizational information systems and provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

Media Protection (MP)

Compendium
CSU Office of Information Technology Services must protect the information system media both paper and digital, limit access to information on information system media to authorized users, and sanitize or destroy information system media before disposal or release for reuse.

Contingency Planning (CP)

Compendium
CSU Office of Information Technology Services must establish, maintain, and effectively implement plans for emergency response, backup operations, and post disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

CSU will

- Tests the contingency plan for the information system to determine the effectiveness of the plan and the organizational readiness to execute the plan.
- Reviews the contingency plan test results.
- Initiates corrective actions, if needed.

Methods for testing contingency plans

CSU's methods for testing contingency plans to determine the effectiveness of the plans and to identify potential weaknesses in the plans include, for example, walk-through and tabletop exercises, checklists, simulations (parallel, full interrupt), and comprehensive exercises. CSU conducts testing based on the continuity requirements in contingency plans and include a determination of the effects on organizational operations, assets, and individuals arising due to contingency operations. CSU has flexibility and discretion in the breadth, depth, and timelines of corrective actions.

CSU CP Enhancement Methods and Acknowledgement

Coordinate with related Plans
Plans related to contingency plans for University information systems include Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, and CSU Incident Response Plans. CSU coordinates the organizational elements of related plans and aligns such elements to related plans to facilitate control enhancement of managing CSU's contingency plan.

Alternate Processing Sites
CSU tests the contingency plan at the alternate processing site

- To familiarize contingency personnel with the facility and available resources.
- To evaluate the capabilities of the alternate processing site to support contingency operations.

Automated Testing
CSU endorses the benefit of automated mechanisms to more thoroughly and effectively test the contingency plan by providing more complete coverage of contingency issues, by selecting more realistic

test scenarios and environments, and by effectively stressing the information system and supported missions.

Full Recovery/ Reconstitution
The CSU ITS acknowledges and will include a full recovery and reconstitution of the information system to a known state as part of contingency plan testing.

Personnel Security (PS)

Compendium
CSU Office of Information Technology Services must ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions, ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers, and employ formal sanctions for personnel failing to comply with CSU Code of Conduct and procedures.

CSU performs

- Screening of individuals prior to authorizing access to the information system.
- Rescreening of individuals according to defined conditions requiring rescreening and, where rescreening is so indicated.

CSU implements:

Classifying Information Access
CSU ensures that individuals accessing a University information system processing, storing, or transmitting University information are cleared and indoctrinated to the highest classification level of the information to which they have access on the system.

Formal Indoctrination
CSU ensures that individuals accessing a University information system processing, storing, or transmitting the various types of University information needing formal indoctrination, are formally indoctrinated for all the relevant types of information to which they have access on the system.

Special Compliance Measures
CSU ensures that individuals accessing a University information system processing, storing, or transmitting University information requiring special protection have valid access authorizations and satisfy University and BOR defined additional personnel screening criteria**.**

Physical Protection

Compendium
CSU Office of Information Technology Services must limit physical access to information systems, equipment, and the respective operating environments to authorized individuals, protect the physical site and support infrastructure for information systems, provide supporting utilities for information systems, protect information systems against environmental hazards, and provide appropriate environmental controls in facilities containing information systems.

CSU implements

Information System Access
The organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility at server rooms, media storage areas, data and communications centers.

Information System Boundaries
The organization performs security checks at the physical boundary of the facility or information system for unauthorized exfiltration of information or removal of information system components.

Continuous Guards/Alarms/ Monitoring
CSU employs the Clayton State Police Department and/or alarms to monitor every physical access point to the facility where the information system resides 24 hours per day, 7 days per week.

Tamper Protection
CSU utilizes employs defined security safeguards to detect and prevent physical tampering or alteration of defined hardware components within the information system.

Facility Penetration Testing
CSU endorses a penetration testing process that includes, unannounced attempts to bypass or circumvent security controls associated with physical access points to the facility.

Risk Assessment (RA)

A risk assessment is a process which determines what information resources exist that require protection and understand and document potential risks from IT security failures that may cause loss of information confidentiality, integrity, or availability. The purpose of a risk assessment is to help management create appropriate strategies and controls for stewardship of information assets.

CSU Information Technology Services, with the aid of other departments, will conduct an annual risk assessment and/or business impact analysis in order to

- Inventory and determine the nature of campus information resources.
- Understand and document the risks in the event of failures that may cause loss of confidentiality, integrity, or availability of information resources.
- Identify the level of security necessary for the protection of the resources.

