Ohio Administrative Code

Rule 3344-8-02 Administrative data policy.

Effective: September 11, 2016

(A) Purpose

(1) Information maintained by Cleveland state university is a vital asset that shall be available to all employees who have a legitimate need for it. The university is the owner of all administrative data with individual units or departments having stewardship responsibilities for portions of that data. The university intends that the volume of freely accessible data be as great as possible while recognizing the university's responsibility toward the security of data.

(2) The university expressly forbids the use of administrative data for anything but the conduct of university business. Employees accessing data shall observe requirements for confidentiality and privacy, shall comply with protection and control procedures, and shall accurately present the data in any use.

(3) The university determines levels of access to administrative data according to principles drawn from various sources. State and federal law provides clear description of some types of information to which access shall be restricted.

(4) This policy is for the internal use of information for employees at Cleveland state university. External requests for information are handled in accordance with the Ohio Public Records Act.

(B) Policy

(1) Definition of administrative data

(a) The university's database consists of information critical to the success of the university as a whole. Data may be stored on paper or as digital text, graphics, images, sound, or video. This rule applies to data generated for or by the administrative functions of the university, including (but not limited to) finance, student and enrollment services, and human resources, and to data stores and

systems which access such data, regardless of where it resides, including (but not limited to) servers, desktops, flash drives, cloud services and mobile devices.

(b) Some examples of administrative data include student course grades, employee salary information, vendor payments, and the university's annual fact book. Administrative data do not include personal electronic calendar information, faculty grade books, research data and similar material.

(c) Copies of official data are not official data where they are found on portable storage media, individual hard drives, department servers, or as files on other shared systems. These copies or downloads cannot be used as substitutes for official records kept by the authorized data custodians of the university. However, such information may be used to generate official reports on behalf of the university with the knowledge and permission of the data custodians. Such files and any resulting reports are covered by the same constraints of confidentiality and privacy as the official records.

(d) Prior to the development of a system that will download official records and manipulate them for subsequent update or application to official records, permission shall be obtained from the data custodian for such transfer.

(e) Data custodians shall also authorize any university administrative data captured independent of a university system.

(2) Data classifications and protection

(a) Sensitive information

"Sensitive information" is that data found upon review by the data trustees or general counsel to require restrictions on access. Sensitive information may not be subject to disclosure under the Public Records Act and is only available to CSU employees that have a business or educational need to access the data. Sensitive information is broadly defined as that which the university is legally obligated to protect. For example:

(i) Educational records, as defined by the Family Educational Rights and Privacy Act (FERPA.)

(ii) Health records, as defined by the Health Insurance Portability and Accountability Act (HIPAA.)

(iii) Financial and personnel information, as governed by the Fair Credit Reporting Act (FCRA.)

(iv) Financial information governed by payment card industry standards (PCI-DSS.)

(v) Examples (not all-encompassing):

(a) Class rosters, transcripts, schedules, attendance

(b) Lists of names, addresses, identity numbers, dates of birth

(c) Records of medical care, including psychological counseling

(d) Identification photographs, including archived copies of government issued identification

(e) Account numbers or images of any financial instrument, including credit cards

(f) Pre-employment or routine background check information

(b) Private information

"Private information" is data that the data trustees judge to require special procedures for access. Private information may be subject to disclosure under the Public Records Act and is made available to certain Cleveland state employees based on their job function. Private information is broadly defined as that which should be reasonably protected from inadvertent disclosure beyond authorized Cleveland state university employees. For example:

(i) Data not specifically protected by statute, regulation, or other legal obligation or mandate.

(ii) Shall be protected due to contractual, ethical, or privacy considerations.

(iii) Access, disclosure, or modification could cause financial loss or damage to CSU's property.

(iv) Examples (not all-encompassing)

(a) Directory information of students who have not requested FERPA privacy inclusion

(b) Instructional information such as tests, quizzes, and course shells in a learning management system (LMS)

(c) Proprietary information used to run the business of the university

(c) Public information

"Public information" is all data that is neither restricted, nor judged by data trustees to be sensitive or private. The accessible data volume should be as great as possible to enable those who need the information to have access. Data should be part of an open atmosphere and readily available. Public information is subject to disclosure to all Cleveland state employees as well as the general public under the Ohio Public Records Act. Public information is broadly defined as that which is intentionally displayed for anyone to use, including:

(i) Disclosure is routine, deliberate or required by contract or university policy.

