Data Classification Policy

AN ADMINISTRATIVE INFORMATION SECURITY POLICY

PURPOSE

Washtenaw Community College uses data classification and security levels to ensure all data and the systems on which it is stored, accessed, transmitted, or have the ability to impact the security of the data have appropriate security controls to protect the confidentiality, integrity, and availability of the data. This Data Classification Policy establishes a baseline derived from federal laws, state laws, regulations, and College policies that govern the privacy and confidentiality of data.

SCOPE

The Data Classification Policy is to be applied to all data (e.g. student, research, financial, employee data collected in electronic or hard copy form that is generated, maintained, and entrusted to Washtenaw Community College) except where a different standard is required by grant, contract, or law. No data item is too small to be classified.

ROLES & RESPONSIBILITIES

Data Owner: Data Owners are College officials having direct operational-level responsibility for the management of one or more types of data. Data Owner responsibilities include:

- The application of this and related policies to the systems, data, and other information resources under their care or control
- Assigning data classification labels using the College's data classification methodology
- Identifying and implementing safeguards for Sensitive Data

- Communicating and providing education on the required minimum safeguards for protected data to authorized data users and data custodians

Data Custodian: Data Custodians are Information Technology or application administrators responsible for the operation and management of systems and servers that collect, manage, and provide access to College data. The appropriate Data Owner must authorize Data Custodians. Data Custodian responsibilities include:

- Maintaining physical and system security and safeguards appropriate to the classification level of the data in their custody
- Complying with applicable College computer security standards
- Managing Data Consumer access as authorized by appropriate Data Owners
- Following data handling and protection policies and procedures established by Data Owners and the Information Security Office

Data User: Data Users are the individual College community members who have been granted access to College data in order to perform assigned duties or in fulfillment of assigned roles or functions at the College. This access is granted solely for the conduct of College business. Data User responsibilities include:

- Following the policies and procedures established by the appropriate Data Owner and Information Security Office
- Complying with federal and state laws, regulations, and policies associated with the College data used
- Implementing safeguards prescribed by appropriate Data Owners for Sensitive Data
- Reporting any unauthorized access or data misuse to Information Security Office or the appropriate Data Owner for remediation

Information Security Office: The Information Security Office (ISO) is responsible for ensuring compliance with this policy as well as other information security-related activities including:

- Coordinate and document the College's information security program activities

- Support the creation and maintenance of the College information security and privacy related policies, standards, guidelines and controls
- Perform institutional risk assessments related to College information security
- Provide support for compliance with information security related laws, regulations, standards and contractual requirements
- Coordinate the development and implementation of a College-wide information security training and awareness program
- Disseminate information on current risks, threats, attacks, exploits and corresponding mitigation strategies through alerts, advisories, web pages and other technical publications

Security Incident Response Team: The Security Incident Response Team is a group of individuals who have been trained in security incident management, each having distinct response roles. The team is tasked with the following responsibilities:

- Determining the impact, scope and nature of the event or incident
- Understanding the technical cause of the event or incident
- Identifying what else may have happened or other potential threats resulting from the event or incident
- Researching and recommending solutions and workarounds
- Coordinating and supporting notification, communication and response strategies to other parts of the institution and other outside authorities, including IT groups and specialists, information and physical security groups, business managers, executive leadership, public relations, human resources, legal counsel and law enforcement
- Maintaining a repository of incident and vulnerability data and activity that can be used for correlation, trending, and developing lessons learned to improve the College's security posture and incident management processes

REQUIREMENTS & PRACTICES

The various units and departments at the College have a multitude of types of documents and data. To the extent particular documents or data types are not explicitly addressed within this policy, Data Owners in each business unit or department are responsible for classification of data by considering the potential for harm to individuals or the College in the event of unintended disclosure, modification, or loss. The Chief Information Officer or designated Information Security Office member may assist with the classification process and help coordinate efforts to achieve consistency across the College.

All institutional data must be classified into one of four (4) sensitivity levels, or classifications that Washtenaw Community College has identified, which are defined as Confidential, Restricted, Internal and Public. Although all the enumerated data values require some level of protection, particular data values are considered more sensitive and correspondingly tighter controls are required for these values.

