COMPLETELY REVISED to go with Revised Policy 1090

Procedure

1090.1

SCHOOLCRAFT COLLEGE

18600 Haggerty Road, Livonia, Michigan 48152-2696

INFORMATION SECURITY PROCEDURES

Table of Contents

Compliance Requirements regarding information classification, security, roles, access, use, compliance, and enforcement

(Refer questions and comments to the office of the CIO)

9/19/18

Information Security Procedures

Introduction

Information Security is the process of protecting three domains of information. The first one involves protecting the confidentiality of data; here we keep the data out of the hands of those who should not have it, ensuring privacy. The second domain revolves around protecting the integrity of that data. It is important that what we enter is accurate and remains accurate throughout its lifespan. In essence, we are ensuring the data’s quality. The final domain revolves around availability; here we strive to make sure the data is always available when it is needed. Therefore, the goal of information security is to provide accurate information to only those who are authorized to have it, when they need it.

Purpose

The College is committed to protecting information assets and the information resources that support our organization. The College collects, transmits, stores, and processes a large volume of data in its mission to educate students. Our Security Compliance Requirements are a collection of controls and security measures that protect our information assets. Without these protections in place our assets and system would be subject to possible damage, exposure and theft.

Scope

This Compliance Requirement covers all information assets owned or leased by Schoolcraft College, regardless of their location.

Information Assets

Information assets are any electronic device owned by Schoolcraft College that has the capability to electronically store, process, or transmit information. This includes, but is not limited to computers, laptops, servers, SANS (Storage Area Networks), Storage, Backup & Archive tablets, smartphones, network communication devices, and internet access. It also includes the data that is contained within these systems, such as imaged documents, student information, employee information, and budgetary information. Information includes data stored on removable or portable media, data stored in computer memory, or Schoolcraft College intellectual property stored on personal devices.

Information assets are also any information that is physically present on the campus grounds or at an authorized storage facility. This can include student forms, sign off sheets, and construction documents.

Roles and Responsibilities

- CEO / President – Overseers all college activities.

- Board of Trustees – Provides formal "authorization" of all College Policies.
- Cabinet – College Executive Leadership Team approves prior to being heard by the Board of Trustees for authorization.
- VP & CIO – Oversees the College Information Technology systems and the information contained on them.
- Executive Sponsors – Senior officials who have Compliance Requirement-level responsibility and accountability for data, including its creation and maintenance of this data, within their appropriate functional area.
- Data Stewards – Responsible for initial classification of data maintaining the integrity of the data and carrying out the data policies.
- Data Custodian – Person, automated application, or process that oversees the safe transport and storage of data.
- Data Classification Committee – Oversees the final classification of data types.
- Data Users – Individual who use the data to perform business operations.
- Controller – Oversees financial services.
- Director of Risk Management – Oversees the College's overall risk concerns.
- Executive Director of Information Security and Networking – Responsible for the leadership in all areas of Information Security and network infrastructure.
- Executive Director of Server Administration & Business Continuity – Responsible for all server and storage as well as backup, archive, business continuity and disaster recovery.
- Director of Technology Support – Responsible for the leadership of IT end user systems both physical and virtual.
- Executive Director of Academic and Administrative Systems – Responsible for the leadership of enterprise wide applications and database systems.
- Vendors – Considered acting as employees of the department who are responsible for the information.

Compliance Regulations

- Schoolcraft College policies are designed to meet the requirements set forth by Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99). This is a Federal law that protects the privacy of student education records. By extension the Federal Trade Commission has ruled colleges that are FERPA compliant, meet the requirements for Gramm-Leach-Bliley Act (GLBA) which requires institutions protect customer financial information.
- Schoolcraft College must also comply with the Payment Card Industry Data Security Standards (PCI DSS).
- Schoolcraft College must also comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996) and its amendments

Reporting Violations

- All employees are expected to report violations of this Policy and its procedures to their supervisor.
- Supervisors are expected to report Compliance Requirement violations of employees to Human Resources. Human Resources will notify Information Security and Campus Police Department as College Policy dictates.
- Supervisors and Instructors are expected to report Compliance Requirement violations of students using the SCAWARE incident response portal at the following url: (http://www.schoolcraft.edu/scaware/sc-aware) and the standard SCAWARE process as prescribed by policy and procedure will be executed.
- Vendors who do business with Schoolcraft College and active students are obligated to report known violations using the SCAWARE incident response web portal as described above.

Compliance Requirement Enforcement

Who provides Enforcement?

- Human Resources – Responsible for employee Compliance Requirement enforcement and disciplinary actions.
- Student Disciplinary Committee – Responsible for student Compliance Requirement enforcement and disciplinary actions.
- Campus Police Department plays an active role in the enforcement of policies and procedures if:
  - They are asked to participate by either governing body.
  - Compliance Requirement violation involves hostile action.
  - Compliance Requirement violation involves illegal activity.
  - Campus Police Department are the first responders.
  - Legal department and Risk Management, if Compliance Requirement violation involves third-party vendor.

Potential disciplinary action can include, but not limited to:

- Employees
  - Employee's requirement to re-certify understanding of Compliance Requirement.
  - Formal warning or write up in permanent record.
  - Suspension.
  - Termination.
- Students
  - Compliance Requirement review with Advisors.
  - Formal warning or write up in permanent record.
  - Semester expulsion.
  - Permanent expulsion.

- Vendors
  - Formal warning.
  - Monetary penalties (per contract terms).
  - Termination of contract (per contract terms).
  - Legal action

Exceptions

- Any exception to this procedure must be approved by the Information Security Team, CIO or in advance.

Authority and Authorization

Schoolcraft College Board of Trustees on the recommendation of the President and Executive Leadership Team authorizes this Information Security Procedure.

Compliance Requirements

Acceptable Use Compliance Requirement (AUCR)

Introduction

Schoolcraft College's Acceptable Use of Information Technology Resources Compliance Requirement (AUCR) provides for access to information technology (IT) resources that are intended to carry out the legitimate operational functions of the College. Use of these resources is not intended for non-college related purposes. In addition, Schoolcraft College is committed to protecting itself, students, and employees from inappropriate, illegal, or damaging actions by individuals using these systems.

Purpose

This Compliance Requirement is to define the acceptable use of college information, and the systems which process this information, and the network at Schoolcraft College. These rules are in place ensuring that members of the Schoolcraft College have access to reliable systems that safely guard confidential information.

The rules will also guide students and employees to use good practices to protect the College. An individual's unsecure practices and malicious acts can expose Schoolcraft College, students, and employees to risks that can compromise their system or the network resulting in the loss of data, loss of confidential information, or loss of services. Security breaches could affect students, employees, and damage the College's reputation. Legal action for individuals or the College may result from a data breach.

Scope

The AUCR applies to anyone who uses the College's information technology (IT) systems, network or information including, but not limited to students, employees, College Board members, contractors, conference guests, third party vendors, or any individuals or entities who use these systems at Schoolcraft College.

This Compliance Requirement applies to all IT resources owned or used by Schoolcraft College including, but limited to computer equipment, software, operating systems, network, and the Internet access. It also includes any media that is used to transport information.

Securing and protecting these resources are the responsibility of everyone who uses them; security is only as strong as its weakest link. There is a significant cost associated with the protection of information assets and the integrity of systems use on a global scale; everyone is expected to participate in securing our organization.

Procedure

Unless otherwise specified in this procedure or other college policies, use of college information technology resources is restricted to purposes related to the College's mission. Eligible individuals are provided access in order to support their studies, instruction, duties as employees, or business with the College. Unless specifically identified as an authorized user to the system, access to IT systems is forbidden.

Departments may develop complementary use policies and procedures, as long as they are consistent with this Compliance Requirement and any other applicable technology use policies of the College.

Incidental personal use of IT systems must adhere to all applicable college policies.

Unacceptable Use

- Users are prohibited from engaging in any activity that is illegal under local, state, federal, and international law or in violation of college Policy and or Compliance Requirement. The items listed below are by no means the only areas of restriction; items listed are only an attempt to provide a framework for activities that fall into the category of unacceptable use.
- While respecting users' confidentiality and privacy, the College reserves the right to access and examine all computer files, email content and history, internet access history, network access and usage.
- Use of unauthorized devices where public network connections are not available is prohibited.
- Priority for the use of IT resources is given to activities related to the College's missions of education, and conferencing facilities.

