Developing a Security Policy for a Campus Network

CSC 302-01: Computer Security

Dr. Liu Cui

Almaraz Alejandro, Sean Berlin, Rebecca Bourne

December 12th, 2023

1. Introduction

This security policy is being offered to assist with protecting the campus' physical and information technology (IT) assets and settings. The campus is divided into three sections: Academics, Management, and IT, and the campus network supports both wireless and wired connection.

This security policy is guided by the three major general security principles: confidentiality, integrity, and availability. Confidentiality is the avoidance of the unauthorized disclosure of information - or in other words, providing access only to those with authorization and preventing others from learning about protected information. Integrity is the assurance that information has not been altered unauthorized and is accurate and reliable, and availability is the concept that information is easily accessible and modifiable by people with the authority to do so.

To keep up the standards of good security, routine audits should be conducted to assess compliance with security policy. It is integral this security policy must also be routinely reviewed as security, security concerns, and campus change over time. This policy is a living document requiring regular reviews and undergoing inevitable relevant changes as the policy adapts to current cybersecurity concerns.

2. Academics

2.1 Introduction:

The Academics section comprises six colleges/schools, each hosting servers accessible within the campus or remotely through the IT department. The colleges include the College of Arts and Humanities, College of Health Sciences, College of Business and Public Management, College of the Sciences and Mathematics, College of Education and Social Work, and Wells

School of Music. This section outlines the security measures and practices to be implemented within academic institutions to safeguard the confidentiality, integrity, and availability of sensitive information.

2.2 Information Access:

As custodians of academic data, each college must uphold the principles of least privilege and role-based access control to restrict information access to authorized personnel only. Different roles, such as "Student," "Faculty," and "Administrator," should be defined, each with specific access rights based on their responsibilities within each specific college/school. To reiterate, a key distinction for this section is the unique access paths for each college. Recognizing the distinct needs of each college, specific access paths will be established. These tailored access routes will be designed to meet the specific requirements of each academic unit while adhering to overarching security policies. Additionally, regular reviews should be conducted to ensure that unnecessary accounts and privileges are promptly revoked.

2.3 Authentication and Authorization:

Access to academic servers and information must be authenticated through robust means, including passwords and multi-factor authentication. Multi-factor authentication adds an extra layer of security by requiring users to provide additional proof of their identity, such as a code sent to their mobile device or email. Password policies, including maximum age, length, and complexity requirements, must be enforced to enhance the overall security of authentication. For remote access, individuals are required to connect through the IT department, which serves as an intermediary for secure connections to department servers. Access permissions will be granted based on the unique requirements of each academic unit, ensuring that sensitive data remains protected during remote connections and follows established security protocols.

2.4 Data Integrity:

Ensuring the precision and dependability of academic information within the Academic department is of utmost importance. Any alterations or updates to data, encompassing grades and student records, will be meticulously documented and logged. To safeguard against potential disruptions, comprehensive backups and archiving procedures will be instituted, guaranteeing the ability to recover data in the face of system failures, data loss, or corruption. Periodic checks and audits specific to the Academic department will be conducted to systematically verify and fortify the integrity of stored academic data. This proactive approach not only safeguards against inadvertent errors but also ensures a resilient and reliable academic data infrastructure.

2.5 Faculty and Student Training:

Faculty and students within academic institutions should undergo mandatory security awareness training regularly. Training modules should cover a range of topics, including recognizing and mitigating common cyber threats, safeguarding sensitive data, and reporting security incidents promptly. This proactive approach helps build a resilient community that is vigilant against potential security risks.

2.6 Physical Security:

Physical security measures must be implemented within academic institutions to control access to sensitive resources. Areas housing servers and networking equipment should be physically secure, and access should be restricted to authorized personnel only. For added security, sensitive physical documents should be stored in secure locations, such as safes, and access to these locations should be limited and monitored.

2.7 Server and Database Security:

The servers and databases within each academic institution should undergo regular security assessments, including system hardening, updates, and patch installations. The attack surface of these systems should be minimized by removing unnecessary programs and functions. Encryption should be applied to data during transmission and storage to protect it from unauthorized access. Compliance with privacy laws and regulations is crucial, especially when handling sensitive academic information.

