

Data Classification Policy

Purpose

The Wartburg College Data Classification policy is intended to provide the College with a method to categorize the information collected, stored, and managed by the College community. These data classifications will be used internally and referenced by other policies to improve the College's ability to prevent, deter, detect, respond to, and recover from internal and external compromises to its electronic information resources.

Scope

This policy applies to all persons or entities that have access to College data. It applies to all data utilized by the College community for the purpose of carrying out the institutional mission of research, teaching, outreach, and data used in the execution of required business functions, limited by any overriding contractual or statutory requirements.

Policy Statements

College data are essential to the operations of the College and its quality and safety must be ensured to comply with legal, regulatory, and administrative requirements. Information will be classified according to the risk of unauthorized exposure and the resulting impact. College data shall be classified as Level I (public - low potential impact), Level II (moderate potential impact), or Level III (private - high potential impact).

Unless otherwise classified by a Data Custodian or policy, all College data shall be classified as Level II.

Definitions

AVAILABILITY – A loss of availability is the disruption of access to or use of information or an information system.

CONFIDENTIALITY – A loss of confidentiality, for the purposes of this policy, is the unauthorized disclosure of information.

DATA CUSTODIAN– Data Custodians are senior College officials who have planning, management, and policy-level responsibility for data within their functional areas. A Data Custodian has the authority to authorize or deny access to data. For example, the Registrar, Director of Human Resource, Business Office Controller, Executive Director of Admissions, Department Chairs, Vice Presidents, and the College President would all be Data Custodians. College administrators may act as Data Custodians for departments under their authority.

DATA ELEMENT – A data element is the smallest portion of data contained within a larger document, database, or other electronic record.

INTEGRITY –A loss of integrity is the unauthorized modification or destruction of information.

POTENTIAL IMPACT - The level of adverse effect a loss of confidentiality, integrity, or availability could be expected to have on College operations, College assets, or individuals.

COLLEGE DATA – College data are information that supports the mission and operation of the College. It is a vital asset and is owned by the College. Some College data are shared across multiple units of the College as well as outside entities.

Governing Laws, Regulations, and Standards

Wartburg College is bound by laws and regulations as it relates to the handling of data that is collected, maintained, and used by the institution. Those would include Federal Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), Iowa's Personal Information Security Breach Protection law (Iowa Code Chapter 715C), Payment Card Industry Data Security Standard (PCI DSS), other contractual obligations and any other regulations that may be put into force by federal and state governing authorities. Any changes and/or additions to regulations may override the data definitions below and thus this policy should be reviewed annually for recent changes.

Policy Statements

College data will be classified into three levels, where level I requires the least security and level III requires the highest security.

Data must be consistently protected throughout its life cycle in a manner commensurate with its sensitivity regardless of where it resides or what purpose(s) it serves. Extracts of data shall have the same classification level and utilize the same protective measures as the same data in the system of record.

Data Custodians may utilize the negative potential impacts listed below to evaluate data under their purview if the data does not clearly fall under the laws, regulations, or examples listed. The highest negative impact rating received shall classify data within that category. Data that has no negative impacts to the College but may cause significant harm to individuals must be categorized as Level III.

Level I: Public - Low Potential Impact:

Level I data may or must be open to the general public. This information is not restricted by local, state, national, or international statute regarding disclosure or use. Access is available to the general public but may need to be granted by the Data Custodian.

The loss of confidentiality of Level I data should be expected to have limited adverse effects on College operations, College assets, or individuals. A loss of integrity or availability of Level I data may have limited adverse effects on College operations, College assets, or individuals.

The loss of confidentiality of Level I data may result in some of the following:

1. No loss of mission capability, but inconveniences may be experienced by some individuals
2. No damage to College assets
3. No financial damages and/or fines
4. Insignificant harm to individuals
5. Little, if any, negative impact on the College's reputation

The loss of availability or integrity of Level I data may result in some of the following:

1. Limited degradation in or loss of mission capability to an extent and duration that the College is able to perform its primary functions, but the effectiveness of the functions may be noticeably reduced.
2. No or very minor damage to College assets
3. No direct financial damages and no fines
4. Insignificant indirect financial damages
5. Insignificant harm to individuals
6. Possible negative impact on the College's reputation, generally dependent on the visibility of loss of integrity or availability to the community

Examples include published “white pages,” directory information, maps, departmental websites, lists of email addresses, academic course descriptions, and other information readily published and provided to the public at large.

Level II: Private - Moderate Potential Impact:

Level II data are information whose access must be guarded due to proprietary, ethical, or privacy considerations. This classification applies even though there may not be a statute requiring this protection. This information is not intended for public dissemination, but its disclosure is not restricted by Federal or state law.

Unless otherwise classified by a Data Custodian or policy, all College data shall be classified as Level II.

The loss of confidentiality, integrity, or availability of Level II data should be expected to have moderate adverse effects on College operations, College assets, or individuals.

The loss of confidentiality, integrity, or availability of Level II data may result in some of the following:

1. Limited degradation in or loss of mission capability to an extent and duration that the College is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced.
2. Minor damage to College assets
3. Minor direct financial damages and/or fines
4. Minor indirect financial damages
5. Minor harm to individuals
6. Minor negative impact on the College’s reputation

Examples include student grades maintained by an instructor, class lists, lists of students in a major in a department, internal memos, financial records, email communications, and other documents not intended for public distribution that are not otherwise Level III data.

Level III: Legally Protected - High Potential Impact:

Level III data include all data protected by federal or state law, including, but not limited to FERPA , HIPAA, GLBA, Iowa Code Chapter 715C, PCI DSS and other contractual obligations.

The loss of confidentiality, integrity, or availability of Level III data should be expected to have serious adverse effects on College operations, College assets, or individuals. The loss of confidentiality, integrity, or availability of Level III data may result in some of the following:

1. Severe degradation in or loss of mission capability to an extent and duration that the College is not able to perform one or more of its primary functions
2. Major damage to College assets
3. Major direct financial damages and/or fines
4. Major indirect financial damages
5. Significant harm to individuals
6. Major negative impact on the College’s reputation

Examples include credit card numbers, social security numbers, driver’s license numbers, health records, student transcripts, financial aid data, and human subject research data that identify an individual. Other examples include credentials used as passwords, passphrases, or fingerprints as well as the data stored to allow self-service reset of the credentials.

Intermingling of Data Classifications

Multiple classifications of data may reside together in the same document, database, or electronic record. A document, database, or electronic record containing multiple classifications of data shall be

classified according to the highest level of any single data element contained therein. Adequate redaction or removal of data elements will cause a document, database, or electronic record to be reclassified according to its new contents.

Non-Compliance

Violation of this policy constitutes data misuse and the Wartburg Student Conduct System will govern disciplinary actions for students. Data misuse by employees of Wartburg College may be grounds for disciplinary action, up to and including termination of employment governed by the Wartburg College Faculty Handbook and the Staff Handbook. Violations of this policy are to be referred to the Assistant Vice President for ITS or designee.

Revision History

ITS Review completed Nov 22, 2019

VP EM Review completed Dec 2, 2019

External Review completed Dec 9, 2019

Final Revision Edited Dec 17, 2019

Cabinet Approved January 13, 2020