Unacceptable Activities

Participation or assisting in any form of security breaches or malicious use of network communication including, but not limited to:

- Procurement of configuration information about the network or system on the network for which the user does not have the responsibility to maintain.
- Participation or assisting in activities intended to hide the user's identity, to purposefully increase network traffic, or other activities that purposefully endanger or create nuisance traffic for the network or systems attached to the network.
- Circumventing any authentication mechanism, including electronic or physical barriers to access data, accounts, or systems that the user is not expressly authorized to access.
- Implementation of a Denial Of Service (DOS) for any Information Technology system, or its users on the College's network. This includes using college facilities or networks to interfere with or deny service to persons outside the College.

Unauthorized Use of Intellectual Property

- Use of college IT systems or networks to violate the ethical and legal rights of any person or company protected by copyright, patent, intellectual property rights, or similar laws or regulations is prohibited.

- Participation or assisting with the unauthorized use, duplication, distribution, or publication of copyrighted material, unless it meets the requirements of the fair use doctrine. This includes but is not limited to, use of copyrighted images, music, video, or programing code.
- Unauthorized use of any licensed trademarks of Schoolcraft College or any other organization.
- Theft of, or unauthorized removal of Schoolcraft College intellectual or physical property in any format is prohibited. This includes but is not limited to information, equipment, or documents.
- Using any IT Systems or network resources to engage in academic dishonesty, plagiarizing, altering, or tampering with the work of others is prohibited.

Misuse of Electronic Communications

Email and other electronic communications are required to carrying out the activities of the College, its employees, and students. Electronic communications include but are not limited to email, social media, texting, instant messaging or any other form of communication transmitted over the network or Internet.

- Both employees and students are reminded that, legally, email is treated like any other form of written communication. Messages are subject to the same legal restrictions and potential liabilities as those of paper documents. This could include the Patriot Act and other state and federal laws. Email messages may be subpoenaed and are subject to the Freedom of Information Act (FOIA) or discovery requests.
- Use of the email systems for personal gain, conducting of private business, or furthermost of political agendas is prohibited.
- Sending unsolicited messages, including "junk mail" or other advertising material to individuals who did not specifically request such material, except as approved under the email usage Compliance Requirement is prohibited.
- Harassment of any person or organization by means of electronic communications whether through content or frequency of the messages is prohibited.
- Use of one’s electronic address (email addresses); electronic signature or electronic identity with the intent to send or receive unauthorized information or unauthorized response is prohibited.
- Use of anyone’s electronic address (email addresses); electronic signature or electronic identity that the user is not explicitly authorized to use, is prohibited for any reason. (This includes use by former employees, retirees (including those with Emeritus or Honoree status), students, faculty, individuals, etc. – any person whose active relationship with the College has ended or been terminated at the sole discretion of Schoolcraft College.)

Inappropriate or Vindictive Use of IT Systems or Internet

This is the use of any IT systems for an intent other than to conduct normal business operations, or in the course of student learning as part of the normal curriculum. The following actions are prohibited.

- IT systems or network must not be used for the harassment of persons or organizations, encouragement of workplace hostility, or other illegal activity. This applies to systems used either on or off the campus for any reason.
- Intentionally sending or receiving material of a profane, pornographic, hate or threatening nature.
- Setting up any form of peer-sharing system in which information may be shared without the College's knowledge including protected information or other intellectual property that can be illegally shared.
- Sabotage, misuse, or abuse of IT systems, including intentionally introducing malicious programs into the IT systems or network (e.g., viruses, worms, Trojan horses, adware/malware, etc.).
- Any attempt to access, information or systems that one is not authorized to access is prohibited including the sharing of authorized information, account privileges and system access with anyone or any organization that is not authorized to have this information.
- Any attempt to adversely modify, alter or subvert any security or operating configurations of any IT systems or network resource by authorized or unauthorized parties is prohibited.
- Any inappropriate use or sharing of authorized IT privileges or resources.

Data Classification Compliance Requirement

Introduction

The Schoolcraft College Data Classification Compliance Requirement (DCCR) provides the College with a method to categorize the information collected, stored, and managed by the College community. Using the data classification method will improve the ability of the College employees to manage access to college information in compliance with federal, state, regulatory, and Compliance Requirements.

Scope

The DCP applies to anyone who has access to the College's electronic and physical data used by the organization for the purpose of carrying out the College's mission. This including but not limited to students, employees, College Board members contractors, conference guests, third party vendors, or any individuals or entities that use these Schoolcraft College systems.

This Compliance Requirement applies to all IT resources owned or used by Schoolcraft College including but limited to, computer equipment, software, operating systems, network, and the Internet access. It also includes any media that is used to transport information.

Securing and protecting these resource is the responsibility of everyone who uses them. There is a significant cost associated with the protection of information assets and the integrity of systems use on a global scale; so, everyone is expected to participate in securing our organization.

Schoolcraft College data stored on college or non-college resources must be verifiably protected according to the Minimum-Security Standards and Guidance.

Compliance Requirement

Data stewards are responsible for the data's integrity and; therefore, must classify information according to the impact resulting from unauthorized exposure as defined by the information classification categories. Data stewards will report classification decisions to the Data Classification committee for verification of proper classification of a new data type.

Custodians and users must inform data stewards of any new type of data that requires classification. Stewards, custodians, and users shall be held responsible for ensuring data is protected according to the classification assigned. Data classifications are to be documented by the Data Steward and reported to the Data Classification committee. Information Security will maintain a global list of data classifications.

Classification

- Data shall be initially identified with a classification level proposed by the data stewards. The Data Classification committee shall review the proposal for final determination. Before data is made available.
- Any employee, contractor or student information that is Personally Identifiable Information (PII), Protected Healthcare Information (PHI), or Financial Aid information shall be classified as **Confidential**.
- Directory information which is information that is generally not considered harmful or an invasion of privacy if released is exempt from this level of classification.
- PII for which disclosure to persons outside of the College is governed by FERPA regulations.
- PHI for which disclosure to persons outside of the College is governed HIPPA regulations.
- Data shall be classified as Confidential, Internal use, General, or Public

  Confidential information:

  - Information whose unauthorized exposure, use, access, disclosure, modification, loss, or deletion could result in severe damage to Schoolcraft College, its students, employees, or customers, as determined by committee and/or governing law. Financial loss, damage to the Schoolcraft's reputation, and legal action could occur.
  - Access to this information is granted only to those users who must use the data to perform their job duties.
  - Access to this information must be logged so that data users, stewards, and custodians who access, update or alter the information are identified along with the time this happened.

- Disclosure of this information to anyone not authorized by the College, requested via proper legal means (e.g., FOIA), or subpoenaed is prohibited.
- Storage of this information is to be encrypted using keys lengths of sufficient size to comply with industry standards.
- Transmission of this information is to be encrypted using keys lengths of sufficient size to comply with industry standards. The latest web encryption standards are to be used for transmission across the internet.
- Minimum encryption standards for this information shall be defined by the Information Security office and are subject to periodic review and updating.
- This information is not to be removed from the College or its systems. Storage of this information on personal equipment is prohibited.

Internal use information:

- Information intended solely for use within the Schoolcraft College and limited to those who need to know it.
- Access to this information is granted only to those users who must use the data to perform their job duties.
- Disclosure of this information to anyone not authorized by the College or subpoenaed is prohibited
- Storage of this information should be encrypted using keys lengths of sufficient size to comply with industry standards.
- Transmission of this information can be encrypted the latest web encryption standards are to be used for transmission across the internet.
- Storage of this information on personal equipment is to be encrypted using keys lengths of sufficient size to comply with industry standards.

General information:

- Access to this information is granted to any employees who must use the data to perform their job duties.
- Disclosure of this information is at the discretion of the employee.
- Storage of this information should be restricted from the public.
- Transmission of this information requires no special precautions.
- Storage of this information on personal equipment is permissible but not recommended.