Identifying internal and external risk

CSU follows a standard, with structural implementation support from USG that are set out by NIST, in conducting a risk assessment that typically include the following six steps

- Identify and Document Asset Vulnerabilities.
- Identify and Document Internal and External Threats.
- Acquire Threat and Vulnerability Information from External Sources.
- Identify Potential Business Impacts and Likelihoods.
- Determine Enterprise Risk by Reviewing Threats, Vulnerabilities, Likelihoods and Impacts.
- Identify and Prioritize Risk Responses.

Compendium

CSU Information Technology Services must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

Clearly defined system boundaries are a prerequisite for effective risk assessments. Such risk assessments consider threats, vulnerabilities, likelihood, and impact to organizational operations, organizational assets, and individuals based on the operation and use of CSU systems.

Risk assessments also consider risk from external parties (e.g., service providers, contractors operating systems on behalf of the organization, individuals accessing organizational systems, outsourcing entities). Risk assessments, either formal or informal, can be conducted at the organization level, the mission or business process level, or the system level, and at any phase in the system development life cycle. CSU utilizes NIST Special Publication 800-30 to provide guidance on conducting risk assessments.

Developing and implementing safeguards to control the risks

The risks and international regulations (General Data Protection Regulation) that apply to University system environments have made CSU incorporate, as a business process, the aspect of information security. Like all processes, CSU needs to be assigned resources and budgets to ensure proper implementation. Because the objective of the security process is to minimize exposure to risk, it is important to determine the effectiveness of the implemented controls.

CSU ITS standards will continue to provide and support a framework for information security risk management within the University. The purpose of this system is to identify and minimize risks when handling information within the company's processes, so the confidentiality, integrity and availability of the information are preserved, maximizing its value as input to the value chain processes within the University.

CSU ITS implements a **Plan, Do, Check, Act** cycle within the University based on the following scheme:

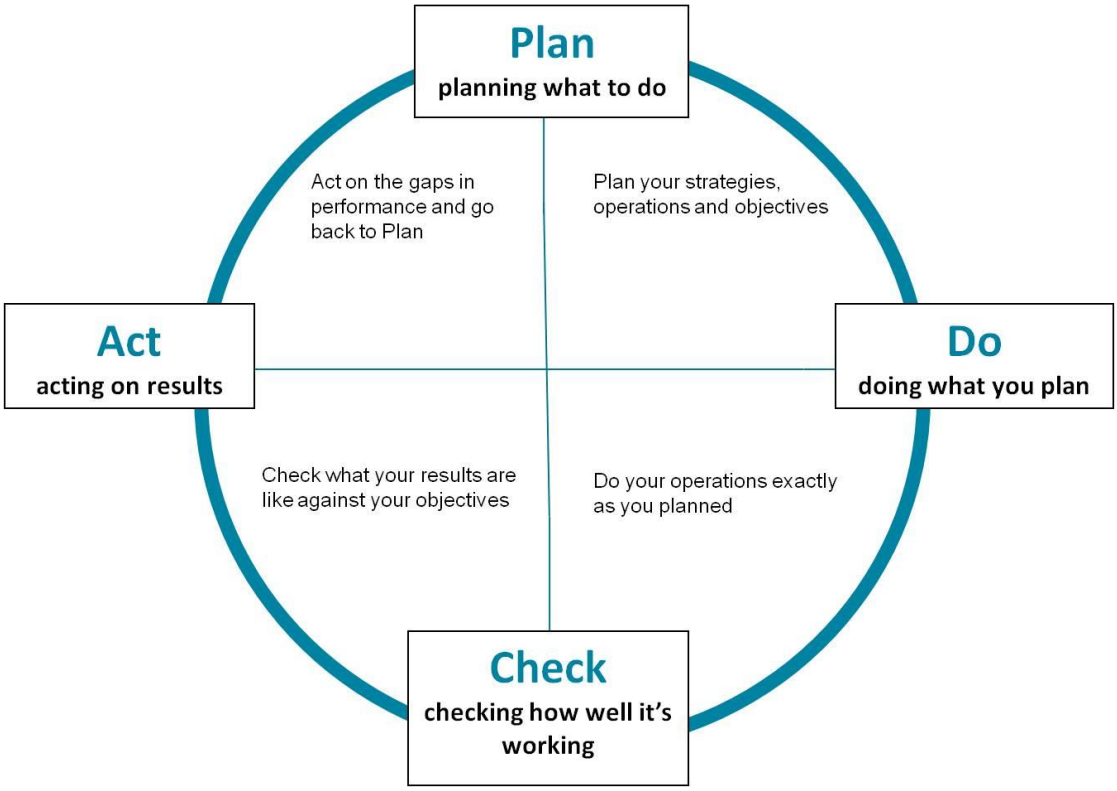

Figure 2: Plan, Do, Check, Act

CSU objectives for each step of the cycle are

- **Plan:** To establish information security policy and objectives to manage risk and improve the level of risk exposure.
- **Do:** Implement the security controls planned for the CSU systems in accordance with established information policy and security objectives.
- **Check:** To evaluate and measure process performance and controls against

established guidelines.

