Information Sensitivity Policy

Date: 05/01/06	**Policy ID:** UVAW-3	**Status:** Approved

Contact Office: Office of Information Technology

Oversight Executive: Director of Information Technology

Applies to: All UVa-Wise users

Reason for Policy: Information maintained by the University of Virginia's College at Wise is a vital asset that will be available to all employees who have a legitimate need for it, consistent with the College's responsibility to preserve and protect such information by all appropriate means. The College is the owner of all administrative data; individual units or department may have stewardship responsibilities for portions of that data.

The value of data as an institutional resource is increased through its widespread and appropriate use; its value is diminished through misuse, misinterpretation, unnecessary restrictions to its access, or failure to maintain quality. The College expressly forbids the use of administrative data for anything but the conduct of College 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. In addition, the College and its employees do comply with applicable state and federal laws and regulations, including state ITRM standards and guidelines.

The College 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. In an academic community, ethical considerations are another important factor in determining access to administrative data (see Appendix A).

Questions about these guidelines should be addressed to the IT Security and Policy Coordinator.

Definitions: Access (to data): Either (a) the capacity for data processors to enter, modify or delete data or (b) the capacity for data users to view, copy or download data.

Categories (of data): See Appendix A

General administrative – see Appendix A
Legally restricted – see Appendix A

Limited-access – see Appendix A

Domain (of data): The entire collection of data for which a College employee functioning as a data steward or data security contact (see roles in Appendix B) is responsible. The data domain also includes rules and processes related to the data.

Quality (of data): In this context, quality is a collective characteristic that encompasses utility, objectivity, integrity, accuracy and completeness. Data quality is supported by presentation in an accurate, clear, complete, and unbiased manner, with sources identified in appropriate fashion, with potential sources of error identified, and with disclosure of the degree to which the data has been protected from unauthorized access or revision, from compromise through corruption, and from falsification.

Roles and Responsibilities: See Appendix B

Policy Statement:

All UVa-Wise information is categorized into three main classifications (see Appendix A):

- General administrative
- Legally restricted
- Limited access

The University of Virginia's College at Wise subscribes to restricting access to "sensitive data", including legally restricted and limited access, to only those employees with a legitimate need-to-know and denying access either implicitly or explicitly to all others. UVa-Wise personnel are encouraged to use common sense judgment in securing the College's administrative data to the proper extent. The College's administrative data consists of information critical to the success of the College as a whole. This data may be unit/department specific, UVa-Wise specific and/or part of a larger database i.e. at the University of Virginia. Specific types of data, such as research data and electronic mail "boxes," may be covered by additional specially tailored policies.

Data may be digital text, graphics, images, sound, or video. The College regards data that are maintained in support of a functional unit's operation as part of the College's administrative data if they meet at least one of the following criteria:

- If at least two administrative operations of the College use the data and consider the data essential;
- If integration of related information requires the data;
- If the College must ensure the quality of the data to comply with legal and administrative requirements for supporting statistical and historical information externally;

- If a broad cross section of College employees refers to or maintains the data; or
- If the College need the data to plan.

Some examples of administrative data include student course grades, employee salary information, vendor payments, and the College's web site. Administrative data does not include personal electronic calendar information and similar material.

If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their supervisor for further clarification.

As part of their job, College employees take on various roles and responsibilities (see Appendix B) with respect to College administrative data. Under the guidance of various College leaders, especially the chief information officer of the College, individuals may fill the roles of data stewards, data security contacts, data users, data processors, and system sponsors. In addition, various individuals and groups provide data-related services, especially the agency information security officers, data administrators, and data security administrators in the Office of Information Technology.

Procedures: Requests for Access to College Administrative Data

1.1 Legally Restricted or Limited-Access Data

Access to legally restricted or limited-access data (for definitions of the three categories of College administrative data, see Appendix A) by College employees, employees of College-related foundations, or non-UVa-Wise employees sponsored by a College manager requires that a formal request be made to the appropriate data security contact.

1.2 Exceptions

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

1.3 Denial

The data security contact must provide a written record of the reasons for denial of any request to access College administrative data. E-mail records are acceptable.

1.4 Appeal

Members of the College community may appeal any decision that denies access to College administrative data. Appeals may be made to the appropriate data steward.

2.0 Responsibilities of Data Users

2.1 Use of administrative data only in the conduct of College business

The College 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 steward. In this context, disclosure means giving the data to persons not previously authorized to have any type of access to it. The College also forbids the 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.

2.2 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 they access, and abide by applicable laws and policies with respect to accessing, using, or disclosing information. All data users having any access to legally restricted or limited-access data will formally acknowledge (by signed statement or some other means) their understanding of the level of access provided and their responsibility to maintain the confidentiality of data. Each data user will be responsible for the consequences of any misuse.

2.3 Protection of data

Users will comply with all reasonable protection and control procedures for administrative data to which they have been granted the ability to view, copy or download.

2.4 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.

2.5 Maintenance of data quality

Users are responsible for notifying data stewards or data security contacts when they recognize that data is in error, incomplete, obsolete or missing.

This policy has been taken, with permission, from the University of Virginia in whole or in part and may have been modified to better meet the needs and infrastructure of the University of Virginia's College at Wise. The University of Virginia's policy can been found at http://www.itc.virginia.edu/policy/itcadminnew.htm#5.0

Related Information:

Appendix A – Definitions and Examples of Administrative Data Categories
Appendix B – Roles and Responsibilities Related to College Administrative Data

Background: Approved by Brian Ward, CIO – UVa-Wise, June 2, 2006