Public information:

- No special precautions need to be taken for access, as the public can access the information.
- Review should be performed before intentionally exposing to public for appropriateness.
- Storage of this information on personal equipment is permissible.

Examples include but are not limited to:

Confidential information (especially when paired to a name).

- Social Security number or Tax ID.
- Credit card numbers.
- Bank account or debit card information
- Passwords, PIN numbers, Biometric information, or other credentials that grant access to systems.
- Birth date with last four digits of Social Security number. Driver's license number, state ID card, or other forms of national or international identification numbers.
- Healthcare information.
- Criminal background check or law enforcement personnel records.

Internal use information:

- Student contact information including birth date, and photo.
- Schedule or curriculum information.
- Test Scores and grades.
- College intellectual property other than curriculum.
- Security information related to a data or system.
- Employee contact information and employment status.
- Race and ethnicity.
- Names of family members.
- Verification information such as Birthplace, Mother's maiden name, or gender.
- Marital Status.

General

- Facility plans, or contractor selection.
- Student processing procedures.
- Internal communications, not containing confidential or internal use information.
- Curriculum design work.
- Internal enrollment reports.

Public

- Website marketing information
- External enrollment reporting
- Cleary Act reporting information.

Risk Assessment Compliance Requirement

Introduction

Schoolcraft College's Risk Assessment Compliance Requirement which is part of the Information Security Policy (RACR) provides the College with a method and schedule to review risk to information across the organization.

Purpose

This Compliance Requirement is to empower the Information Security department of Schoolcraft College to perform periodic information security risk assessments of all the College's systems both electronic and physical, for determining areas of vulnerability that could compromise the College's information confidentiality, integrity and its availability. It will also allow for the appropriate remediation of the discovered vulnerabilities, and ensure the remediation is performed to completion. This Compliance Requirement will also ensure that departments understand their role in mitigating risk of compromise of Schoolcraft College's data as categorized.

Scope

The RAP applies to all college departments and its employees, who access, manipulate, manage, or otherwise use college IT systems, or access college information. Risk Assessments (RAs) can be conducted on any IT systems within the organization or those systems that have been outsourced to alternate facilities or third-party vendors. RAs can be conducted on any IT system, to include applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained. Processes and tools are used to do this, and include but are not limited to: Qualsys® Vulnerability Analysis scans, Cisco® Firepower™ IPS (Intrusion Prevention System), LogRythm® SIEM tool (Security Information Event Management), ForcePoint® DLP (Data Loss Prevention System), etc.

Securing and protecting these resource is the responsibility of everyone who uses them. There is a significant cost associated with the protection of information assets and the integrity of systems use on a global scale; so everyone is expected to participate in securing our organization.

Compliance Requirement

Unless otherwise specified in this Compliance Requirement or other Schoolcraft College policies, use of college information technology resources is restricted to purposes related to the College's mission. Eligible individuals are provided access in order to support their studies, instruction, duties as employees, or business with the College. Unless specifically identified as an authorized user to the system, access to IT systems is forbidden. Departments may develop complementary use policies and procedures, as long as they are consistent with this Compliance Requirement and any other applicable technology use policies of the College.

Roles

- Executive Director of Information Security and Networking - Responsible for the leadership in all areas of Information Security and network infrastructure.
- Executive Director of Server Administration & Business Continuity – Responsible for all server and storage as well as backup, archive, business continuity and disaster recovery.
- Director of Technology Support – Responsible for the leadership of IT end user systems both physical and virtual.
- Executive Director of Enterprise Applications - Responsible for the leadership of enterprise wide applications.
- Information Security Risk Assessment Team - Responsible for performing the risk assessment. It is comprised of members of the Information Security team, the Information Technology team, and the Enterprise Applications team. Members are selected at the discretion of the Executive Director of Information Security, in coordination with the Executive Director of Server Administration & Business Continuity, with approval by the VP & CIO.
- Department teams will include members who are responsible for the data being reviewed. To ensure proper resources are allocated, these members will be selected by the Information Security Risk Assessment team, in coordination with area supervisors, and with selection approval by the VP & CIO and appropriate Cabinet member.

Outsourcing Contracts

Contracts for systems that will be maintained at a vendor’s site should be written in a manner, which will allow the Information Security Risk Assessment team to perform standard risk assessments independent of the entity housing theses system. This includes latitude in when these tests are to be performed. For the purposes of outsourced systems, containing college information, they will be treated no differently than data that resides on the College’s equipment.

Compliance Requirement Execution

The execution, development and implementation of remediation programs are the joint responsibility of Information Security and the department responsible for the systems that is being assessed. Departments and their employees are expected to cooperate fully with any risk assessment being conducted on systems for which they are held accountable. Allocation of resources includes but is not limited to informational interviews, information discovery, and process discovery and/or documentation creation. Employees are further expected to work with the Information Security Risk Assessment Team in the development and execution of a remediation plan. Automated means of monitoring and analysis access to, and use of, data will include but is not limited to the technological systems mentioned previously including anti-virus.

Periodic risk assessments will be performed on all systems. The more critical systems will require full risk assessments to be performed on an annual basis. Partial risk assessments are to be performed when configuration changes are made to these systems. Partial risk assessments can be the result of vulnerability assessments, penetration tests, network monitoring, security information event monitoring (SEIM), Data Loss Prevention (DLP), Intrusion Prevention Systems (IPS), etc.

The full risk assessment is to follow the National Institute of Standards and Technology's (NIST) risk assessment framework Identified in the special publications (SP) 800 series.

(NOTE: All NIST Special Publication documents (e.g., SP800-53) can be found at the following location - https://csrc.nist.gov/publications/sp800)

This framework will include the following requirements:

Categorize Information Systems

- Identify the different systems and categories into criticality and sensitivity of the information and define potential impact of the loss. SP800-60

Impact examples:

	Low	**Moderate**	**High**
Confidentiality	Disclosure of course enrolment information before it is made public.	Disclosure of e-mails identifying private college finical information.	Disclosure of student social security number or an administrative password.
Integrity	Defacement of the ski clubs web site.	Unauthorized modification of course schedules, causing student confusion.	Unauthorized modification of state reports, that are used to identify State funding causing embarrassment for the College
Availability	Denial of service attacks on primary website during non-peak hours.	Attack on the registration or payment gateway during priority registration weekends.	Attack on the network core devices paralyzing the network and its systems.
Authorized Use	A student shares his/her password with significant other to allow them to use our IT services.	Gaining unauthorized access to a computer and then using the computer to capture unencrypted packet information on the network.	Gaining unauthorized access to a computer and then using the computer to attack the Enterprise Resource Planning system (ERP).

- Select baseline security controls that should protect these systems under the guidance of SP800-53. The security control baselines control matrix is used to determine the gaps in controls.

  (NOTE: All NIST Special Publication documents (e.g., SP800-53) can be found at the following location - https://csrc.nist.gov/publications/sp800)

  Examples include but not limited to:

  - AC-6 Least Privilege
  - AU-1 Audit and Accountability Policy and Procedures
  - CM-3 Configuration Change Control
  - IA-5 Authenticator Management
  - PE-10 Emergency Shutoff

- Use the risk assessment results comparison using both SP800-30 and 53 to supplement the necessary security control baseline as needed to ensure adequate security and due diligence.
- Under guidance of SP800-18 the security plan must be document. This includes the security requirements for the information system and the security controls in place, and those that will be added.
- Implement security controls; apply security configuration settings using the guidance of checklists found in SP800-70
- Measure the new security control's effectiveness. Determine if the control was implemented correctly, operating as intended, meeting security requirements. Under the guidance of SP800-53A
- Any remaining risk will be reported to the VP & CIO and the appropriate area Vice President. If remaining risk is deemed is acceptable, the Executive Director of Information Security will authorize information system operation under guidance of SP200-37.
- Continuously track changes to the information system that may affect security controls and reassess control effectiveness as changes occur.

Purchasing Card Industry (PCI) Compliance Requirement

Introduction

The Payment Card Industry Data Security Standards (PCI DSS), is a set of requirements for payment account data security. PCI DSS was developed by the PCI Security Standards Council for managing the security standards. Compliance with the PCI set of standards is enforced by the founding members who include American Express, Discover, Japan Credit Bureau, MasterCard and Visa Inc.