- **Act:** Take corrective and preventive actions based on the results of verification in order to implement a continuous improvement to the CSU systems.

As part of this process, the CSU ITS must implement the necessary security controls and the required measurement to lower the risk exposure of the organization to an acceptable level. Understanding that attaining resources while aligning business needs can often be a difficult task, it is imperative to reinforce the significant justifications to determine if information security controls are necessary and good for the University. In order to provide accurate data to Leadership, CSU ITS must identify risks to organizational processes and develop a measurement system capable of determining the effectiveness of safeguards and controls.

CSU ITS Internal Control Model

Preventive Controls
At CSU prevention is the first line of the defense in the control structure. Preventive controls are passive techniques designed to reduce the frequency of occurrence of undesirable events. Preventive controls force compliance with prescribed or desired actions and thus screen out aberrant events. When CSU ITS designs internal control systems, an ounce of prevention is most certainly worth a pound of cure. Preventing errors and fraud is far more cost effective than detecting and correcting problems after they occur.

Detective Controls
Detective controls form CSU's second line of defense. These are devices, techniques, and procedures designed to identify and expose undesirable events that elude preventive controls.

Within CSU, preventive and/or detective controls are activities that prevent or detect threats or vulnerabilities to mitigate risks. Anti-virus, anti-malware and anti-spyware protect and prevent known and emerging computer viruses, malicious programs and unwanted software applications on the endpoint. CSU incorporates Cylance Endpoint Security for these measures.

Per section 5.8.3 of the USG Information Technology Handbook
All endpoint devices must have installed and activated anti-virus, anti-malware and anti-spyware protection software. Anti-virus is a mandatory foundational control for protecting state-owned assets against certain attack vectors. Where possible, anti-virus software must be installed and configured for automatic updates on desktops, portables and mobile assets.

Corrective Controls

CSU's corrective controls are actions taken to reverse the effects of errors detected in the previous step. CSU ITS makes an important distinction between detective controls and corrective controls. Detective controls identify anomalies and draw attention to them; corrective controls actually fix the problem.

Linking a corrective action to a detected error, as an automatic response, may result in an incorrect action that causes a worse problem than the original error. For this reason, CSU views error correction as a separate control step that should be taken cautiously.

Implementing a Risk Management Program

The goal of a risk management program is to identify the risks, understand their likelihood and impact on the business, and then put in place security controls that mitigate the risks to a level acceptable to CSU. In addition to assessment and mitigation, a robust risk management program includes ongoing evaluation and assessment of cyber security risks and controls throughout the program life cycle.

Under the Security Guidelines GLBA section 501 and 505(b), a CSU and USG risk assessments must include the following four steps

- Identifying reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of CSU information or CSU information systems.
- Assessing the likelihood and potential damage of identified threats, taking into consideration the sensitivity of the CSU information.
- Assessing the sufficiency of the policies, procedures, CSU information systems, and other arrangements in place to control the identified risks.
- Applying each of the foregoing steps in connection with the disposal of information.

Security Assessment (SA)

Compendium

CSU Office of Information Technology Services must periodically assess the security controls in organizational information systems to determine if the controls are effective in their application, develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems, authorize the operation of organizational information systems and any associated information system connections, and monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

CSU will

- Develop a security assessment plan that describes the scope of the assessment including

    - ✓ Security controls and control enhancements under assessment.
    - ✓ Assessment procedures to be used to determine security control effectiveness.
    - ✓ Assessment environment, assessment team, and assessment roles and responsibilities.

- Assess the CSU security controls in the information system and its environment of operation to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements.
- Produce a security assessment report that documents the results of the assessment.
- Provide the results of the security control assessment to CSU ITS and University Leadership.

CSU assesses security controls in University information systems and the environments in which those systems operate as part of initial and ongoing security authorizations, Board of Regents annual assessments, continuous monitoring, and system development life cycle activities.

Security assessments ensure that information security is built into University information systems, identify weaknesses and deficiencies early in the development process, provide essential information needed to make risk-based decisions as part of security authorization processes, and ensure compliance to vulnerability mitigation procedures. CSU utilizes other types of assessment activities such as vulnerability scanning and system monitoring to maintain the security posture of information systems during the entire life cycle.

