



## **Administrative Data Policy**

### **PURPOSE**

Information maintained by the University is a vital asset that will 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.

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

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 must be restricted.

This policy is for the internal use of information for employees at the Cleveland State University. External requests for information are handled in accordance with the State of Ohio Public Records Act.

### **POLICY**

#### **1. Definition of Administrative Data**

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.

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.

Copies of official data are NOT official data where they are found on diskettes, 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.

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

Data custodians must also authorize any University administrative data captured independent of a University system.

## **2. Data Trustees, Data Custodians and Data Users**

**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.

**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.

**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.

## **3. Responsibilities of Data Trustees, Data Custodians, and Information Services and Technology**

### **3.1 General Access Data**

General access data are all data that are not either restricted or judged by Data Trustees to be limited-access data. 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 broadly available.

General Access data are subject to disclosure to all Cleveland State employees as well as the general public under the Freedom of Information Act.

### **3.2 Limited Access Data**

Limited access data are data that the Data Trustees judge to require special procedures for access. Limited access data may be subject to disclosure under the Freedom of Information Act. Limited access data are made available to a select group of Cleveland State employees based on their job function.

### 3.3 Sensitive Data

Sensitive data are those data found upon review by the Data Trustees or General Counsel to require restrictions on access. Sensitive data may not be subject to disclosure under the Freedom of Information Act. Sensitive data are only available to CSU employees that have a business or educational need to access the data.

### 3.4 Criteria for Determining Access

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 limited access data include the following:

**HR/Payroll data** can be made available as follows:

- Personnel in the employee's supervisory chain of authority
- Human Resources/Payroll/Business contacts in departments will have access to HR/Payroll data for employees in their departments.
- Authorized employees of the Department of Human Resources, Payroll Department, Budget Office, Controller's Office, Grant Accounting, Internal Audit, the Legal Office, the Office of Equal Opportunity Programs, and the Department of Law Enforcement and Safety, will have access to HR/Payroll data on a case by case basis as appropriate for them to perform their job responsibilities. Similarly, HR/Payroll data will be provided on a case by case basis in response to judicial orders or lawfully issued subpoenas.
- 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 worker's compensation, unemployment insurance or other employee benefits which will have case by case access to the portions of the official personnel files which are appropriate for their business.
- To appropriate parties in a health or safety emergency.

**Financial data** can be made available as follows:

- President, Vice Presidents, Provost, Deans, Department Heads and other Personnel with responsibility for the management and oversight of financial resources
- Business Managers and business office staff in departments.
- Authorized employees of Business and Finance, Office of General Counsel, Division of Law Enforcement and Safety and the Office of Internal Audit who have a business need to access the data

**Student data** can be made available as follows:

- To school officials with legitimate educational interests;  
{A school official is a person employed by the University in an administrative, supervisory, academic or research, or support staff position; a person or company with whom the University has contracted (such as an attorney, auditor, or collection agent); a person serving on the Board of Trustees; or a student

serving on an official committee, such as a disciplinary or grievance committee, or assisting another school official in performing his or her tasks.}

A **school official** has a **legitimate educational interest** if the official needs to review an educational record in order to fulfill his or her professional responsibility.

- To officials of other institutions in which the student seeks or intends to enroll provided that the student had previously requested a release of his/her record;
- To authorized representatives of the U.S. Department of Education, the Comptroller General of the United States, state education authorities, organizations conducting studies for or on behalf of the University, and accrediting organizations;
- In connection with a student's application for, or receipt of, financial aid;
- To comply with a judicial order or lawfully issued subpoena;
- To parents of dependent students as defined by the Internal Revenue Code, Section 152;
- To appropriate parties in a health or safety emergency;

### **3.4 Development of Access Policies and Procedures**

Each Data Custodian will be individually responsible for establishing data access procedures that are unique to a specific information resource or set of data elements. These procedures will ease access and will ensure data security.

### **3.5 Promotion of Accurate Interpretation and Responsible Use**

Data Trustees will develop policy to promote the accurate interpretation and responsible use of administrative data.

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.

Data Custodians will support users in the use and interpretation of administrative data, primarily through documentation, but also in the form of consulting services.

### **3.7 Determination of Security Requirements**

The Data Custodians, in consultation with Information Services and Technology, will determine security requirements for administrative data and will be responsible for monitoring and reviewing security implementation and authorized access.

### **3.8 Establishment of Disaster Recovery Procedures**

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 will play an active role in assisting IS&T in this responsibility.

With the Data Trustees' advice, IS&T will 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.

### **3.9 Responsibilities of Information Services and Technology**

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

IS&T works with the Data Trustees to establish long-term direction for effectively using information resources to support University goals and objectives.

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. The group ensures that the technical integrity of the data is maintained and that data security requirements are met.

## **4. Requests for Access**

### **4.1 Restricted or Limited-Access Data**

Access to sensitive or limited-access data by University employees or employees of University-related foundations requires that a formal request be made to the appropriate Data Custodian.

### **4.2 Exceptions**

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

### **4.3 Denial**

The Data Custodian must provide a written record of the reasons for denial of any access request. E-mail records are acceptable.

## **5. Responsibilities of Users**

### **5.1 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 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.

## **5.2 Maintenance of confidentiality and privacy**

Users will 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 limited-access data will 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 will be responsible for the consequences of any misuse. Users are expressly prohibited from releasing identifiable information to any third party.

## **5.3 Protection of data**

Users will comply with all reasonable protection and control procedures for administrative data to which they have been granted access. Sensitive data can never be stored on departmental computers or servers. Sensitive data can never be stored on diskettes, cd's, jump drives or any easily transportable medium. All sensitive data must be stored on secured storage located within the University's data center.