Purpose

PCI DSS includes controls for security management including the requirement for policies and procedures to prevent credit card fraud, or exposure. The standards apply to all organizations that store, process or transmit cardholder information. The policies and procedures are to comply with the requirements of the purchasing card industry. Failure to do so could mean that credit card agencies will refuse to do business with Schoolcraft College, or the College may face legal action if credit card fraud were to occur.

This Compliance Requirement will ensure that the standards in place to protect cardholder information of students, employees, and any individual or entity that utilizes a credit card to transact business with the College. PCI DSS requirements as established and revised by the PCI Security Standards Council. This Compliance Requirement is only intended to be used as supplement to this full set of requirements.

Scope

Any departments that accepts credit and debit card payment, or have access to credit card information must comply with PCI Compliance Requirement. These currently include:

- Financial Services – Accepts and processes credit cards for payment of student accounts.
- Campus Book Store – Accepts and processes credit cards for the payment of books, supplies and other products.
- Henrys Food Court / American Harvest Restaurant – Accepts and processes credit cards for the payment of food items.
- Schoolcraft College Fitness Center - Accepts and processes credit cards for the payment for membership.

Roles

The Director of Risk Management and the Controller shall serve as the coordinator of the Compliance Requirement, which includes responsibility for notifying the Information Security, applicable department supervisors about changes to the Compliance Requirement. IT Department directors will assist in this process as needed.

General Requirements

Payment Card Restrictions:

- Storage of any credit card information in an electronic format on any computer, server, mobile device, or database is prohibited.
- Credit card information must not be transmitted via email.
- Transmission of credit card information in any manner other than PCI complaint encryption mechanisms and systems is prohibited.
- Systems that process credit card information must be monitored and system software must be kept at current levels to meet PCI DSS requirements.
- Third party quarterly PCI compliancy scans must be performed on networks that process credit card information.
- Any action that violates PCI DSS requirements is prohibited.

Procedures

Schoolcraft College requires compliance with PCI standards. To achieve compliance, departments accepting credit cards for the College must meet the following requirements.

Requirements

- All employees involved in processing credit card payments must demonstrate understanding of the Information Security policies of Schoolcraft College. This demonstration must be kept in their Human Resource file for the life of their employment in that capacity.
- All Credit card merchant accounts must be approved by the Controller.
- Supervisors and their employees must be familiar with and adhere to the current PCI DSS requirements. These requirements are set forth by the PCI Security Standards Council.
- Supervisors in departments accepting credit cards must conduct self-assessment against the requirements annually. These self-assessments results must reported to both the Controller, the risk management office, and the VP & CIO.
- Any proposal for a new process (electronic or paper) related to the storage, transmission or processing of credit card data must be brought to the attention of and be approved by the Controller.
- The Executive Director of Server Administration & Business Continuity, Director of Risk Management and the Controller must approve all equipment and technologies used to process credit card information.

Storage and Disposal

- Credit card information must not be captured or stored on College systems, including but not limited to network servers, workstations, laptops, or storage systems.
- Web payments must use a PCI compliant service provider approved by the Controller. Credit card numbers must NOT be entered into server hosted on the College's network.
- All credit card processing machines must be configured to only print last four or first six digits of a credit card number.
- Any physical documents containing credit card information should be limited to only information required to transact the business. These documents must be stored in a secure location, and must be destroyed as soon as possible using the College's document destruction processes. In no instance shall this exceed record retention requirements.
- Information security will perform an annual network using the ForcePoint™ Data Loss Prevention System to scan to ensure that credit card information has not been stored on any Schoolcraft College computer resources.
- The Controller must approve all existing, or proposed, merchant bank or processing contract of any third-party vendor who will process credit card information.
- The Controller must ensure contractually and in practice that any third-party vendors also adhere to all rules and regulations governing PCI DSS.
- The Controller must ensure third-party vendors provide proof of current compliance and plans for ongoing compliance.

Self-assessment

The Director of Risk management or the Controller will notify relevant department supervisors of when they must complete and submit the annual assessment. The PCI self-assessment questionnaire must be completed by the director of the department approved to accept credit cards. The director is in effect the merchant account owner.

Training

Ongoing training programs must be offered to train employees on PCI DSS and importance of compliance. Employees must be recertified in their understanding PCI DSS and the Information Security Compliance Requirement every two years.

Authentication and Authorization Compliance Requirement

Introduction

Schoolcraft College's Authentication and Authorization (AA) Compliance Requirement of the Information Security Policy provides the College with a method to ensure the proper controls are in place to limit access to information to only those users who should have access to it. Access is based on the College's Data Classification Compliance Requirement.

Purpose

Federal, State and the credit industry regulations require the protection of assets. This along with security best practices and privacy protections set forth by national organizations set guidelines for due care and due diligence. These regulations and best practices define the security that must be in place to protect information that is classified as confidential, and to a lesser degree in-house. This AA Compliance Requirement is designed to address both the regulatory requirements, along with best practices to ensure proper authentication, and authorization to information is in place.

Scope

The AA Compliance Requirement applies to anyone who accesses, manipulates, manages, otherwise uses college IT systems, or has access to college information.

Securing and protecting these resource is the responsibility of everyone who uses them. There is a significant cost associated with the protection of information assets and the integrity of systems use on a global scale. Everyone is expected to participate in securing our organization.

Compliance Requirement

In accordance with the Schoolcraft College Data Classification Compliance Requirement, all IT systems that create, receive, process, store, or transmit data classified as confidential or for internal use must adhere to the authentication and authorization guidelines of this of this document.

Roles

- Vice President and Chief Information Officer for Information Technology oversight.
- Information Technology department for implementation and management.
- Human Resources for change approvals.
- Department directors for change requests.

Outsourcing Contracts

Contracts for systems that will be maintained at a vendor's site should be written in a manner, which will allow for enforcement of this Compliance Requirement.

Access to *Internal Use* information

Department directors that manage internal use systems are responsible for requesting and ensuring access to those systems is based on job duties.

Directors must document the requested access using the 'user account management' template, for access to these internal use systems. This documentation must be submitted as an email to 'user account management' email address before access is granted.

Human Resources will process termination requests for any employ that is separated from the College. All access will be revoked when termination date and time has been formally determined and all approvals are in place.

Access to *Confidential* information

Department directors that manage confidential systems are responsible for requesting and ensuring access to those systems is based on job duties. Directors must document, the requested access using the 'user account management template' for access to these confidential systems.

- This documentation must be submitted as an email to 'user account management' email address before access is granted. The email must originate from the director and must be sent from directors' email to signify approval of the change. Confirmation emails will be returned to director verifying the change request and change completion.
- The 'user account management template' is also used for the timely termination of workforce member and vendor access to confidential systems whenever appropriate (does not apply to employee separation).

When access change need is determined like a change in role or position. Department directors must request changes to the access of data in a timely manner.

Human Resources will process termination requests for any employ that is separated from the College. All access will be revoked when termination date and time has been formally determined and all approvals are in place.

Department directors must maintain a document of who accesses what systems, or process. Information must include:

- Document name, department, organization, position and contact information. This should include third party vendors. (Third party vendors are considered to be reporting to the director in which the data's steward would report to).
- Authorization methods may (method not actual ID) include but are not limited to:
  - College Active Directory ID
  - ERP system ID
  - Module ID

   - Vendor ID
   - Two Factor Authentication
   - Keys
- Authentication methods also include the manner and type of authentication:
   - Passwords
   - Remote access
   - Token
   - Biometrics
- Methods for evaluating access to confidential systems based on the need to fulfill an appropriate business purpose.
- Documentation of the department process to review access of authorized users, this review should occur on an annual basis.
- Documentation of the process for regularly assessing effectiveness of access controls to Confidential systems
- Documentation of the department's internal procedure for determining the requirements for adding or removing, users or vendors access to confidential systems during normal operations and during an emergency.
- The College uses Cisco ISE™ (Identity Services Engine) that combines user credentials and device profiling to assign access rights at the network switch access port level.

Unique identification of users.