By adhering to these guidelines, the Academics section aims to establish a secure environment that promotes the confidentiality, integrity, and availability of academic data within the campus network. Regular assessments and updates should be conducted to adapt to evolving security concerns and technologies

3. Management

3.1 Introduction:

The Management of the campus has three offices: the Provost office, the Registrar office, and the Billing office. The Provost's office has all the forms needed by students, employees, and faculty members, the Registrar's office has servers storing academic information such as the students' registered classes, grades, and degree progress reports, and the Billing office stores the students' contact and billing information. The following sections in section 3 give a general overview of steps each office must take to uphold the security concepts of confidentiality, integrity, and availability.

3.2 Information Access

Because the three management offices have information-management responsibilities, upholding confidentiality by restricting information access to authorized personnel only is vital to ensuring security. To accomplish this an access control policy the principle of least privilege must be used where information access and modification rights are granted on a “need to know/use” basis. The access control policy should be role-based and the number of roles and their permissions based on the different positions at each office. Different roles may include a “Student” role given to students with the ability to access and modify their information, a “Worker” role given to office employees with the ability to access and modify information, and an “Admin” role with the ability to access and modify information as well as alter the access abilities of those with the “Worker” and “Student” roles. Unnecessary and unused accounts and privileges should be removed.

3.3 Authentication and Authentication

Not only must access to information be granted based on the access control policy, but the identity and role of those attempting to access information must be correctly and securely determined so that access is granted to the right persons and roles. The identity or role of a person can be determined in each of the offices through passwords and multi-factor authentication. To enforce multi-factor authentication along with a password, users must be tested on something they know (such as a PIN), something they have (such as a badge or phone), and/or something they are (such as fingerprints or vocal recognition) to access information. For this security policy, the method of having a code sent to a phone or email that must be entered may be used.

A proper password policy is required to maintain the security of passwords. A maximum password age and length policy as well as complexity requirements enforced to ensure

passwords are changed on a routine basis and are themselves complex enough to defer password attacks. Likewise, this password information should be properly stored and encrypted in the servers. Users should receive email notifications to remind them to change their password.

3.4 Data Integrity

To ensure the accuracy and reliability of information, any changes to information such as grades and student records and information should be documented and logged. Logs can be used in determining performance, solving bugs, and spotting and analyzing attacks. Logging both the actions performed on the information itself as well as the account performing said action also ensures accountability, where every action can be traced to the account. In the servers and databases used by the offices, regular backups and archiving should be done so that data may be recovered in the case of system failures, data loss, or data corruption and the integrity of stored data must be regularly verified through routine checks and audits.

3.5 Employee Training

Employees and students must undergo regular mandatory security awareness training to remain educated on security best practices and threats as many types of security attacks exploit the vulnerability of humor error, such as phishing attacks. These modules should cover a variety of topics such as common cyber-attacks, social networking attacks, how to create a good password, how to spot cyber attacks, and what to do in the event of one.

Security awareness training should cover present and emerging cybersecurity topics and best practices. To provide hands-on training, simulating phishing exercises can be used to educate employees but also gauge employee’s susceptibility to phishing and other social engineering attacks and ways the security training can improve. Employees should also be educated to immediately report any suspicious activities or security attacks.

3.6 Physical Security

Physical barriers to limit access to protected resources should be implemented in the physical location of each office. Physical spaces containing servers and other devices should be built and maintained in a way that the devices are not vulnerable to both attacks from people (break-ins, robberies, keyloggers, etc.) and attacks from nature (floods, heat, cold, etc.). For example, spaces containing particularly sensitive information could require key-card access. If any personal information is held in a physical state, such as on paper, it must be stored in a secure location such as a safe.

3.7 Server and Database Security

It is important that the servers and databases used by the offices to store information are properly secured. System hardening should be conducted and the server routinely updated and patches installed to fix security vulnerabilities and bugs as well as improve its performance and usability. The attack surface of the system should be minimized as much as possible with superfluous programs, functions, applications, roles, etc. removed to lessen the opportunity of an attacker breaching the system via one of their vulnerabilities. The attack surface can be further minimized by encrypting passwords and other credentials, patching software and firmware vulnerabilities, and having proper network security.