CSU Enhancement Methods for Security Assessments

Independent Assessors
CSU employs assessors or assessment teams to conduct security control assessments. Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of University information systems. Impartiality implies that assessors are free from any perceived or actual conflicts of interest regarding the development, operation, or management of the University information systems under assessment or to the determination of security control effectiveness.

Specialized Assessments
CSU includes as part of security control assessments, announced or unannounced in-depth monitoring, vulnerability scanning, malicious user testing, insider threat assessment, and performance/load testing.

CSU employs information system monitoring, verification and validation testing to improve readiness by exercising University capabilities and indicating current performance levels as a means of focusing actions to improve security. CSU conducts assessment activities in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

External Organization

CSU may often rely on assessments of specific information systems by other (external) organizations. Utilizing such existing assessments (i.e., reusing existing assessment evidence) can significantly decrease the time and resources required for University assessments by limiting the amount of independent assessment activities that CSU needs to perform. The factors that CSU considers in determining whether to accept assessment results from external organizations can vary. Determinations for accepting assessment results can be based on, for example, past assessment experiences CSU has had with contracting organization. The reputation, the level of detail of supporting assessment documentation provided, or mandates imposed upon contractor by federal legislation, policies, or directives are an acceptance factor too.

Timeline for Security assessment:

CSU shall assess the risk associated with each business system to determine what security requirements are applicable. The security assessment determines the appropriate placement of each system and application within the security framework and evaluates the network resources, systems, data and applications based upon their criticality. As the critical nature of the data and applications increases, the security measures required to protect the data and applications also increase.

Security assessments must observe the following requirements:

- Security controls must be assessed under a Continuous Monitoring program supporting a frequency defined by the Information Security Officer for at least once every three (3) years, or when significant changes are made to the system or supported environment; and until the system is decommissioned.
- CSU shall provide USG their bi-annual compliance and assessments reports.

This certification includes compliance of cloud service providers. Any deficiencies identified within the CSU which would preclude them from being compliant, must be addressed using the ITS Change Management Process. Annual reports must ensure the agency has identified their security deficiencies and estimated cost for remediation.

The report may include, but is not limited, to the following:

- Security boundary devices, e.g. firewalls, intrusion detection/prevention systems (IDPS)
- Vulnerability management e.g. scanning and patching systems
- Resource constraints
- Cybersecurity training deficiencies
- System development lifecycle (SDLC) deficiencies

When changes are made to an information system, a Security Impact Analysis shall be conducted to determine the extent to which changes to the information system will affect the security state of the system. CSU shall follow the procedures below when significant changes are made to the information system:

- Document assessment results and include correction or mitigation recommendations, to enable risk management and oversight activities.
- Provide the assessment results to the ISO and ITS Leadership.
- The security controls in the information system will be assessed on an annual basis to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
- Cloud vendors must provide as an attestation of compliance.

System and Communications Protection (SC)

Compendium
CSU Office of Information Technology Services must monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of CSU information systems, and employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within CSU information systems.

System and Information Integrity (SI)

Compendium
CSU Office of Information Technology Services must identify, report, and correct information and information system flaws in a timely manner, provide protection from malicious code at appropriate locations within CSU organizational information systems, and monitor information system security alerts and advisories and take appropriate actions in response.

CSU ITS utilizes a CSU Log Standard and Policy to govern this control, with Service Now and system alerts as conduits to manage thus policies.

Software Development Life Cycle (SDLC) Controls

Secure software is a product of a secure software development process. If CSU develops software internally, it should make sure that it does so by leveraging security activities during the various phases of software development.

Compendium
CSU Office of Information Technology Services must: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development lifecycle processes that incorporate information security considerations; (iii)employ software usage and installation restrictions;

Third-Party Oversight Management Controls

Compendium
CSU Office of Information Technology Services must ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

The Security Guidelines of GLBA and USG set forth specific requirements that apply to CSU's arrangements with service providers. CSU will

- Exercise appropriate due diligence in selecting its service providers.
- Require its service providers by contract to implement appropriate measures designed to meet the objectives of the Security Guidelines.
- Where indicated by its risk assessment, monitor its service providers to confirm that they have satisfied their obligations under the contract described above.

Violations of Policy and Misuse

All individuals accessing University data at CSU are required to comply with federal and state laws, University policies and procedures regarding security of highly sensitive data. Suspected violations of this policy should be reported to the appropriate persons in the CSU IT Helpdesk, the individual's manager, or other University officials.

Compendium
CSU Office of Information Technology Services must protect and enforce the prevention of unauthorized modification and exposure of this cyber security plan and the underlying policies, when applicable.

Violations of this policy include, but are not limited to accessing information to which the individual has no legitimate right, enabling unauthorized individuals to access information, disclosing information in a way that violates applicable policy, procedure, or other relevant regulations or laws, inappropriately modifies or destroys information, inadequately protects information, or ignores the explicit requirements of Data Owners for the proper management, use, and protection of information resources.

Violations may result in network removal, access revocation, corrective action, and/or civil or criminal prosecution. Violators may be subject to disciplinary action up to and including dismissal or expulsion, pursuant to campus policies, collective bargaining agreements, codes of conduct, or other instruments governing the individual's relationship with the University. Third party vendors found to have violated this policy may incur financial liabilities, in addition to termination of contract.

Monitor and Measuring Controls

To measure the controls, CSU needs to develop good quality metrics for each one of them. Those good quality metrics will maintain the following characteristics:

- CSU monitoring and measuring control methods must be universal, which means the metrics can be applied regardless of the architecture, code, interface or system conditions. A metric is universal if it is composed of a clearly defined set of variables that can be used in any type of information security management system to which you want to apply the measurement.

- CSU methods must yield significant results with respect to the issue it seeks to measure. Hence the importance of defining a set of metrics that are useful to the assessment group to get what you really want to know, without elaboration and without the need for further information.

- Measurements of metrics must be accurate and represent what the Information Security Officers/ CSU really want and need to know. CSU ITS metrics should not divert attention to another aspect other than the purpose for which it was intended. Moreover, it should accurately portray the results, avoiding bias, both by the group responsible for the measurement and the decision makers. Obtaining results should be feasible, i.e., CSU ITS will foster in the culture of obtaining the data and variables involved in the measurement, so as to optimize resources and avoid waste of effort, time and money on measurements impossible perform.

- CSU monitoring and measuring control metrics must be reproducible, so that different people at different times can make the same measurement. It is vital the metric be consistently

repeatable, regardless of who made the measurement or the moment in time that the measurement takes place, provided that the conditions for measurement are preserved.

- CSU monitoring and measuring control methods must be objective, i.e. must not be tied to variable factors such as the knowledge of people, the ability to memorize, perception, among others, avoiding subjective factors that could skew or corrupt the results.

- CSU monitoring and measuring control methods must be impartial. A metric must be fair and equitable, must have a clearly defined set of values with which one can determine if the result is acceptable or not, and to know the level and/or the trending of attributes of the system.

CSU defines a measurement method with the following steps

- Complete list of the controls implemented in accordance with USO standard.
- Method for measurement of attributes associated with controls.
- Base measure for the control attributes.
- Generation of the indicator.

According to the result of the risk matrix, CSU ITS will select those controls that have the greatest ability to decrease the risk of exposure to the process information. The controls will consist of variables, which determine its level of functioning. Those variables are called attributes.

The attributes are proxies for control in risk exposure. The state of the attributes of control implies a specific level of risk, which is measured through a specific mechanism. Some of CSU ITS mechanisms are

- Questionnaires and personal interviews.
- Audit reports.
- Records of events.
- Risk Assessments
- Cybersecurity Program Reviews
- Behavioral Analytics FOR USER AND System Activities
- Log Audits
- Nessus Vulnerability Assessments
- Penetration Testing – External and Internal
- Application of Maturity Model Framework

CSU ITS' approach to the results of the implementation of the measuring mechanism is to control the attributes of the call-based measures. These measures when applied to the basic attributes of the same risk can be combined using techniques of weighted average, simple average, percentages, among

others. These combined measures are called derived measures and are the main input for the creation of indicators.

The indicators must express the current level of security compared to the desired security level, based on the level of residual risk accepted by the organizational processes. The goal of the indicator is to reflect the level of risk exposure by the current implementation status of a CSU control.

Conclusion:

A cyber-attack is hard for any University or business to recover from and having plans in place to help prevent and/or recover from a breach will make CSU less of a target, mitigate the risk of an attack, or lessen the impact of that attack.

Responding to a breach requires much forward planning. The elements in this Cyber Security Program Plan will assist all those responsible for dealing with the security situation of the University in knowing what to do, having the resources at hand to stop the attack, secure the network, and deal with any ramifications.

The Cyber Security Plan must adapt to the types of data protected and the circumstances involved. It requires cooperation and governance across all people, technologies, and processes in the CSU community.