When classifying data, each Data Owner should weigh the risk created by an unintended disclosure, modification or loss against the need to encourage open discussion, improve efficiency and further the College's mission of providing accessible and excellent educational programs and services. Data Owners should be particularly mindful to protect sensitive personal information, such as Social Security Numbers, drivers' license numbers and financial account numbers, disclosure of which may create the risk of identity theft.

All College data is to be reviewed on a periodic basis and classified according to its use, sensitivity and importance to the College and in compliance with federal and/or state laws.

Washtenaw Community College has pre-defined several types of sensitive data. The level of security required depends in part on the effect that unauthorized access or disclosure of those data values would have on College operations, functions, image or reputation, assets, or the privacy of individual members of the College community.

The College's data security classifications are:

Level 1 - Confidential (High Sensitivity)

Confidential Use data includes any information that the College has a contractual, legal, or regulatory obligation to safeguard in the most stringent manner. Confidential data requires a high level of protection against unauthorized disclosure, modification, transmission, destruction, and use. Level 1 data is intended solely for use within Washtenaw Community College and is limited to those with a "business need-to-know".

Any unauthorized disclosure, compromise, or destruction would result in severe damage to the College, its students, or employees. The College's obligations will depend on the particular data and the relevant contract or laws. In some cases, unauthorized disclosure or loss of this data would require the College to notify the affected individual and state or federal authorities.

Examples of Confidential data include:

- Information covered by the Family Educational Rights and Privacy Act (FERPA) for records for current and former students which requires special protection requirements, including Personality Identifiable Information (PII) or financial record information. This includes:
    - Medical and health records that the school creates or collects and maintains
    - Personal information such as a student's identification code, social security number, picture (if considered part of student record), or other information that would make it easy to identify or locate a student
    - Financial aid records, including applications, history information, verification documentation, counseling records, cost of attendance, financial records, judgment decisions, refusals, SARS, ISIRs, SAP documentation, work-study payroll information
- Electronic Protected Health Information (PHI) subject to the Health Insurance Portability and Accountability Act (HIPAA), which sets standards for protection of medical records and patient data. PHI is defined as "individually identifiable health information" transmitted by electronic media, maintained in electronic media or transmitted or

maintained in any other form or medium. PHI is considered individually identifiable if it contains one or more of the following identifiers:

- Name
- Address (all geographic subdivisions smaller than state including street address, city, county, precinct or zip code)
- All elements of dates (except year) related to an individual including birth date, admissions date, discharge date, date of death and exact age if over 89)
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate number
- Device identifiers and serial numbers
- Universal Resource Locators (URLs)
- Internet protocol (IP) addresses
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic or code that could identify an individual

- Personally Identifying Information (PII) as defined under the State of Michigan Identity Theft Protection Act (MCL §445-63) means a name, number, or other information that is used for the purpose of identifying a specific person or providing access to a person's financial accounts, including, but not limited to, a person's name, address, telephone number, driver license or state personal identification card number, social security number, place of

employment, employee identification number, employer or taxpayer identification number, government passport number, health insurance identification number, mother's maiden name, demand deposit account number, savings account number, financial transaction device account number or the person's account password, any other account password in combination with sufficient information to identify and access the account, automated or electronic signature, biometrics, stock or other security certificate or account number, credit card number, vital record, or medical records or information.

Legislation introduced under the State of Michigan Biometric Data Privacy Act (HB 5019) to regulate the acquisition, possession, and protection of biometric identifiers and biometric information by private entities. A "biometric identifier" is defined as a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. "Biometric information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. This pertains to biometric data collected outside of a health care setting. Potential example applications include biometric time clocks, door entry controls, and fingerprint or face geometry use on college-owned equipment, e.g. laptops, PDAs or phones.