Information should be encrypted during transmission (at transit) and in storage (at rest) using secure encryption algorithms to ensure that even if data is intercepted, it remains unreadable. In the billing office, communicating and verifying billing details should also be over secure channels and financial information confidential.

Because of the presence of billing and contact information, the management of this information and billing practices should comply with privacy laws and regulations. In an era

where private information is frequently under attack, this security policy acknowledges the importance of complying with laws and legal privacy regulations. This security policy should be routinely updated not just to keep up-to-date with the current cybersecurity environment but to also keep up-to-date with present-day laws.

4. IT Department

4.1 Introduction

The IT department oversees a multifaceted infrastructure comprising servers dedicated to Remote Access authentication, enabling student access to the registrar, billing, and department servers. In addition to managing these servers, the department is responsible for the entire array of network devices, including routers, Wi-Fi access points, and switches. That being said, the security policies will address critical aspects of information security, spanning access controls, network protection, endpoint security, data encryption, incident response, and patch management. The overarching goal is to establish a robust security posture that protects sensitive data, prevents unauthorized access, and enables swift and effective responses to potential cyber threats. Each policy contributes to a layered defense strategy, emphasizing proactive measures such as access restrictions, encryption protocols, and regular updates.

4.2 Access Control

The Access Control Policy establishes guidelines for managing and restricting user access to critical systems and data. By implementing role-based access controls, the policy ensures that employees only have the necessary permissions for their specific roles, minimizing the risk of unauthorized access and data breaches.

4.3 Network Security

The Network Security Policy is designed to protect the organization's digital infrastructure from unauthorized access and potential threats. It encompasses measures such as firewalls to monitor and control network traffic, encryption for secure data transmission, and intrusion detection systems to identify and respond to suspicious activities. This policy forms a robust defense mechanism against cyber threats, safeguarding the integrity and confidentiality of data flowing through the organization's network.

4.4 Endpoint Security

The Endpoint Security Policy is focused on securing individual devices within the organization, including servers, routers, and switches. It emphasizes the importance of keeping these devices up-to-date with the latest security patches and firmware updates. The policy also promotes the use of antivirus software and endpoint protection measures to defend against malware and unauthorized access.

4.5 Data Encryption

The Data Encryption Policy addresses the critical need to protect sensitive information both during transmission and storage. By implementing encryption protocols, particularly for remote access and critical transactions, the policy ensures that data remains confidential and secure. This extends to encrypting stored data on servers housing sensitive information, providing a comprehensive approach to data protection and reducing the risk of data breaches. For example, the use of hash values and salt so it can effectively handle a broad range of cyber threats.

4.6 Incident Response and Reporting

The Incident Response and Reporting Policy is a strategic guide for effectively handling and mitigating cybersecurity incidents. It establishes clear procedures for identifying, reporting,

and responding to incidents promptly. This policy emphasizes the importance of regular training and drills for IT staff to ensure a well-prepared response team capable of managing incidents efficiently.

4.7 Patch Management

The Patch Management Policy is a proactive approach to maintaining the security and stability of the organization's IT infrastructure. It outlines processes for regularly updating devices with the latest security patches and firmware. By prioritizing vulnerabilities based on risk and conducting thorough testing before deployment.

5. Conclusion

This contained security policy offers the guidance needed to safeguard the campus' physical and information technology assets and covers the three main areas of campus: academics, management, and the IT department. Guided by the three major security principles of confidentiality, integrity, and availability and recognizing the importance of authorization to access necessary resources, this robust framework creates a secure environment protecting the sensitive information of students.

In conclusion, this comprehensive security policy stands as a vigilant guardian over the campus' physical and information technology assets across its academic, management, and IT realms. Governed by the steadfast principles of confidentiality, integrity, and availability, the framework has been meticulously crafted to foster a secure environment. Recognizing the critical role of authorization in accessing essential resources, this policy not only fortifies the defense mechanisms against potential cyber threats but also ensures the safeguarding of sensitive student information. As the technological landscape and security concerns evolve, this living document

remains adaptable, and poised to undergo routine audits and reviews, thereby sustaining its effectiveness in an ever-changing campus ecosystem.