Davidson College
Administrative Data Security Policy

Prepared by:

Information Technology Services

May 2007

TABLE OF CONTENTS

Introduction

This document details the Data Security Policy, which governs the handling, dissemination, and protection of Davidson College's administrative data. Administrative data is any data that support the functions of the college and is non-instructional in nature. Administrative data resides in applications like Banner, One Card, and Kronos.

Administrative data and applications are valuable assets which the college has an obligation to manage, secure and protect. All administrative data that reside on computers both within ITS and around campus, data as paper hard copy, and data on electronic media to include but not limited to diskette, CD-ROM, USB Removable Media (Thumb Drive, Flash Drive, Memory Stick), and DVD are governed by this document.

Audience

This document is intended for use by all individuals, staff, faculty, or employed students, given access to Davidson College's administrative data. Other users (consultants, volunteers, etc.) given special permission must also review and adhere to the statements outlined within this document.

College Responsibilities

Electronic information at Davidson College is stored on central servers and on individual desktop computers. This networked environment poses significant risk to the security of information. Protecting this college resource is a shared responsibility between Information Technology Services (ITS) and the individual users of that information. Network security, including firewall technology, has been implemented to protect central servers and the campus network.

Due to current threats that exist from unauthorized access to administrative data, state and federal privacy and security related laws have been enacted to protect both individuals and institutions of higher education. The college must comply with a combination of federal and state regulations as well as by accrediting organization standards. Those that are known to be applicable at Davidson are as follows:

- Family Educational Rights and Privacy Act of 1974 (FERPA)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Electronic Communication Privacy Act (ECPA)
- Gramm-Leach-Bliley Act of 2000 (GLB)

To meet these obligations, the college must routinely assess information security vulnerabilities and risks. The college must also continuously review its policies and procedures in which access to sensitive information is managed and permitted. The college must secure and control access to administrative data.

Data Classification

Administrative data owned, used, created or maintained by the college is classified into the following three categories:

1. Confidential
2. Official Use ONLY
3. Public

Confidential data may be protected by federal and state regulations and are intended for use only by individuals who required that information in the course of performing their college functions. If confidential data are to be accessed across multiple functional areas or college-wide, the appropriate Senior Staff member must authorize access.

Examples of confidential data include but are not limited to:

- Employee data - includes EEO data, salary data, termination/disability data, appointment data, non-salary related benefits, biographical data, and salary survey results
- Faculty data - includes instructor evaluation data
- Student data - financial aid data, parents' financial data, student accounts receivable data, students' grade data, biographical and academic data
- Financial data - financial data by operating unit
- Alumni and Friends data - gift and pledge data, financial data, employment data, biographical data

Confidential data must be treated as completely confidential and should not be discussed or disclosed with others, except in the course of performing one's college function.

Official Use Only data is information that must be guarded due to proprietary, ethical, or privacy considerations, and must be protected from unauthorized access, modification, transmission, storage or other use. This classification applies even though there may not be a civil statute requiring this protection. Official Use Only Data is information that is restricted to members of the college community who have a legitimate purpose for accessing such data.

Examples of confidential data include but are not limited to:

- college partner or sponsor information where no more restrictive confidentiality agreement exists
- Internal telephone books and directories

Public data is information that may or must be open to the general public. It is defined as information with no existing local, national or international legal restrictions on access or usage. Public data, while subject to the College disclosure rules, is available to all members of the college community and to all individual or entities external to the college community.

Examples of public data include but are not limited to:

- Publicly posted press releases
- Publicly posted college events
- Publicly available college maps, newsletters, newspapers, and magazines
- Data accessible through the Davidson College Web site

Data and Application Security

Each administrative department shall designate a Data Custodian, typically the head of the department, who is responsible for administrative data and specific administrative applications in his/her functional area. The Data Custodian's specific responsibilities may include:

- Review and approval of all requests for access to and update capability for specific administrative data and applications
- Ensuring that departmental use of administrative data is consistent with existing college policies
- Ensuring that administrative systems which are not managed by Information Technology Services (ITS) are secured and protected from unauthorized use, improper disclosure, accidental alteration, and that such systems are properly maintained and backed up.