(ii) Can be subject to use restrictions (copyright) but no harm done in disclosure.

(d) Protection of data

(i) Users shall comply with all reasonable protection and control procedures for administrative data to which they have been granted access. Sensitive and private data can never be stored on departmental computers or servers, cd's, thumb drives or any easily transportable medium. All sensitive data shall be stored on secured storage located within the university's data center.

(ii) It is never acceptable to store sensitive data such as grades, social security numbers,

correspondence between student and faculty, classified research, etc., on externally hosted systems, including cloud-based storage systems (includes, but is not limited to, services such as dropbox, google drive, and microsoft onedrive), without a contract that is fully vetted for compliance with university policies. Vendors providing hosted services shall complete the hosting services security checklist.

(iii) Any contract that will provide a third party (e.g. contractors, consultants, service providers, vendors) with sensitive information, or access to Cleveland state university systems or applications that contain sensitive information shall, at a minimum, include the following provisions:

(a) Explicit acknowledgment that the contract allows the contractor access to confidential information

(b) A specific definition of the confidential information being provided

(c) A stipulation that the confidential information shall be held in strict confidence and accessed only for the explicit business purpose outlined in the contract

(d) A guarantee from the contractor that it shall ensure compliance with the protective conditions outlined in the contract

(e) A guarantee from the contractor that it shall protect the confidential information it gets according to commercially acceptable standards and no less rigorously than it protects its own customers' confidential information

(f) A provision allowing for the return or destruction of all confidential information obtained by the contractor on completion of the contract

(g) A stipulation allowing injunctive relief, without posting bond, to prevent or remedy breach of the contract's or contractor's confidentiality obligations

(h) A stipulation that a violation of the contract's protective conditions amounts to a material breach of contract and entitles the university to immediately end the contract without penalty

(i) A provision allowing auditing of the contractor's compliance with the contract's safeguard requirements

(j) A provision ensuring that the contract's protective requirements shall ending the agreement

(3) Data trustees, data custodians and data users

(a) "Data trustees" are senior management personnel (typically at the level of vice president, associate or vice provost, dean, or university director) who have planning and policy-making responsibilities for data in their operational area. The data trustees, as a group, are responsible for overseeing the establishment of data management policies and procedures.

(b) "Data custodians" are managers of functional areas (typically at the level of controller, registrar or director of admissions) who oversee the capture, maintenance, and dissemination of data for a particular operation. Data custodians are responsible for making security decisions regarding access to the data under their charge.

(c) "Data users" are individuals who access university data in order to perform their assigned duties or to fulfill their role in the university community. Data users are responsible for protecting their access privileges and for proper use of the university data they access.

(4) Responsibilities of data trustees, data custodians, and information services and technology

(a) Criteria for determining access

(i) Data custodians are ultimately responsible for assigning access to all types of data on an individual basis; however, general criteria for determining access to both sensitive and private information include the following:

(ii) Human resources/payroll data can be made available as follows:

(a) Personnel in the employee's supervisory chain of authority

(b) Human resources, payroll, and business contacts in departments shall have access to human resources/payroll data for employees in their departments.

(c) Authorized employees of the department of human resources, payroll department, budget office, controller's office, grant accounting, department of audits, the office of general counsel, the office for institutional equity, and the department of law enforcement and safety, shall have access to human resources/payroll data on a case-by-case basis as appropriate for them to perform their job responsibilities. Human resources/payroll data shall be provided on a case by case basis in response to judicial orders or lawfully issued subpoenas.

(d) Legally authorized law enforcement personnel, authorized federal or state agencies, members of duly appointed grievance committees, representatives of authorized accrediting organizations, and agencies processing claims made by the employee for workers' compensation, unemployment insurance or other employee benefits which shall have case-by-case access to the portions of the official personnel files which are appropriate for their business.

(e) To appropriate parties in a health or safety emergency.

(iii) Financial data can be made available as follows:

(a) President, vice presidents, provost, deans, department heads and other personnel with responsibility for the management and oversight of financial resources

(b) Business managers and business office staff in departments.

(c) Authorized employees of business and finance, office of general counsel, division of law enforcement and safety and the department of audits who have a business need to access the data

(iv) Student data can be made available in accordance with FERPA.