All users who need to access systems, at a minimum are issued user ID's, passwords, and Prox cards. In some cases, additional verification mechanisms are required. All of these methods, when used to gather authorizing information, are referred to as a user's credentials and are unique to every individual. Access to confidential or internal use information or systems must be performed using your unique set of credentials. These credentials must belong only to the user or process to which it has been assigned.

- Sharing of credentials is prohibited.
- Accessing confidential information by using anything other than one's own credentials makes it impossible to properly log and audit access. Therefore, it is not acceptable for any user to use another user's credentials or open terminal screen to access confidential information or systems.

Directors managing confidential internal use systems are responsible for ensuring that access technologies and methodologies for those systems incorporate the following:

- All their users or processes use a unique user ID's with appropriate authentication mechanism.
- Enforce the Compliance Requirement for not sharing or disclosing of password(s).
- Enforce the use of strong passwords that contain, at minimum, a combination of capital and lower-case letters, and numbers or symbols. All passwords must be at least fourteen characters long. All passwords must be difficult to guess.

- Regularly used domain administrative accounts in addition should be at least sixteen characters long using both numbers *and* symbols
- Special administrative and service accounts in addition should be at least eighteen characters long using both numbers and symbols
- Required password changes must happen at a minimum of every 90 days for those who access confidential information and 180 days for all others.
- Passwords cannot be reused after expiration. New passwords must be created.

In some circumstances, such as in specialized computer labs, is it acceptable to use a 'shared' account for login. In cases where shared accounts are required, managers and administrators of confidential systems must ensure that shared accounts are used only to access data classified as general or public. Shared accounts must not access confidential or internal use information at any time. (Note: we are moving away from this…)

Supervisors or Instructors of systems that have shared passwords should keep a log of who is using the system and when they were on it. (Note: we are moving away from this…)

Account Lockout

In accordance with security best practices, User accounts will be automatically locked out for a set period if multiple incorrect login attempts are attempted. This is to protect against automated attacks, which are focused on illegally accessing a system by attempting to guess the user’s password. Users will be able to attempt login again using their credentials after the period has elapsed.

Audit Control

Access to any confidential systems or its information must be electronically logged. Logged information is audited continually using the Schoolcraft College appointed SIEM system and will issue alerts & block certain activity. Audit results are logged and kept per the approved retention Compliance Requirement. For those who do not have an approved retention Compliance Requirement this information must be kept for at least three years. Inappropriate access must be reported to the Executive Director of Information Security and remediated immediately.

Automated log collection and analysis is performed to review user’s access and their activities when using network and IT system resources. Logging should be used for each layer including, but not limited to network, system application, and at the database layer itself. Access logs systems or security administrators must have procedures in place to log and review administrative and user access to IT resources.

Automated monitoring and alerting for any security events (intrusions) and performance (network and servers) changes are performed continuously using the LogRythm® SIEM system and the Cisco® Firepower™ IPS. Monitoring of the automated systems should be performed regularly to ensure it is operating as expected.

Specialized administrative and system accounts

Configuration of systems, including network, and servers often require a local or global administrator. In addition, systems that communicate with each other often have a shared account.

- These accounts are to be used only by senior level technicians for initial configuration these systems. They may not be used for any other function.
- System administrators performing administrative functions should use an administrative account that is unique to the individual performing the function.
- System accounts that needed to run system-to-system processes should only be created by senior level technicians and never used for any other function.

Enforcement of the use of strong passwords that contain, at minimum, a combination of capital and lower-case letters, and numbers and symbols are required. All passwords must be at least eighteen characters long. All passwords must be difficult to guess.

Executive Director of Information Security will be responsible for secure storage of these passwords. Executive Director of Information Security must document the names of those people who have access to the special passwords.

VPN & Remote Access Compliance Requirement

Introduction

Remote access to our corporate network is essential to maintain our Team’s productivity, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security posture than our corporate network. While these remote networks are beyond the control of The Schoolcraft College Compliance Requirement, we must mitigate these external risks the best of our ability.

Purpose

The purpose of this Compliance Requirement is to define rules and requirements for connecting to Schoolcraft College's network from any host. These rules and requirements are designed to minimize the potential exposure to Schoolcraft College from damages which may result from unauthorized use of Schoolcraft College resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Schoolcraft College internal systems, and fines or other financial liabilities incurred as a result of those losses.

Scope

This Compliance Requirement applies to all Schoolcraft College employees, contractors, vendors and agents with a Schoolcraft College-owned or personally-owned computer or workstation used to connect to the Schoolcraft College network. This Compliance Requirement applies to remote access connections used to do work on behalf of Schoolcraft College, including reading or sending email and viewing intranet web resources. This Compliance Requirement covers any and all technical implementations of remote access used to connect to Schoolcraft College networks.

Compliance Requirement

It is the responsibility of Schoolcraft College employees, contractors, vendors and agents with remote access privileges to Schoolcraft College's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Schoolcraft College. All remote access logins are required to use Two-Factor Authentication.

General access to the Internet for recreational use through the Schoolcraft College network is strictly limited to Schoolcraft College employees, contractors, vendors and agents (hereafter referred to as "Authorized Users"). When accessing the Schoolcraft College network from a personal computer, Authorized Users are responsible for preventing access to any Schoolcraft College computer resources or data by non-Authorized Users. Performance of illegal activities through the Schoolcraft College network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User's access. For further information and definitions, see the *Acceptable Use Compliance Requirement.* Authorized Users will not use Schoolcraft College networks to access the Internet for outside business interests.

Monitoring & Enforcement Compliance Requirement

Overview

Logging from critical systems, applications and services can provide key information and potential indicators of compromise. Although logging information may not be viewed on a daily basis, it is critical to have from a forensics standpoint.

Purpose

The purpose of this document attempts to address this issue by identifying specific requirements that information systems must meet in order to generate appropriate audit logs and integrate with an enterprise's log management function.

The intention is that this language can easily be adapted for use in enterprise IT security policies and standards, and also in enterprise procurement standards and RFP templates. In this way, organizations can ensure that new IT systems, whether developed in-house or procured, support necessary audit logging and log management functions.

Scope

This Compliance Requirement applies to all production systems on the Schoolcraft College Network.

Log Retention

All systems that handle confidential information, accept network connections, or make access control decisions shall record and retain audit-logging information sufficient to answer the following questions:

1. What activity was performed?
2. Who or what performed the activity, including where or on what system the activity was performed from?
3. What the activity was performed on?
4. When was the activity performed?
5. What tool(s) was the activity performed with?
6. What was the status, outcome, or result of the activity?

The Information Security team will verify compliance to this Compliance Requirement though various methods, including but not limited to, periodic walk-throughs, security tools, internal and external audits. The Information Security team must approve any exceptions to the Compliance Requirement.

Email & Electronic Communication Usage Compliance Requirement

Introduction

Electronic communications are pervasively used in almost all industry verticals and is often the primary communication and awareness method within an organization. At the same time, misuse of electronic communication can post many legal, privacy and security risks, thus, it is important for users to understand the appropriate use of electronic communications.

Purpose

The purpose of this Compliance Requirement is to ensure the proper use of the Schoolcraft College Email system and make users aware of what Schoolcraft College deems as acceptable and unacceptable use of its Email system and other electronic communication systems. This Compliance Requirement outlines the minimum requirements for use of electronic communications within Schoolcraft College Network.

Scope

This Compliance Requirement covers appropriate use of any Electronic message sent from a Schoolcraft College address and applies to all employees, vendors, and agents operating on behalf of Schoolcraft College.

Compliance Requirement

All use of Email must be consistent with Schoolcraft College policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.