- The Washtenaw Community College ID Number, when stored with other identifiable information such as name, date of birth or e-mail address
- Information covered by the Gramm-Leach-Bliley Act (GLBA), which requires protection of certain financial records
- Financial account numbers covered by the Payment Card Industry Data Security Standard (PCI-DSS), which controls how credit card information is accepted, used, and stored, including:
    - Cardholder name
    - Service code
    - Expiration date
    - CVC2, CVV2 or CID value
    - PIN or PIN block

    - Contents of a credit card's magnetic stripe
- Information that is the subject of a confidentiality or non-disclosure agreement
- Legally privileged information

Any unauthorized disclosure or loss of confidential data must be reported to the appropriate dean or department head. The dean or department head should determine whether to report the unauthorized disclosure or loss of confidential data to the College's Information Security Office and Security Incident Response Team.

Level 2 - Restricted (High to Medium Sensitivity)

Restricted Use data includes any information that the College has a contractual, legal, or regulatory obligation to safeguard in the most stringent manner. In some cases, unauthorized disclosure or loss of this data would require the College to notify the affected individual and state or federal authorities. In some cases, modification of the data would require informing the affected individual. The College's obligations will depend on the particular data and the relevant contract or laws.

Examples of Restricted use data include:

- Student record information covered by the Family Educational Rights and Privacy Act (FERPA) that is not identified as Personality Identifiable Information (PII) or financial record information. This includes:
    - Parents(s) and/or guardian addresses, and where parents can be contacted in emergencies
    - Grades, test scores, courses taken, academic specializations and activities, and official letters regarding a student's status in school
    - Special education records
    - Disciplinary records
    - Documentation of attendance, schools attended, courses taken, awards conferred, and degrees earned

- Personally identifiable health information that is not subject to HIPAA but used in research, such as Human Subjects Data, where so designated by a Institutional Review Board (IRB)
- Personally Identifiable Information (PII) entrusted to our care that is not classified as confidential data, such as information regarding applicants, alumni, donors, or potential donors
- Abbreviated Social Security Numbers, e.g. the last 4 digits
- Individual employment information, including salary, benefits and performance appraisals for current, former, and prospective employees
- "Criminal Background Data" that might be collected as part of an application form or a background check
- Unencrypted data used to authenticate or authorize individuals to use electronic resources, such as passwords, keys, and other electronic tokens
- Controlled Unclassified Information required to be compliant with NIST 800-171

By default, all College data that is not explicitly classified as either Public, Internal or Confidential should be treated as Restricted Use data. Any unauthorized disclosure, unauthorized modification, or loss of Restricted Use data must be reported to the College's Security Incident Response Team.

Level 3 – Internal (Private, Medium Sensitivity)

Internal Use information must be guarded due to proprietary, ethical or privacy considerations. Although not specifically protected by statute, regulations, or other legal obligations or mandates, unauthorized use, access, disclosure, acquisition, modification, loss or deletion of information at this level could cause financial loss, damage to Washtenaw Community College's reputation, or violate an individual's privacy rights (e.g., educational student records, employment history, and alumni biographical information). Data in this category is not routinely distributed outside the College. It may include, but is not limited to non-Confidential data contained within: internal communications, interim financial reports, minutes of meetings, unless such minutes are intended or required to be made public, and internal project reports.

Level 4 - Public (General Use, Low Sensitivity)

This is information that is not publicly disseminated, but accessible to the public. Public data can be explicitly defined as public information (e.g., state employee salary ranges), intended to be readily available to individuals both on and off campus (e.g., an employee's work email addresses or student directory information), or not specifically classified elsewhere in the protected data classification standard. Knowledge of this information does not expose Washtenaw Community College to financial or reputational loss, or jeopardize the security of College assets. Publicly available data may be subject to appropriate review or disclosure procedures to mitigate potential risks of inappropriate disclosure data to organize it according to its risk of loss or harm from disclosure.

