LOUISIANA DELTA
COMMUNITY COLLEGE

POLICIES & PROCEDURES

Title: Information Security Policy
Document Number: IT_001
Effective Date: March 4, 2020
Revised Date: March 23, 2020
Department: Information Technology

Purpose

Louisiana Delta Community College is committed to defining and managing the information security requirements for maintaining data privacy and protection. This policy and the related documents set forth the information security practices for accessing, protecting, managing, storing, transmitting, sanitizing, and distributing data to ensure its availability, integrity, authenticity, non-repudiation and confidentiality.

This policy and the related documents are designed to clearly inform the applicable operational entities of their roles, responsibilities, and requirements, as this is critical to the overall success of the College's Information Security Program.

Scope

Entire College community.

Policy

The College's Information Technology Department has adopted the CAG (Consensus Audit Guidelines) 20 as defined by the Center for Internet Security (CIS). As defined by CIS, this process is a list of best practices that mitigate the most common attacks against systems and networks. Based on the guidelines of CIS the College has identified at implementation group 2 level.

Along with this policy, the College will create an information security plan that will define its approach to the twenty controls defined by CIS and their sub controls. As the plan for each control is fully executed it will move to this policy. These documents are intended to be working documents that will change as the College has the resources to implement the various controls.

Related Document

Information Security Plan

CIS Control 10: Data Recovery Capabilities

Critical College server data will be protected from deletion and corruption with backups to a separate device and location. This backup process will allow for multiple versions being stored on the backup data repository.

Purpose

When attackers compromise machines, they often make significant changes to configurations and software. Sometimes attackers also make subtle alterations of data stored on compromised machines, potentially jeopardizing organizational effectiveness with polluted information. When the attackers are discovered, it can be extremely difficult for organizations, without a trustworthy data recovery capability, to remove all aspects of the attacker's presence on the machine.

Sub Controls - Control 10: Data Recovery Capabilities

Sub Control	Control Title	Control Description	Impl Groups
10.1	Ensure Regular Automated Back Ups	Ensure that all system data is automatically backed up on regular basis.	1, 2, 3
10.2	Perform Complete System Backups	Ensure that each of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.	1, 2, 3
10.3	Test Data on Backup Media	Test data integrity on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.	1, 2
10.4	Protect Backups	Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.	1, 2, 3
10.5	Ensure Backups Have At least One Non-Continuously Addressable Destination	Ensure that all backups have at least one offline (i.e., not accessible via a network connection) backup destination.	1, 2, 3

CIS Control 17: Implement a Security Awareness and Training Program

The College utilizes an online service named KnowBe4 for continuous employee testing and training relative to security related risks and behaviors. All staff are required to complete their assigned training with completion reports being provided to leadership.

Purpose

It is tempting to think of cyber defense primarily as a technical challenge, but the actions of people also play a critical part in the success or failure of an enterprise. People fulfill important functions at every stage of system design, implementation, operation, use, and oversight. Examples include: system developers and programmers (who may not understand the opportunity to resolve root cause vulnerabilities early in the system life cycle); IT operations professionals (who may not recognize the security implications of IT artifacts and logs); end users (who may be susceptible to social engineering schemes such as phishing); security analysts (who struggle to keep up with an explosion of new information); and executives and system owners (who struggle to quantify the role that cybersecurity plays in overall operational/mission risk, and have no reasonable way to make relevant investment decisions).
Attackers are very conscious of these issues and use them to plan their exploitations by, for example: carefully crafting phishing messages that look like routine and expected traffic to an unwary user; exploiting the gaps or seams between policy and technology (e.g., policies that have no technical enforcement); working within the time window of patching or log review; using nominally non-security-critical systems as jump points or bots.

Sub Controls - Control 17: Implement a Security Awareness and Training Program

Sub Control	Control Title	Control Description	Impl Groups
17.1	Perform a Skills Gap Analysis	Perform a skills gap analysis to understand the skills and behaviors workforce members are not adhering to, using this information to build a baseline education roadmap.	2, 3
17.2	Deliver Training to Fill the Skills Gap	Deliver training to address the skills gap identified to positively impact workforce members' security behavior.	2, 3
17.3	Implement a Security Awareness Program	Create a security awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization. The organization's security awareness program should be communicated in a continuous and engaging manner.	1, 2, 3

Sub Controls(cont.) - Control 17: Implement a Security Awareness and Training Program

Sub Control	Control Title	Control Description	Impl Groups
17.4	Update Awareness Content Frequently	Ensure that the organization's security awareness program is updated frequently (at least annually) to address new technologies, threats, standards and business requirements.	2, 3
17.5	Train Workforce on Secure Authentication	Train workforce members on the importance of enabling and utilizing secure authentication.	1, 2, 3
17.6	Train Workforce on Identifying Social Engineering Attacks	Train the workforce on how to identify different forms of social engineering attacks, such as phishing, phone scams and impersonation calls.	1, 2, 3
17.7	Train Workforce on Sensitive Data Handling	Train workforce on how to identify and properly store, transfer, archive and destroy sensitive information.	1, 2, 3
17.8	Train Workforce on Causes of Unintentional Data Exposure	Train workforce members to be aware of causes for unintentional data exposures, such as losing their mobile devices or emailing the wrong person due to autocomplete in email.	1, 2, 3
17.9	Train Workforce Members on Identifying and Reporting Incidents	Train employees to be able to identify the most common indicators of an incident and be able to report such an incident.	1, 2, 3

Banner Access Procedures

Establishing/Modifying Banner Access

- Access to the Banner HR, Finance, Financial Aid, and Student Administration modules are granted to Louisiana Delta Community College employees and authorized affiliates who have an approved business need to work with or view data and reports.
- In order to obtain/modify access to any of the Banner systems, a Banner Security Form must be completed for the security classes within each Banner module (HR, Finance, Financial Aid, and Student Administration) that is required for the requestor to perform their duties. This form will route the request to the functional level approval.
- When approvals are complete, the request is routed to the security administrator for implementation.
- The user is notified of the completed security class actions to their account.

Removing Banner Access

- For standard terminations, access is removed by a process that is controlled by the termination date that Human Resources adds to the employee record in Banner. This daily process will look for employees that have active Banner security classes and termination dates equal to or less than the current date and if matches are found the process will drop the access.
- For non-typical terminations or employees that have broad based access to sensitive information; department heads, functional leads, executive members or human resources can request that the security administrator remove access immediately to prevent harm to the college.
- For active employees, if the employee's supervisor determines that an employee no longer needs Banner access, he/she must complete the Banner Security Form indicating "Delete" and this request will be routed to the Banner Security Administrator.
- The Banner Security Administrator or the termination process, upon receipt of notification or if the process determines actions need to be taken,
    - Removes the appropriate security classes from the users account.
    - Removes Self Service Access from the applicable FOMPROF record
    - Deletes the GOAEACC record
    - Removes all manually added Luminis Roles (COGNOS, Admin, Etc.)
    - Removes all AD security groups except the Domain Users group
- The security administrator regularly monitors payroll termination reports in Banner. If an employee is noted as terminated and the security administrator has not received a notice to otherwise retain the account, the security administrator will inactivate the security classes from that user account.

Internal Access Auditing

The security administrator will send quarterly reports to the functional level approvers or directors. The approvers or directors will then verify that the appropriate access is assigned for their respective areas. If changes need to be made they will initiate the relevant procedures defined above.