Although some of the responsibilities of the Data Custodian may be delegated to others in his/her functional area, the Data Custodian continues to have overall accountability for the use and security of the data.

Requesting Authorization for Access

Requests for access to administrative data should be submitted in writing to the ITS Help Desk. Only access to the specific applications and data related to the employee's specific college responsibilities should be requested.

Before a user can be given an account, the Data Custodian or his/her designee must review and approve the request. No user outside of ITS will be given administrator level access or access to power user accounts.

If the individual requires access to a system that is not supported and maintained by IT, he/she must request and receive written permission from the Data Custodian of that system.

Termination or Change of Status of Employees

Administrative Department Heads and Academic Department Chairs are responsible for informing the Human Resources (HR) Office, of an employee's change in status or termination. Changes in status may include leaves of absence, significant changes in position responsibilities or transfer to another department. The HR Office is responsible for making a record of the change in status and notifying the appropriate organizations, including Information Technology Services.

Information Technology Services is then responsible for modifying or terminating the employee's access to administrative data.

Distributing Administrative Information - Data Extraction

Extraction/downloading of institutional data for processing on systems other than the central administrative systems should be done with the permission of the Data Custodian and only if the confidentiality, integrity and accuracy of the data and downloaded data can be ensured. Desktop and laptop computers provide the most vulnerable point of access to administrative information. Staff must physically protect their computers from unauthorized access and theft.

Data extraction is to be done only by individuals who have been given specific rights by the Database Administrator and the Data Custodian to do so. Requests for rights are handled in the same manner as requesting access to data and applications.

Extracted data are the responsibility of the user and must be secured. Data should not be extracted for purposes that duplicate data entry or processing done on the administrative system.

Requests for data extraction are to be evaluated based on guidelines determined by the Data Custodian.

Maintaining Confidentiality

It is the responsibility of the Data Custodian to ensure that all individuals who are given access to restricted or sensitive data are instructed about their confidential nature. The Data Custodian is also responsible for conveying the status and level of confidentiality of the data.

Unauthorized release of sensitive or restricted information is a breach of data security and is cause for disciplinary action, which includes the possibility of dismissal.

Reviewing Data Security Configurations

On a semi-annual basis, users' access and controls to administrative data, specifically Banner, are reviewed. Each member of the Banner Team Leaders (BTLs) is assigned one or more Banner Security Classes to review. The BTL is responsible for identifying any user account that should be removed from the user class that he/she is reviewing, identifying any user classes that should be redefined, and identifying any new user classes. Each member documents his/her information and stores the resulting document in a secure file share on the network.

At the end of the semi-annual review, the ITS Banner Support team is responsible for reviewing the changes identified by the Banner Team Leaders and updating the privileges of the users accordingly using the security utilities within Banner.

Reporting Data Security Breaches

Should someone become aware of or see possible breaches in data or computer security, he/she is required to report all such occurrences to the Executive Director of ITS and the Data Custodian. The security breach will be referred to the appropriate Senior Staff person.

Data security breaches include, but are not limited to: the distribution of login credentials to other individuals, neglecting to log off systems when away from workstations, inappropriate dissemination of sensitive or restricted data, and accessing, using, or changing data that are not necessary to perform the individual's college functions or for which the individual has not received written permission from the Data Custodian.

Unauthorized or inappropriate use of data and applications or lack of adherence to security policies and procedures carries serious consequences and may result in disciplinary action, which is not limited to termination of employment.

Appendix A – Guidelines for Data Handling

Storing Data on Laptop Computers

Confidential data should not be stored on laptop computers. All confidential data should remain within the Administrative Application or on a secure network drive. Users that travel and/or work in remote locations can request VPN access through the ITS Help Desk to access this information. VPN uses encryption and other security mechanisms to ensure that only authorized users can access the college network and that the data being accessed cannot be intercepted.