(b) Development of access policies and procedures

Each data custodian shall be individually responsible for establishing data access procedures that are unique to a specific information resource or set of data elements

(c) Promotion of accurate interpretation and responsible use

(i) Data trustees shall develop policy to promote the accurate interpretation and responsible use of administrative data.

(ii) Data custodians are responsible for making known the rules and conditions that could affect the accurate presentation of data. Persons who access data are responsible for the accurate presentation of that data.

(iii) Data custodians shall support users in the use and interpretation of administrative data, primarily through documentation, but also in the form of consulting services.

(d) Determination of security requirements

The data custodians, in consultation with information services and technology, shall determine security requirements for administrative data and shall be responsible for monitoring and reviewing security implementation and authorized access.

(e) Establishment of disaster recovery procedures

(i) Information services and technology is ultimately responsible for defining and implementing policies and procedures to assure that data are backed up and recoverable. The data trustees shall play an active role in assisting information systems and technology (IS&T) in this responsibility.

(ii) With the data trustees' advice, IS&T shall develop a workable plan for resuming operations in the event of a disaster, including recovery of data and restoration of needed computer hardware and software.

(f) Responsibilities of information services and technology

(i) IS&T develops and applies standards for the management of institutional data and for ensuring that data are accessible to those who need it.

(ii) IS&T works with the data trustees to establish long-term direction for effectively using information resources to support university goals and objectives.

(iii) IS&T makes institutional data available to authorized users in a manner consistent with established data access rules and decisions. It develops views of data as directed by the data custodians. IS&T and the data custodians ensure that the technical integrity of the data is maintained and that data security requirements are met.

(iv) IS&T and the data custodians ensure that the university community is aware of this policy and the requirements and restrictions it contains.

(5) Requests for access

(a) Sensitive or private data access

Access to sensitive or private data by university employees or employees of university-related foundations requires that a formal request be made to the appropriate data custodian.

(b) Exceptions

All requests for exceptions to data access policies shall be made in writing to the data custodian. E-mail requests are acceptable. The request shall specify the data desired and their intended use.

(c) Denial

The data custodian shall provide a written record of the reason(s) for denial of any access request. E-mail records are acceptable.

(6) Responsibilities of users

(a) Use of administrative data only in the conduct of university business

The university expressly forbids the disclosure of unpublished administrative data or the distribution of such data in any medium, except as required by an employee's job responsibilities and approved in advance by the employees supervisor and the respective data custodian. In this context, disclosure means giving the data to persons not previously authorized to have access to it. The university also forbids the access or use of any administrative data for one's own personal gain or profit, for the personal gain or profit of others, or to satisfy personal curiosity. Users agree to use the information only as described in the request for data access. Failure to do so could result in disciplinary or legal sanctions as set forth in university policy.

(b) Maintenance of confidentiality and privacy

Users shall respect the confidentiality and privacy of individuals whose records they access, observe any ethical restrictions that apply to data to which they have access, and abide by applicable laws and policies with respect to access, use, or disclosure of information. All data users having access to sensitive or private information shall formally acknowledge (by signed statement) their understanding of the level of access provided and their responsibility to maintain the confidentiality of data they access. Each data user shall be responsible for the consequences of any misuse. Users are expressly prohibited from releasing identifiable information to any third party.

(c) Accurate presentation of data

(i) Users shall be responsible for the accurate presentation of administrative data when presenting data on behalf of the university. Users shall be responsible for the consequences of any intentional misrepresentation of that data.

(ii) The office of institutional research (IR) serves as the comprehensive source for data about Cleveland state university. The primary goal of IR is to collect, comprehend, combine, and analyze institutional data pertaining to a range of operational activities. IR assists in the analysis and interpretation of these data to explain past patterns and predict future trends in university performance.

(iii) The office of institutional research shall be the university's clearinghouse for official reports to external agencies including federal and state governments.

(d) Management oversight

(i) All levels of management are responsible for ensuring that all data users within their area of accountability are aware of their responsibilities as defined in this policy. Specifically, managers are responsible for validating the access requirements of their staff according to their job functions, and for insuring a secure office environment. The head of each unit will authenticate the need for individual access to data and shall request and obtain authorization for access to data from the custodian of such data.

(ii) Administrative and academic unit heads are responsible for taking the necessary steps to ensure that data access is terminated for employees who transfer to another department within the university or leave employment of the university.