## **5.4 Accurate presentation of data**

Users will be responsible for the accurate presentation of administrative data, and will be responsible for the consequences of any intentional misrepresentation of that data.

The Office of Institutional Research shall be the University's clearinghouse for official reports to external agencies including federal and state governments.

## **5.5 Management Oversight**

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 must request and obtain authorization for access to data from the custodian of such data.

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.

## 6. Appendix A – Data Trustees

<b>Cleveland State University Data Trustees</b>	
Payroll Data	Vice President for Business Affairs and Finance
Financial Data	Vice President for Business Affairs and Finance
Facilities Data	Vice President for Business Affairs and Finance
Human Resources Data	Vice President for Business Affairs and Finance
Library Data	Director, University Library / Director, Law Library
Development Data	Vice President for University Advancement
Admissions Data - Graduate, Law, International	Provost and Senior Vice President for Academic Affairs
Admissions Data - Undergraduate	Vice President for Administration
Alumni Data	Vice President for University Advancement
Financial Aid Data	Vice President for Administration
Student Data	Provost and Vice Provost for Academic Affairs
Student Medical Data Student Counseling Data Student Housing Data Student Discipline Data	Provost and Vice Provost for Academic Affairs
Student Advisement Data	Provost and Vice Provost for Academic Affairs
Course Data	Provost and Vice Provost for Academic Affairs
Faculty Data	Provost and Vice Provost for Academic Affairs
Communications Data	Vice President for Administration

## 7. Appendix B – Data Custodians

<b>Cleveland State University Data Custodians</b>	
Financial Data Payroll Data	Controller Director of Accounting Services Director of Financial Services/Bursar
Human Resources Data	Director of Salary Administration & HR Systems
Development Data	Senior Director, Advancement Administration Senior Director, Advancement Services
Admissions Data	Director , Undergraduate Admissions Director, Graduate Admissions Director of Enrollment Services and Registrar, School of Medicine
Alumni Data	Senior Director, Advancement Administration Senior Director, Advancement Services
Financial Aid Data	Director, Student Financial Aid and Scholarships Regional Financial Aid Officers
Student Data	University Registrar Director of Financial Services/Bursar Director, Student Health Services Director, Counseling and Human Development Centers Director, Graduate Admissions
Course Data	University Registrar Senior Associate Registrar
Faculty Instruction Data	University Registrar Senior Associate Registrar
Communications Data	Vice President for Information Services

## 8. Appendix C – Sensitive Data

**NOTE:** The following lists of sensitive data are provided as a general guide and **DO NOT** constitute a complete and comprehensive list of all university sensitive data.

### Human Resources/Payroll Data

Restricted	Limited Access
<ul style="list-style-type: none"> <li>• Medical</li> <li>• Garnishments</li> <li>• Benefits</li> </ul> <p>Personal Nature:</p> <ul style="list-style-type: none"> <li>• Handicapped / disability status</li> <li>• Home/Mailing Address</li> <li>• Home Phone</li> <li>• Date of Birth</li> <li>• Social Security Number</li> <li>• Marital Status</li> </ul>	<p>Personal Nature:</p> <ul style="list-style-type: none"> <li>• Education</li> </ul>
<ul style="list-style-type: none"> <li>• Total Compensation</li> </ul>	<p>Total Compensation (as defined under FOI)</p>
<p>Performance</p> <ul style="list-style-type: none"> <li>• Review Rating</li> <li>• Review Date</li> <li>• Pay for Performance</li> </ul>	
<ul style="list-style-type: none"> <li>• Salary History/Employment History</li> </ul>	<p>Salary History/Employment History (as defined under FOI)</p>
<p>Basic Information:</p> <ul style="list-style-type: none"> <li>• Emergency Contact &amp; Phone</li> <li>• Leave Balances</li> <li>• Training Records</li> </ul>	<p>Basic Information:</p> <ul style="list-style-type: none"> <li>• State Service Date</li> <li>• Leave Base Date</li> <li>• Class/Slot</li> <li>• Exempt/Non-exempt status</li> <li>• Salary Band</li> </ul>

<ul style="list-style-type: none"> <li>Employee Disciplinary Records</li> </ul>	<p>Basic Faculty Data:</p> <ul style="list-style-type: none"> <li>Tenure Status</li> <li>Tenure Date</li> <li>Tenure Department</li> <li>Date on Tenure Track</li> <li>Date of Rank</li> <li>CIP of Degree</li> </ul>
<ul style="list-style-type: none"> <li>E-mail files concerning or created by an employee</li> </ul>	<ul style="list-style-type: none"> <li>Accounting Information/FTE</li> </ul>
<ul style="list-style-type: none"> <li>Employee ID Photographs</li> </ul>	<ul style="list-style-type: none"> <li>Supervisor (Name, Class, Slot)</li> </ul>

### Student Data

Restricted	Limited Access
<p>Personally identifiable student data not designated as Directory Information:</p> <ul style="list-style-type: none"> <li>Student identification (usually Social Security Number)</li> <li>Admissions data</li> <li>Financial aid data</li> <li>Student enrollment data, including student course schedule and grades</li> <li>Student accounts data</li> <li>Student disciplinary records</li> <li>Student employment records (if employment is contingent upon enrollment)</li> <li>E-mail files concerning or created by a student</li> <li>Student ID photograph</li> <li>Student medical and counseling data</li> <li>Student advisement data</li> </ul>	<p>Faculty Instruction Data</p>

## Financial Data

Restricted	Limited Access
<ul style="list-style-type: none"><li>• Donor Information (if donor requested that privacy be maintained)</li></ul>	<ul style="list-style-type: none"><li>• All financial data</li></ul>

## **REVISION HISTORY**

Revised: