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.

Bethany Lutheran College, Inc.

DATA MODIFICATION POLICY

Purpose and Scope

Bethany Lutheran College's (BLC) recognizes the need to update data that exists within a database. Reasons for this include updating incorrect data, adding data, or removing unnecessary or incorrect data. The best method for doing this is to have end users modify the records using the appropriate software application. However, there are times when this is not possible or when it is not feasible (due to the number of records involved). When this is the case, a script or trigger will be written to modify the data.

Only BLC's Information Technology Services (ITS) department has security rights to create and execute scripts or triggers that will directly update a database. As part of their jobs, the ITS staff is trained in using such tools.

Procedure

Request / Approval for Data Modification

In order to create scripts or triggers, a formal request submitted to ITS will be required as documentation. If the modification being requested impacts multiple departments or offices, discussions should convene so all who are impacted are in agreement of the change.

See Data Modification Request Form and Data Modification Request Form instructions.

Testing of Data Modification

All scripts and triggers must be tested in a test environment and reviewed by the requestor to ensure results are what are expected. Approval of the results is required prior to ITS executing them on a live database.

Implementation of Data Modification

Once approvals of the tested modification are received, ITS will work with the requestor to schedule the actual modification to the live database in order to minimize the impact on the end-users.

Notification of Final Data Modification

ITS will notify all departments or offices of the update once it has been made.

Version/Change Log

ITS will be responsible for maintaining documentation of the request and any supporting documentation.

Enforcement

Anyone found to have violated this policy may be subject to appropriate disciplinary action.

Bethany Lutheran College, Inc.
CHANGE MANAGEMENT POLICY

Purpose and Scope

The purpose of this policy is to provide an orderly and documented method in which changes to the College's technology environment are made.

This policy applies to all Bethany Lutheran College Information Technology Services (ITS) staff members.

This policy applies to any type of change, upgrade, or modification that might affect IT resources upon which College students and staff rely. This includes, but is not limited to, the following:

1. Hardware upgrades or additions,
2. Infrastructure changes,
3. Preventative maintenance,
4. Security patches,
5. Software upgrades, updates, or additions, and
6. System architecture and configuration changes.

Responsibility

The responsibility for enforcing this policy lies with the Director of Technology.

Planned Changes

Requested changes to a College ITS resource must be communicated to a member of the ITS department who will in turn share the request with appropriate members of the ITS department for discussion, planning and approval or denial of the request. In the event that an objection to a change cannot be resolved informally, the Director of Information Technology Services (or an appointed designee) will call a meeting of all involved parties to resolve the dispute.

Communications about potential changes can be made by email but must include the following information:

1. A detailed description of the change needed, including who will be responsible for testing and approving the change before the final implementation.
2. Reason for the change.
3. The estimated date for when the change needs to be complete.
4. List of other departments that may be impacted by the requested change and the name of personnel in those departments that have approved the change be implemented.

ITS will be responsible for maintaining documentation of the request and any supporting documentation.

Emergencies

A technological emergency exists when:

1. a business critical component of the College's technology is inoperable and preventing a time-sensitive or mission critical task from being completed,
2. data is providing errant information, or
3. a disaster has occurred.

All emergencies will be handled on a case-by-case basis with the approval of the Director of Information Technology Services or an appointed designee. In any case, the following guidelines must be followed:

- Written approval must be obtained to execute the change. If verbal approval is given, it must be documented by the ITS resource in charge of the change.
- College students and/or staff affected by the emergency will be notified as soon as possible.
- ITS will be responsible for all documentation of the emergency and it's solution.

Bethany Lutheran College, Inc.

CODE MIGRATION POLICY

Purpose and Scope

The College's data and software applications are valuable resources, vital to the College functions and fulfillment of responsibilities. To ensure these resources are appropriately managed and protected, the College has limited the personnel who are able to migrate code. Though some individuals have the necessary security permissions, they may not be authorized to promote code into production.

The scope of this policy covers three main system applications: PowerFaids, Kronos, and Jenzabar EX.

List of personnel who have the security ability to migrate code

- Manager of Administrative Systems – Lisa Shubert
- Computer Systems Specialist – Ellen Bartscher
- Manager of Network Systems – Todd Marzinske
- Programmer – Jon Marozick
- Information Technology Specialist – Jon Moeller

List of staff that is authorized to migrate code

Because each person in the ITS department fulfills multiple roles, authorization to migrate code is granted to more than one person. Those who are authorized must follow both the Change Management Policy as well as the Data Modification Policy when migrating code. John Sehloff, Director of Information Technology Services, has the ability to change this listing if currently authorized staff is not available to do so.

PowerFAIDS application and data

Per our contract with he vendor for PowerFaids we are not allowed to customize their database. If the College would customize it, we forfeit support regarding PowerFaids. For that reason, the only updates that should be made to the PowerFAIDS database should be scripts provided by the College Board or by its updates to the PowerFAIDS application. Updates should be performed by the following authorized personnel.

- Manager of Network Services,
- Manager of Administrative Computing
- Software Vendor (may be granted direct access to the database for support cases and certain updates)

Kronos application and data

Although the Kronos database is not as proprietary as the PowerFAIDS database, the authorization to migrate code is similar. Customized code is not to be introduced into the Kronos database except as provided by Kronos. Updates should be performed by the following authorized personnel.

- Manager of Network Services
- Manager of Administrative Computing
- Software Vendor (may be granted direct access to the database for support cases and certain updates)

Jenzabar EX application and data

The EX database is designed to be customized so that it can adapt to the particular needs of the college. For this reason, code will be migrated more often in this database and by more people. The actual changes may be performed by the following authorized personnel.

- Manager of Administrative Systems,
- Computer Systems Specialist
- Manager of Network Services
- Programmer
- Software Vendor (may be granted direct access to the database for support cases and certain updates)

Bethany Lutheran College, Inc.

COMPUTER DETERMINATION POLICY

Purpose and Scope

Bethany Lutheran College is committed to providing appropriate computer equipment essential to the function of a person's position in a manner which:

1. Promotes the proper stewardship of assets (cost of maintenance and acquisition of computer)
2. Complies with IRS, federal, state and college regulatory requirements
3. Establishes a framework for consistent decision-making and equity among all employees
4. Reduces or eliminates administrative costs whenever possible

Computers can offer efficiency for College employees in the performance of their duties. This policy applies to all employees who use a computer to perform their job. The type of computer (laptop or pc) is determined by job function and past practices of the institution. While job duties change over the course of time, an employee must make a case to his or her supervisor to deviate from the normal assignment of computers to employees by the Director of Information Technology Services.

Request for Different Computer

The use of a computer by an employee for college business is for the benefit of the College in the furtherance of its mission, not for the convenience of the employee. If a supervisor determines that a different computer is needed, a request will be submitted to his or her appropriate senior administrator who will in turn submit the request to the Chief Financial and Administrative Officer and together, they will approve or reject such request.

A valid request is defined as follows:

- The need to have accessible to information that is essential to the performance of their job due to frequent travel throughout the year
- The employee works at a remote location throughout the year, and data collection and processing is unobtainable through other means

Bethany Lutheran College, Inc.

DATA CENTER PHYSICAL ACCESS POLICY

Purpose and Scope

Physical access to the server room is limited to those individuals who maintain the equipment housed in that room. Those people include

- Superintendent of Buildings who maintains keys and locks for the entire campus,
- Director of Information Technology Services who works with the door access server and is the backup for the data network,
- Manager of Network Systems who maintains the servers and the data network,
- Manager of Academic Computing who maintains the Macintosh servers,
- Information Technology Specialist who serves as the backup for maintaining the Windows servers, and
- Director of Studio Services who maintains the communication storage server.

Keys are issued to the above individuals. No other individuals on staff are provided with keys to that room.

The above list of personnel who are granted physical access to the Data Center is reviewed annually by the Chief Financial and Administrative Officer.

Data Modification Request Form

Today's Date: ________________________ Change Request Number: _______________
(To be entered by ITS Department)

Required Change Date: ________________________

System: ___________________________________ (Jenzabar EX, Kronos, PowerFaids, JICS, LMS, etc.)

BLC User Requestor: ____________________________________ ____
Print Name Office

BLC ITS Requestor: ____________________________________ ____
Print Name Title

Explanation of problem: ____

____

____

Cause of problem: ____

____

____

Type of change: Insert Delete Update Other (explain) ___________________________

Proposed solution: (attach SQL code)____

____

____

Table(s), # of records, and other affected database objects: (index, view, package, etc.) __________________________

____

____

Testing activities <u>prior to</u> production implementation: ____

____

____

Data recovery method: (table export, TSM backup) ____

____

Verification plan after implementation:

a) By whom: ______________________________ ______________________________
Print Name Title/Office

b) Describe verification steps: ____

____

____

****

Change Request Approval for Production:

ITS Reviewer (print name)	**ITS Approver** (print name)	**User Approver** (print name)
(signature)	(signature)	(signature)
Date	Date	Date

****
*

DBA (print name)	**DBA** (signature)	**Date Implemented**

Instructions for Data Modification Request Form

This form is used to request approval for implementing changes to data within a Bethany Lutheran College production database.

All fields must be completed. If an item is “Not Applicable”, enter N/A in the field and explain why it is not relevant in this situation.

Once the change has been approved and implemented – fill in the Date Implemented field (at the bottom of the form) and give this form and any attached, supporting documentation to the BLC Manager or Director that originally signed the form as the BLC Change Approver. That person will file the paperwork in a centrally maintained location within the Department.

Today’s Date – supply the date.

Change Request Number – ITS will provide this once the request has been entered into the Change Request Tracker system.

Required Change Date – provide the date when the change must be implemented.

ITS Requestor – name and title of ITS staff member proposing the change.

User Requestor – name and office of the User proposing the change.

Cause of problem – describe how the problem occurred, and include whether it was due to an automated process, manual error, hardware/software error, known defects (bugs), etc.

Type of change – circle all that apply, and provide additional detail if “other” is selected.

Proposed solution – describe the problem resolution logic. Indicate whether the solution was developed in-house, is vendor-supplied, or a combination. Attach SQL code. If appropriate, include additional information about the specific tasks that will be performed.

Table(s), # of records, and other affected database objects – list the database tables, number of records (per table), and other database objects (index, view, package, etc.) that will be affected, and describe how they will be changed. Attach separate documentation to provide the appropriate level of detail.

Testing activities prior to production implementation – describe the testing activities that will occur prior to implementing the change in production. Include information about the databases (test, clone, etc.) that will be utilized for testing. Attach separate documentation to provide additional detail.

Data recovery method – explain the data recovery method (table export, TSM backup, SQL scripts, etc.) that will be used to recover the data, if necessary.

Verification plan after implementation – describe the verification process that will be utilized to determine whether the change was successful. Include information about who will be involved (name and title/office), and a description of the verification steps. Attach separate documentation to provide additional detail, if necessary.

Change Request Approval – several signatures are required to obtain approval for implementation of the production change.

a) ITS Reviewer – ITS staff member. Signature indicates peer review was conducted.
b) ITS Approver - ITS Management. Signature indicates approval for production change.
    a. If only verbal approval is received - print the Approver’s name and write “verbal” on the signature line, followed by your name (printed).
    b. If approval is received by a manager’s designated delegate – print the delegate’s name on the Approver’s line and write “delegate” on the signature line, followed by the delegate’s signature.
c) User Approver – Supervisory personnel within the User’s functional organization. Signature indicates approval for production change.

DBA – ITS Database Administrator involved in implementing the production change.

Date Implemented – after approval has been received and the change implemented – fill in the production implementation date.

Bethany Lutheran College, Inc.

INTERNET FILTERING POLICY

Purpose and Scope

Bethany Lutheran College (BLC) has chosen to provide internet services in order to facilitate access to information that is useful for students in achieving their academic goals and for faculty and staff who assist the students in fulfilling their goals. As a reflection of the Bethany Lutheran College's mission statement, the College chooses to not provide resources that it believes to be contrary to the educational and spiritual mission of the College.

In the same manner in which the BLC Memorial Library selects resources for inclusion in its offerings based upon usefulness in fulfilling the academic mission of the College, Internet service is designed to offer a positive addition to the academic resources available to students, faculty and staff. Just as some publications are not suitable for inclusion in the College library, some internet sites are not suitable for access through the College network.

Review of Sites

As the Internet is constantly growing and changing, the College does not claim the ability to monitor the content and quality of all sites. We have chosen to limit access to certain categories of content that do not seem to have any inherent academic value and are likely to contain material at odds with the mission of the College. Such distinctions are by definition subjective. Some sites that are legitimate for academic research will inadvertently be blocked. Partial sites cannot be blocked. It is all or nothing.

Our internet filter is managed by our internet provider. While it can block many categories, we have the following content blocked:

1. Adult Content such as child and adult pornography is blocked.
2. Explicit art, obscene and tasteless content, and sites with R-rated materials produce a warning.
3. Paper mills which facilitate cheating are blocked.
4. File sharing applications are limited in available bandwidth. This is part of our compliance with the Higher Education Act
5. Known virus, phishing, spyware and proxy sites are blocked.

If there is an obvious category of sites that are legitimate by College standards and are necessary for academic work at BLC, a request to review such content can be submitted to the Director of Information Technology Services (john@blc.edu) or the Dean of Students (tmanthe@blc.edu).

Bethany Lutheran College, Inc.

PASSWORD POLICY

Purpose and Scope

The purpose of this policy is to protect confidential information vital to College business. Password complexity and rollover will help prevent individual user accounts and the information contained therein from being compromised by others.

The scope of this policy applies to all employee accounts in the Bethany Lutheran College, Inc. domain and other systems that contain confidential data.

Password Requirements

Complex passwords will be required by all employee accounts in the Bethany domain and other systems that house confidential data before the information in those accounts can be accessed.

