Bethany Lutheran College, Inc.
ADMINISTRATIVE DATA POLICY

Purpose and Scope

The College's administrative data and applications are a valuable resource, vital to the performance of College functions and fulfillment of responsibilities. The College must therefore ensure that this resource is properly managed, used, protected, and controlled.

This policy defines the security and protection requirements for administrative data and applications residing on College computing systems and is accessible by College employees and faculty. This policy also details the rights and responsibilities of College personnel in the handling, dissemination, security, and protection of the College's data and applications.

Administrative data and applications reside on all computers used for administrative purposes including laptops/notebooks that are maintained and supported by the ITS department. Data on other media such as paper hard copy, diskettes, and other technologies are also considered administrative data. This data policy applies to all administrative data.

Access to administrative data, whether current or archived at the College, is provided to those individuals who, in the course of performing their College responsibilities and functions, must use specified data. Determined by the requirements of their jobs on a "need to know" basis, access to administrative data and applications will be granted to College employees, whether staff or faculty.

With special permission, a faculty or staff member may access specific data for special College projects with the written permission from the Registrar office (student related) or Manager of Human Resources (employee related) under appropriate supervision.

Unauthorized or inappropriate use of the data and applications, or lack of adherence to security policies and procedures will not be tolerated and will result in disciplinary action, which may include termination of employment.

Sensitive Data versus Non-Sensitive Data

Data belongs to the College as an institution and not to any particular function, department, unit or individual. Data is available to any staff or faculty member who demonstrates a "need to know" relevance as it relates to the performance of his/her job.

Data has varying levels of sensitivity. There are three categories of administrative data: public, campus-wide (Directory Information), and restricted/sensitive.

Public Data

Public data is defined as data that is available or distributed to the general public regularly or by special request. Public data includes the following:

1. Employee name and Title;
2. Department and employment dates;
3. Names, Degrees, and majors of graduating seniors;
4. Annual Financial Reports;
5. Admissions Summary Reports; and,
6. Bethany Lutheran College Catalog.

Campus-Wide Data (Directory Information)

Campus-wide data are those which are typically found in the College's directory or the Alumni directory and thus are sometimes referred to as directory information.

For students, the data include:

1. Name, classification, on-campus housing information.
2. Class Year,
3. Major Field of study;
4. Dates of attendance at the College;
5. Degree, Honors and Awards received; and,
6. Home address and phone numbers (unless the student requests that home info be suppressed).

For employees, the data include:

1. Name and Title;
2. Department, work phone and e-mail address;
3. Dates of employment; and
4. Home address and phone (unless the employee requests that home info be suppressed).

Restricted/Sensitive Data

Restricted/sensitive data may be protected by federal and state regulations and are intended for use only by individuals who require that information in the course of performing their College functions. Employees are required to sign a Confidentiality Agreement before they can have access to restricted/sensitive data. If restricted data is to be accessed across multiple functional areas or College-wide, the appropriate senior administrator must authorize access.

Examples of restricted/sensitive data include (not a complete list):

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

Restricted/sensitive data must be treated as completely confidential and should not be discussed with others, except in the course of performing one's College function.

Requesting Authorization for Access to Administrative Data

Requests for access to administrative data should be submitted in writing to the Manager of Administrative Computing in the ITS department with their supervisors approval.

Only access to the specific applications and data related to the employee's specific College responsibilities should be requested. If an employee requires access to a system that is not supported and maintained by the ITS department, he/she must request and receive written permission from the department head in which that system is housed.

New Hire, Termination, or Change of Status of Employees

The Human Resource department is responsible for informing the Manager of Administrative Computing of an employee's hire, change, or termination (if possible, preferably prior to the event). This individual will share the necessary information with the rest of the ITS staff.

Maintaining Confidentiality of College Data

It is the responsibility of the department manager to ensure that all individuals who are given access to restricted or sensitive data are instructed about their confidential nature. The person producing the data for dissemination is responsible for conveying the status and level of confidentiality when the data is distributed.

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.

Reporting Data Security Breaches

Should you be aware of or see possible breaches in data or computer security, you are required to report all such occurrences to the ITS department. The security breach will be referred to the appropriate senior administrator.

Data security breaches include, but are not limited to:

- The distribution of login Ids and passwords to other individuals;
- Neglecting to lock computer systems when away from workstations;
- Inappropriate dissemination of sensitive or restricted data; and,
- Accessing, using, or changing data that is not necessary to perform the individual's College functions or for which the individual has not received written permission from the Data Owner. The Data Owner is the person responsible for maintaining the data while the constituent is in a certain role. For example, while a constituent is a student, the Registrar’s office is the Data Owner. Human Resources would be the Data Owner for employee information.)

Unauthorized or inappropriate use of data and applications or lack of adherence to security policies and procedures will not be tolerated and may result in disciplinary action, which may include termination of employment.