Examples of Public data include:

- The Family Educational Rights and Privacy Act (FERPA) defines "directory information" as information contained in the education records of a student that would not generally be considered harmful or an invasion of privacy if disclosed. "Directory information" can include:
    - Student's name
    - Address
    - Telephone listing
    - Electronic mail address
    - Photograph
    - Date and place of birth
    - Major field of study
    - Enrollment status
    - Dates of attendance and graduation
    - Grade level
    - Participation in officially recognized activities and sports
    - Weight and height of members of athletic teams
    - Degrees, honors and awards received
    - The most recent educational agency or institution attended

> A school may disclose "directory information" to third parties without consent if it has given public notice of the types of information which it has designated as "directory information," the parent's or eligible student's right to restrict the disclosure of such information, and the period of time within which a parent or eligible student has to notify the school in writing that he or she does not want any or all of those types of information designated as "directory information." The means of notification could include publication in various sources, including a newsletter, in a local newspaper, or in the student handbook. The school could also include the "directory information" notification as part of the general notification of rights under FERPA. The school does not have to notify a parent or eligible student individually. (34 CFR § 99.37).

Additionally, press releases, course catalogs, application and request forms, and other general information are examples of public information that can be openly shared. The type of information a department would choose to post on its website is a good example of public data.

COMPLIANCE

This policy is a component of Washtenaw Community College information security program that is intended to comply with the PCI-DSS, FERPA, GLBA, GDPR, HIPAA and other regulations.

EXCEPTIONS

The Chief Information Officer (CIO) or a designated appointee is authorized to make exceptions to this policy. Any requests for exceptions shall be made using the *Request for Policy Exception* form and a copy maintained by the CIO.

VIOLATIONS

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Washtenaw Community College reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity.

DEFINITIONS

Data: Information collected, stored, transferred or reported for any purpose, whether electronically or hard copy.

Data Custodian: Responsible for following the procedures determined by the data owner to maintain the confidentiality, integrity, and availability of the data consistent with College policy, applicable state and federal laws, and contracts. Responsible for communicating the data security classification and security level to affected groups and individuals.

Data Owner: Accountable for specified information (e.g., a specific business function), broad type of data (e.g., HIPAA, PCI DSS, GLBA, FERPA), or type of data set (e.g., research data). Responsible for setting the data security classification and security level to meet state and federal laws and regulations, specific contractual requirements, College policy, and appropriate security controls to protect the confidentiality, integrity, and availability of the data. Data Owners are responsible for delegating responsibility to appropriate Data Custodian(s).

Data User: Responsible for maintaining the confidentiality, integrity, and availability of College data they manage and for following all College policies, procedures, and standards related to the data security classification and security level, including applicable state and federal laws, and contracts.

Family Education Rights and Privacy Act (FERPA): FERPA deals with student "education records," defined to mean (with a few exceptions) records containing information directly related to a student that are maintained by a school or its agent.

General Data Protection Regulation (GDPR): General Data Protection Regulation (GDPR) enacted by the European Commission to strengthen and unify data protection and privacy for individuals within the European Union (EU), whilst addressing the export of personal data outside the EU.

Gramm-Leach-Bliley Act for Disclosure of Nonpublic Personal Information (GLBA): The Gramm Leach Bliley Act (GLBA) requires that financial institutions safeguard nonpublic customer data, limit disclosures of such data, and notify customers of their information sharing practices and privacy policies.

Health Insurance Portability and Accountability Act (HIPAA): HIPAA deals with the protection of personally identifiable information relating to health care. HIPAA applies to "covered entities," which includes health care providers who transmit information in electronic form regarding certain standard transactions (generally related to billing). Many institutions of higher education contain units that are covered entities, and some institutions are covered entities in their entirety.

Payment Card Industry Data Security Standards (PCI-DSS): PCI-DSS is a set of comprehensive requirements for enhancing payment account data security**.**

Personally identifiable information (PII): Any Washtenaw Community College information that is not publicly known and includes tangible and intangible information in all forms, such as information that is observed or orally delivered, or is in electronic form, or is written or in other tangible form.

Security Level: A level (high, medium, or low) assigned to data or IT resource. The security level combines the data security classification (confidentiality) with the need to protect the integrity, and availability of the data. The security level, in combination with the data security classification, is used in the Information Security standards to determine whether a security control is required, recommended, or optional at that level.

Users: Any Washtenaw Community College faculty, staff, students or partner who has been authorized to access any College electronic information resource.

REFERENCES

Request for Policy Exception

REVISION HISTORY

Version	Description	Revision Date	Review Date	Approver
1.0	Initial version	10/11/2018	-	WJO