- Schoolcraft College Email accounts should be used primarily for Schoolcraft College business-related purposes; personal communication is permitted on a limited basis, but non-Schoolcraft College related commercial uses are prohibited.
- All Schoolcraft College data contained within an Email message or an attachment must be secured according to policies defined in this document.
- Email should be retained only if it qualifies as a Schoolcraft College business record. Email is a Schoolcraft College business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email.
- Email that is identified as a Schoolcraft College business record shall be retained according to Schoolcraft College Record Retention requirements.
- The Schoolcraft College Email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any Schoolcraft College employee should report the matter to their supervisor immediately.
- Users are prohibited from automatically forwarding Schoolcraft College Email to a third-party Email system. Individual messages which are forwarded by the user must not contain Schoolcraft College confidential or above information.
- Users are prohibited from using any third-party email systems and storage servers such as Google, Yahoo, or Outlook.com (Not the enterprise email application called Outlook) to conduct Schoolcraft College business, to create or memorialize any binding transactions, or to store or retain email on behalf of Schoolcraft College. Such communications and transactions should be conducted through proper channels using Schoolcraft College approved documentation.
- Schoolcraft College employees shall have no expectation of privacy in anything they store, send or receive on the company's Email system.
- Schoolcraft College may monitor messages without prior notice. Schoolcraft College is not obliged to monitor Email messages.

Wireless Security Compliance Requirement

Introduction

Wireless communications are becoming increasingly prevalent for organizations due to the massive number of devices using the internet today.

Purpose

This standard specifies the technical requirements that wireless infrastructure devices must satisfy to connect to the Schoolcraft College network. Only those wireless infrastructure devices that meet the requirements specified in this standard or are granted an exception by the Information Security Team are approved for connectivity to the Schoolcraft College network. Network devices including, but not limited to, hubs, routers, switches, firewalls, remote access devices, modems, or wireless access points, must be installed, supported, and maintained by an Information Security approved support organization.

Scope

All employees, contractors, consultants, temporary and other workers at Schoolcraft College, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of Schoolcraft College must adhere to this Compliance Requirement. This Compliance Requirement applies to all wireless infrastructure devices that connect to a Schoolcraft College network or reside on a Schoolcraft College site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and tablets. This includes any form of wireless communication device capable of transmitting packet data.

Wireless Communication Standard

All wireless infrastructure devices that connect to a Schoolcraft College network or provide access to Schoolcraft College Confidential, Schoolcraft College Highly Confidential, or Schoolcraft College Restricted information must:

- Use Advanced Encryption System (AES) protocols with a minimum key length of 256 bits.
- All Bluetooth devices must use Secure Simple Pairing with encryption enabled.
- Lab and Isolated Wireless Device Requirements
- Lab device Service Set Identifier (SSID) must be different from Schoolcraft College production device SSID.
- Broadcast of lab device SSID must be disabled.
- Home Wireless Device Requirements
- All home wireless infrastructure devices that provide direct access to a Schoolcraft College network, such as those connecting through a VPN, must adhere to the following:
- Enable WiFi Protected Access Pre-shared Key (WPA2)

- When enabling WPA2, configure a complex shared secret key (at least 16 characters) on the wireless client and the wireless access point
- Change the default SSID name
- Change the default login and password

Wireless Communications Compliance Requirement

All wireless infrastructure devices that reside at a Schoolcraft College site and connect to a Schoolcraft College network, or provide access to information classified as Schoolcraft College Confidential, or above must:

- Abide by the standards specified in the Wireless Communication Standard.
- Be installed, supported, and maintained by an approved support team.
- Use Schoolcraft College approved authentication protocols and infrastructure.
- Use Schoolcraft College approved encryption protocols.
- Maintain a hardware address (MAC address) that can be registered and tracked.
- Not interfere with wireless access deployments maintained by other support organizations.

Lab and Isolated Wireless Device Requirements

All lab wireless infrastructure devices that provide access to Schoolcraft College Confidential or above, must adhere to the statements above. Lab and isolated wireless devices that do not provide general network connectivity to the Schoolcraft College network must:

- Be isolated from the corporate network.
- Not interfere with wireless access deployments maintained by other support organizations.

Wireless infrastructure devices that provide direct access to the Schoolcraft College corporate network, must conform to the Home Wireless Device Requirements as detailed in the *Wireless Communication Standard*.

Wireless infrastructure devices that fail to conform to the Home Wireless Device Requirements must be installed in a manner that prohibits direct access to the Schoolcraft College corporate network. Access to the Schoolcraft College corporate network through this device must use standard remote access authentication.

Network Device & Configuration Compliance Requirement

Scope

This Compliance Requirement applies to any network device installed and/or configured by Schoolcraft College employees or appointed vendors. The hardware as well as the configurations of any networks software must meet the requirements stated in this Compliance Requirement.

Compliance Requirement

Networks transmitting unencrypted personal identifiable information must not be on the same subnet that any non-IT personnel has access to. All network connections for all Schoolcraft College networks should be documented and updated once changes are made.

1. The enable password on the router or switch must be kept in a secure encrypted form. The router or switch must have the enable password set to the current production router/switch password from the device's support organization.

2. The following services or features must be disabled:
   - a) IP directed broadcasts
   - b) Incoming packets at the router/switch sourced with invalid addresses such as RFC1918 addresses
   - c) TCP small services
   - d) UDP small services
   - e) All source routing and switching
   - f) All web services running on router
   - g) Cisco discovery protocol on Internet connected interfaces
   - h) Telnet, FTP, and HTTP services
   - i) Auto-configuration

3. The following services should be disabled unless a business justification is provided:
   - a) Cisco discovery protocol and other discovery protocols
   - b) Dynamic trunking
   - c) Scripting environments, such as the TCL shell

4. The following services must be configured:
   - a) Password-encryption
   - b) NTP configured to a corporate standard source

5. All routing updates shall be done using secure routing updates.

6. Use corporate standardized SNMP community strings. Default strings, such as public or private must be removed. SNMP must be configured to use the most secure version of the protocol allowed for by the combination of the device and management systems.

7. Access control lists must be used to limit the source and type of traffic that can terminate on the device itself.

8. Access control lists for transiting the device are to be added as business needs arise.

9. The router must be included in the corporate enterprise management system with a designated point of contact.

10. Each router must have the following statement presented for all forms of login whether remote or local:

11. *"UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this Compliance Requirement may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device. Use of this system shall constitute consent to monitoring."*

12. Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. SSH version 2 is the preferred management protocol.

13. Dynamic routing protocols must use authentication in routing updates sent to neighbors. Password hashing for the authentication string must be enabled when supported.

14. The corporate router configuration standard will define the category of sensitive routing and switching devices, and require additional services or configuration on sensitive devices including:

    a) IP access list accounting
    b) Device logging
    c) Incoming packets at the router sourced with invalid addresses, such as RFC1918 addresses, or those that could be used to spoof network traffic shall be dropped
    d) Router console and modem access must be restricted by additional security controls

Server Security Compliance Requirement

<u>Introduction</u>

Unsecured and vulnerable servers continue to be a major entry point for malicious threat perpetrators. Consistent Server installation policies, ownership and configuration management are all about doing the basics well.

Purpose

The purpose of this Compliance Requirement is to establish standards for the base configuration of internal server equipment that is owned and/or operated by Schoolcraft College. Effective implementation of this Compliance Requirement will minimize unauthorized access to Schoolcraft College proprietary information and processes.

Scope

All employees, contractors, consultants, temporary and other workers at Schoolcraft College and its subsidiaries must adhere to this Compliance Requirement. This Compliance Requirement applies to server equipment that is owned, operated, or leased by Schoolcraft College or registered under a Schoolcraft College-owned network.

Compliance Requirement

General Requirements

Internal servers deployed at Schoolcraft College must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by the Information Security team. Operational groups should monitor configuration compliance and implement an exception Compliance Requirement tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by the Information Security team. The following items must be met:

- Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
  - Server contact(s) and location, and a backup contact
  - Hardware and Operating System/Version
  - Main functions and applications, if applicable
- Information in the corporate enterprise management system must be kept up-to-date.
- Configuration changes for production servers must follow the appropriate change management procedures.
- For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, processes, and network traffic.

Configuration Requirements

- Operating System configuration should be in accordance with approved Information Security guidelines.
- Services and applications that will not be used must be disabled where practical.
- Access to services should be logged and/or protected through access-control methods such as a web application firewall, if possible.

- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication is sufficient.
- Always use standard security principles of least privilege access to perform a function. Do not use root, admin, or administrator accounts when a non-privileged account will do.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or HTTPS).
- Servers should be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled cubicle areas.

Workstation Security Compliance Requirement

Purpose

The purpose of this Compliance Requirement is to provide guidance for workstation security for Schoolcraft College workstations in order to ensure the security of information on the workstation and information the workstation may have access to.

Scope

This Compliance Requirement applies to all Schoolcraft College employees, contractors, workforce members, vendors and agents with a Schoolcraft College-owned or personal-workstation connected to the Schoolcraft College network.

Compliance Requirement

Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitive information, including personally identifiable information and that access to sensitive information is restricted to authorized users.

Schoolcraft College members using workstations shall consider the sensitivity of the information, including personally identifiable information that may be accessed and minimize the possibility of unauthorized access.

Schoolcraft College will implement physical and technical safeguards for all workstations that access electronic protected health information to restrict access to authorized users.

Appropriate measures include:

- Restricting physical access to workstations to only authorized personnel.

- Require 10 minutes screen lockout timers on staff and faculty computers and 2 hours on classroom podium computers and computer lab desktop computers.
- Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected. The password must comply with Schoolcraft College password requirements.
- Complying with all applicable password policies and procedures.
- Ensuring workstations are used for authorized business purposes only.
- Never installing unauthorized software on workstations.
- Storing all sensitive information on network servers.
- Keeping food and drink away from workstations in order to avoid accidental spills.
- Securing laptops that contain sensitive information by using cable locks or locking laptops up in drawers or cabinets.
- Installing privacy screen filters or using other physical barriers to alleviate exposing data.
- Exit running applications and close open documents.
- If wireless network access is used, ensure access is secure by following the *Wireless Communication Compliance Requirement*

Web Application Compliance Requirement

Introduction

Web application vulnerabilities account for the largest portion of attack vectors outside of malware. It is crucial that any web application be assessed for vulnerabilities and any vulnerabilities by remediated prior to production deployment.

Purpose

The purpose of this Compliance Requirement is to define web application security assessments within Schoolcraft College. Web application assessments are performed to identify potential or identified weaknesses as a result of inadvertent misconfiguration, weak authentication, insufficient error handling, sensitive information leakage, etc. Discovery and subsequent mitigation of these issues will limit the attack surface of Schoolcraft College services available both internally and externally as well as satisfy compliance with any relevant policies in place.

Scope

This Compliance Requirement covers all web application security assessments requested by any individual, group or department for the purposes of maintaining the security posture, compliance, risk management, and change control of technologies in use at Schoolcraft College.

All web application security assessments will be performed by delegated security personnel either employed or contracted by Schoolcraft College. All findings are considered confidential and are to be distributed to persons on a "need to know" basis. Distribution of any findings outside of Schoolcraft College is strictly prohibited unless approved by the Chief Information Officer.

Any relationships within multi-tiered applications found during the scoping phase will be included in the assessment unless explicitly limited. Limitations and subsequent justification will be documented prior to the start of the assessment.

Compliance Requirement

- Web applications are subject to security assessments based on the following criteria:
  - New or Major Application Release – will be subject to a full assessment prior to approval of the change control documentation and/or release into the live environment.
  - Third Party or Acquired Web Application – will be subject to full assessment after which it will be bound to Compliance Requirement requirements.
  - Point Releases – will be subject to an appropriate assessment level based on the risk of the changes in the application functionality and/or architecture.
  - Patch Releases – will be subject to an appropriate assessment level based on the risk of the changes to the application functionality and/or architecture.
  - Emergency Releases – An emergency release will be allowed to forgo security assessments and carry the assumed risk until such time that a proper assessment can be carried out. Emergency releases will be designated as such by the Chief Information Officer or an appropriate manager who has been delegated this authority.
- All security issues that are discovered during assessments must be mitigated based upon the following risk levels. The Risk Levels are based on the Open Web Application Security Project (OWASP) Risk Rating Methodology. Remediation validation testing will be required to validate fix and/or mitigation strategies for any discovered issues of Medium risk level or greater.
- High – Any high-risk issue must be fixed immediately or other mitigation strategies must be put in place to limit exposure before deployment. Applications with high risk issues are subject to being taken off-line or denied release into the live environment. Once the immediate risk has been mitigated, the situation will be communicated to the most appropriate cabinet member.
- Medium – Medium risk issues should be reviewed to determine what is required to mitigate and scheduled accordingly. Applications with medium risk issues may be taken off-line or denied release into the live environment based on the number of issues and if multiple issues increase the risk to an unacceptable level. Issues should be fixed in a patch/point release unless other mitigation strategies will limit exposure.
- Low – Issue should be reviewed to determine what is required to correct the issue and scheduled accordingly.
- The following security assessment levels shall be established by the Information Security team or other designated organization that will be performing the assessments.

- Full – A full assessment is comprised of tests for all known web application vulnerabilities using both automated and manual tools based on the OWASP Testing Guide. A full assessment will use manual penetration testing techniques to validate discovered vulnerabilities to determine the overall risk of any and all discovered.
- Quick – A quick assessment will consist of a (typically) automated scan of an application for the OWASP Top Ten web application security risks at a minimum.
- Targeted – A targeted assessment is performed to verify vulnerability remediation changes or new application functionality.

Encryption Compliance Requirement

Purpose

The purpose of this Compliance Requirement is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively.

Scope

This Compliance Requirement applies to all Schoolcraft College employees and affiliates.

Section Glossary

AES - Advanced Encryption Standard

ECC - Elliptic Curve Cryptography

FIPS - Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), is a U.S. government computer security standard used to approve cryptographic modules.

Hash(ing) - is the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string. Used in encryption.

IETF - Internet Engineering Task Force

IRTF - Internet Research Task Force

LWDM - Lane Department Warning Module used in encryption key authentication.

NIST - National Institute of Standards and Technology

RSA - is an acronym that stands for Rivest, Shamir, and Adelman, the inventors of the encryption technique.

SHA – Secure Hash Algorithm used in encryption.

Compliance Requirement

Algorithm Requirements

Ciphers in use must meet or exceed the set defined as "AES-compatible" or "partially AES-compatible" according to the IETF/IRTF Cipher Catalog, or the set defined for use in the United States National Institute of Standards and Technology (NIST) publication FIPS 140-2, or any superseding documents according to the date of implementation. The use of the Advanced Encryption Standard (AES) is strongly recommended for symmetric encryption.

Algorithms in use must meet the standards defined for use in NIST publication FIPS 140-2 or any superseding document, according to date of implementation. The use of the RSA and Elliptic Curve Cryptography (ECC) algorithms is strongly recommended for asymmetric encryption. Signature Algorithms must be at least RSA 2048 or LDWM SHA256.

Hash Functions

Schoolcraft College adheres to the NIST Policy on Hash Functions

Encryption is a process of translation of data into a secret code. A Key, as used in the context of encryption, can be loosely defined as a password or code that is used in the translation, encoding, or scrambling of the data when it is encrypted. This key is also used to access the data after it is encrypted. This key must be protected from being lost as encryption keys cannot be reset like a password and the information cannot be recovered if this key is lost.

Key Agreement & Authentication

- Key exchanges must use one of the following cryptographic protocols: Diffie-Hellman, IKE, or Elliptic curve Diffie-Hellman (ECDH).
- End points must be authenticated prior to the exchange or derivation of session keys.
- Public keys used to establish trust must be authenticated prior to use. Examples of authentication include transmission via cryptographically signed message or manual verification of the public key hash.
- All servers used for authentication (for example, RADIUS or TACACS) must have installed a valid certificate signed by a known trusted provider.
- All servers and applications using SSL or TLS must have the certificates signed by a known, trusted provider.

Key Generation

- Cryptographic keys must be generated and stored in a secure manner that prevents loss, theft, or compromise.
- Key generation must be seeded from an industry standard random number generator (RNG). For examples, see NIST Annex C: Approved Random Number Generators for FIPS PUB 140-2.

Technology Equipment Disposal Compliance Requirement

Introduction

Technology equipment often contains parts which cannot simply be thrown away. Proper disposal of equipment is both environmentally responsible and often required by law. In addition, hard drives, USB drives, CDs, DVDs and other storage media containing various kinds of Schoolcraft College data, some of which is considered sensitive. In order to protect our constituent's data, all storage mediums must be properly erased before being disposed of. However, simply deleting or even formatting data is not considered sufficient. When deleting files or formatting a device, data is marked for deletion, but is still accessible until being overwritten by a new file. Therefore, special tools must be used to securely erase data prior to equipment disposal.