Securing Hard Copy Media

All hard copy media containing confidential data when not attended or in use, at a minimum, should be kept in a secure location such as a locked drawer or file cabinet.

Destroying Hard Copy Media

Paper shredders can be used to destroy flexible media such as paper and diskettes, once the media are physically removed from their outer containers. The shred size of the shredder should be small enough that there is reasonable assurance that the data cannot be reconstructed.

Each office that is responsible for handling administrative data should have a shredder. Each individual should shred all extraneous media containing confidential information. For bulk shredding, the office should use the shredding service provided by the college.

Sharing Data with External Entities

When working with an external organization, at a minimum, the Data Custodian must request a copy of the organization’s written privacy procedures that describe, among other things, who has access to protected information, how such information will be used, and when the information may be disclosed.

Release of Enrollment Data to Public Sources

Any questions relating to the release of enrollment data should be directed to the Office of Planning and Institutional Research. The Office of Planning and Institutional Research has an established annual census date on which enrollment data from the Registrar’s Office is frozen. The use of the specific census date for finalizing enrollment data is standard practice at colleges and universities, enabling the college to report data to federal and state agencies, to consortia with which we share data, and to publications that make our data available to prospective students and other interested parties. Individuals outside of the Office of Planning and Institutional Research are not authorized to report this information and should not do so under any circumstance.

Appendix B - State and Federal Regulations

Family Educational Rights and Privacy Act of 1974 (FERPA)

FERPA is the keystone federal privacy law for educational institutions. FERPA imposes confidentiality rules and regulations around student educational records, prohibiting institutions from disclosing “personally identifiable education information” such as grades or financial aid information, without the students written permission.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

HIPAA was enacted to protect the rights of patients and participants in certain health plans. Colleges and universities that are affiliated with health care providers are considered entities that must adhere to HIPPA. As a result institutions must provide written notice of their affiliated health care provider’s electronic information practices. HIPAA generally requires covered entities to (i) adopt written privacy procedures that describe, among other things, who has access to protected information, how such information will be used, and when the information may be disclosed; (ii) require their business associates to protect the privacy of health information; (iii) train their employees in their privacy policies and procedures; (iv) take steps to protect against unauthorized disclosure of personal health records; and (v) designate an individual to be responsible for ensuring the procedures are followed.

Electronic Communication Privacy Act (ECPA)

Unlike FERPA and HIPAA, which are specific to certain types of entities, the ECPA broadly prohibits the unauthorized use or interception by any person of the contents of any wire, oral or electronic communication. More specifically, the ECPA imposes liability on any person who intentionally accesses without authorization a facility through which an electronic communication service (email or computer network) is provided, or exceeds an authorization to access that facility, if that person thereby obtains, alters or prevents authorized access to a wire or electronic communication while it is in electronic storage.

GRAMM-LEACH-BLILEY ACT OF 2000 (GLB)

The GLBA, enacted in 1999, is applicable to financial institutions, including colleges and universities, and creates obligations to protect customer financial information. The GLBA includes requirements to take steps to ensure the security of personally identifying information of financial institution customers, such as names, addresses, account and credit information, and Social Security numbers.

Appendix C – Data Custodians

Each administrative department must designate a Data Custodian, typically the head of the department, who is responsible for administrative data and specific administrative applications in his/her functional area. As there is no direct correlation between administrative office and the modules within the Administrative System, a Data Custodian can and will in most cases share the responsibility over a functional area. For example, the data custodian for Admissions and the data custodian for the Registrar's Office will be responsible for collectively managing Student Data. Below are the designated Data Custodians.

Hansford Epes, Office of the Registrar – Student Data

Marcia Stoutjesdyk, Office of the Registrar – Student Data

Kim Ball, Human Resources – Employee/Personnel Data

Alan Chester, Office of Admission and Financial Aid – Student Data

Eileen Keeley, College Relations – Alumni/Development Data

Ellen Henshaw, College Relations – Alumni/Development Data

Lori Gaston, Business Services – Financial Data

Lacrissa Barrett, Physical Plant – Financial Data

TBD, Student Life