Purpose

The purpose of this Compliance Requirement it to define the guidelines for the disposal of technology equipment and components owned by Schoolcraft College.

Scope

This Compliance Requirement applies to any computer/technology equipment or peripheral devices that are no longer needed within Schoolcraft College including, but not limited to the following: personal computers, servers, hard drives, laptops, smart phones, tablets, peripherals (i.e., keyboards, mice, speakers), printers, scanners, portable storage devices (i.e., USB drives, compact discs), backup tapes, printed materials. All Schoolcraft College employees and affiliates must comply with this Compliance Requirement.

Compliance Requirement

Technology Equipment Disposal

- When Technology assets have reached the end of their useful life they should be sent to the Technical Support or Server Administration team's office for proper disposal.
- The Technical Support or Server Administration team will securely erase all storage mediums in accordance with current industry best practices.
- All data including, all files and licensed software shall be removed from equipment using disk sanitizing software that cleans the media overwriting each and every disk sector of the machine with zero-filled blocks, meeting Department of Defense standards.
- No computer or technology equipment may be sold to any individual other than through the processes identified in this Compliance Requirement.
- No computer equipment should be disposed of via skips, dumps, landfill etc. Electronic recycling bins may be periodically placed in locations around Schoolcraft College. These can be used to dispose of equipment. The Technical Support or Server Administration team will properly remove all data prior to final disposal.

- All electronic drives must be degaussed or overwritten with a commercially available disk cleaning program. Hard drives may also be removed and rendered unreadable (drilling, crushing or other demolition methods).
- Computer Equipment refers to desktop, laptop, tablet or netbook computers, printers, copiers, monitors, servers, handheld devices, telephones, cell phones, disc drives or any storage device, network switches, routers, wireless access points, batteries, backup tapes, etc.
- The Technical Support or Server Administration team will place a sticker on the equipment case indicating the disk wipe has been performed. The sticker will include the date and the initials of the technician who performed the disk wipe.
- Technology equipment with non-functioning memory or storage technology will have the memory or storage device removed and it will be physically destroyed.

Employee Purchase of Disposed Equipment

- Equipment which is working, but reached the end of its useful life to Schoolcraft College will be made available for purchase by employees.
- A lottery system will be used to determine who has the opportunity to purchase available equipment.
- All equipment purchases must go through the lottery process. Employees cannot purchase their office computer directly or “reserve” a system. This ensures that all employees have an equal chance of obtaining equipment.
- Finance and Information Technology will determine an appropriate cost for each item.
- All purchases are final. No warranty or support will be provided with any equipment sold.
- Any equipment not in working order or remaining from the lottery process will be donated or disposed of according to current environmental guidelines. Information
- Technology has contracted with several organizations to donate or properly dispose of outdated technology assets.
- Prior to leaving Schoolcraft College premises, all equipment must be removed from the Information Technology inventory system.

References

Archive. (2014, April 1). Retrieved April 27, 2014, from http://csrc.nist.gov/groups/SMA/fasp/archive.html

Audit Security Policy Templates. (2014). Retrieved May 1, 2014, from http://www.sans.org/security-resources/policies/audit.php

Barman, S. (2002). Writing information security policies. Indianapolis, IN: New Riders. Retrieved April 20, 2014, from http://techbus.safaribooksonline.com/book/networking/security/157870264x

Bradley, T. (2014, April 01). Whose fault is it that users are the weakest link? Retrieved May 05, 2014, from http://www.csoonline.com/article/2138481/data-protection/whose-fault-is-it-that-users-are-the-weakest-link.html

CSIRT. (2011). Retrieved April 29, 2014, from http://www.csirt.org/sample_policies/index.html

Grama, J. L. (2011). Legal Issues in Information Security. Retrieved April 16, 2014, from http://techbus.safaribooksonline.com/book/networking/security/9780763791858/chapter-13-information-security-governance/400?query=((information+security+policies))#snippet

Greene, S. S. (n.d.). Security program and policies: Principles and practices. Retrieved April 31, 2014,fromhttp://techbus.safaribooksonline.com/9780133481181/app01lev1sec1_html?percentage=0&reader=html

Guel, M. D. (2007). A Short Primer for Developing Security Policies. *The SANS Institute*. Retrieved April 25, 2014, from https://www.sans.org/security-resources/policies/Policy_Primer.pdfGuideline 5.23.1.4 Information Security Incident Response. (2012, January 25). Retrieved April 30, 2014, from http://www.mnscu.edu/board/procedure/523p1g4.html

International Standards Organization, & International Electrotechnical Commission. (2005). Information Technology — Security, second edition. Retrieved May 17, 2014, from http://www.specon.ru/files/ISO-IEC%2017979%20(second%20edition).pdf

Information Technology Security | Policy Library. (2012, November 8). Retrieved April 30, 2014, from http://www.Policy.iastate.edu/Policy/it/security

Kundinger, C. (2008, July). The Benefits of a Policy-Based Security Approach. Retrieved April 6, 2014, from http://www.ibmsystemsmag.com/ibmi/administrator/security/The-Benefits-of-a-Policy-Based-Security-Approach/National Institute of Standards and Technology. (June 2010). Guide for Assessing the Security. *NIST Special Publication 800-53A,* (Rev1). Retrieved May 23, 2014, from http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf

National Institute of Standards and Technology. (September 2012). Guide for Conducting Risk Assessments. *NIST Special Publication 800-30, (Rev1)*. Retrieved May 22, 2014, from http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

National Institute of Standards and Technology. (February 2010). Guide for Applying the Risk Management Framework to Federal Information Systems. NIST Special Publication 800-37, (Rev1). Retrieved May 25, 2014, from http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

National Institute of Standards and Technology. (April 2013). Security and Privacy Controls for Federal Information Systems. *NIST Special Publication 800-53,* (Rev4). Retrieved May 21, 2014, from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Office of Information Technology. (n.d.). IT Standards & Guidelines. Retrieved April 26, 2014, from https://cms.montgomerycollege.edu/oit/standardsandguidelines.aspx?id=327

Park, L. (2014, January 1). Data Breach Trends. Retrieved May 15, 2014, from http://www.symantec.com/connect/blogs/data-breach-trends

Policies - Information Security Office - Lansing Community College. (2014). Retrieved May 3, 2014, from http://www.lcc.edu/infosecurity/policies.aspx

Quinn, S., Souppaya, M., Cook, M., & Scarfone, K. (February 2011). National Checklist Program for IT Products: Guidelines for Checklist Users and Developers. *NIST Special Publication 800-70, (Rev2)*. Retrieved May 23, 2014, from http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

Roman, J. (2014, April 22). Class action Suit filed in College breach. Retrieved April 26, 2014, from http://www.databreachtoday.asia/class-action-suit-filed-in-college-breach-a-6772

SANS. (2014). Information Security Policy Templates. Retrieved May 7, 2014, from http://www.sans.org/security-resources/policies/

Senge, P. M. (2006). 9. In The fifth discipline: The art and practice of the learning organization (pp. 163-190). New York: Doubleday/Currency.

Stine, K., Kissel, R., Baker, W. C., Fahlsing, J., & Gulick, J. (August 2008). Guide for Mapping Types of Information and Information Systems to Security Categories. NIST Special Publication 800-60, 1(Rev1). Retrieved May 22, 2014, from http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf

Stewret, J. M., Chapple, M., & Gibson, D. (2012). CISSP: Certified Information Systems Security Professional Study Guide Ch. 5. Retrieved April 23, 2014, from http://books.google.com/books?id=c0Ii96jfktQC&pg=PA214&dq=information+security+PolicyProcedure+and+due+diligence&hl=en&sa=X&ei=kCeSU9HHHdOKyATmkIH4AQ&ved=0CEkQ6AEwAw#v=onepage&q=information%20security%20Policy%20and%20due%20diligence&f=false

Approved–Cabinet January 20, 2009
Revised—Cabinet September 1, 2009
Completely Revised – Cabinet September 19, 2018