1. All passwords must be at least eight characters in length (twelve characters or more for members of the ITS department).
2. Passwords must not have been used in the four previous passwords.
3. Passwords must not contain the individual's name or account name.
4. Passwords must contain at least three of the following four character groups
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Numerals (0 through 9)
    - Non-alphabetic characters (such as !, $, #, %)

Other Requirements

Since passwords are a major security tool to protecting valuable College information, it is in violation of this policy to:

1. share your password with others (both employees or non-employees).
2. openly display your passwords in your working area.

Minimum Frequency of Change

- Administrative passwords for servers – quarterly (responsibility of the ITS department)
- Administrative passwords on non-server computers – annually (responsibility of the ITS department)
- ITS department staff – quarterly (responsibility of the employee)
- Staff with access to Administrative software products (Jenzabar, PowerFaids or Kronos) – semiannually (responsibility of the employee)
- Staff and Faculty without access to the administrative software mentioned above - annually

If individuals desire to change their passwords more frequently than is outlined here, they are encouraged to do so. If at any point, an individual believes the security of their password has been compromised, they must change their password immediately rather than waiting for the next cycled change.

Enforcement

Anyone found to be in violation of this policy may be subject to appropriate disciplinary action including termination of employment.

See also the Administrative Data Policy for further security information.

Bethany Lutheran College, Inc.

PERSONAL COMMUNICATION DEVICE ALLOWANCE POLICY

Purpose and Scope

Bethany Lutheran College is committed to providing essential, business-related tools and services to its faculty and staff in a manner which:

1. promotes the proper stewardship of assets;
2. complies with IRS, federal, state and college regulatory requirements;
3. establishes a framework for consistent decision-making; and
4. reduces or eliminates administrative costs whenever possible.

Mobile phones and cellular data services offer efficiency for College employees having legitimate business needs for this technology. This policy applies to wireless devices used for voice communication. The capabilities and cost of wireless devices in terms of text messaging, email, and network access are moving targets and an employee must make a case to his or her supervisor based on the “business needs” listed below.

Personal Communication Device Allowance Guidelines

Use of a personal communication device is permitted when a business need exists. Employees must observe applicable laws or ordinances regarding the use of personal communication devices while driving.

Definition of a Business Need

The use of a personal communication device by an employee for college business is for the benefit of the College in the furtherance of its mission, not for the convenience of the employee. A personal communication device will be provided to an employee after the institution has determined such a business need exists. An employee may not self-determine that a device is required. If a supervisor determines such a device is needed, a request will be submitted to his or her appropriate senior administrator who will in turn submit the request to the Chief Financial and Administrative Officer and together, they will approve or reject such request.

A valid business need” is defined as follows:

- The need to be readily accessible for contact with the public or with college faculty, staff, or students, for required or essential business communication needs due to frequent travel, working at a remote location (limited access to a land line), etc.,
- The need to receive or initiate communication in emergency situations, or
- The need to be accessible and available during working hours (when away from assigned land-line telephone) or during non-business hours by electronic means at all times.

Available Options for Personal Communication Devices

Departments have three options when requiring an employee to carry a personal communication device in order to perform his/her duties:

1. Assign a College-owned device.
2. Authorize an allowance to cover the costs related to the employee’s purchase of a personal access plan and personal communication device to utilize that device for both personal and business purposes.
3. Authorize reimbursement for employees who have occasional minimal use of a personal communication device for business purposes.

Purchase and Use of a Personal Communication Device funded by Grants or Contracts

Personal communication devices may be purchased and used for a sponsored project/grant or contract when the sponsored project/grant or contract language stipulates that the principle person(s) involved need such connectivity devices to carrying out the sponsored project/grant or contract requirements. In this case, the need for a communication device must be documented in the grant proposal and budget justification during the grant submission process, and the sponsor must approve (or not specifically disapprove) the expense as a direct charge on the grant. The grant/contract administrator must ensure that monthly recurring charges are clearly identified as part of the initial budget request and must document usage during performance of the project/grant or contract.

Bethany Lutheran College, Inc.

SYSTEM BACKUP POLICY

Purpose and Scope

The primary purpose for the backup system is to provide for disaster recovery of key network servers. The backup system is not a long term archival and is not set up to recover individual email messages.

Schedules

1. Full backups of production databases are done on a daily basis to another machine.
2. Full backups of the main administrative storage server are done weekly with differential backups done on the other weekdays.
3. Full backups of other major servers, including email, are done on a weekly basis.

The weekly backups are copied to encrypted hard drives on a weekly basis to be taken off-site to a safety deposit box.

Retention

For on-campus backups, each weekly backup overwrites the previous week's backup.

Off-campus backups are done with a two set rotation where the current backups are copied to one set of drives and brought off-campus to replace the other set of drives that had the previous week's backups.

Shadow copies are also kept on the storage servers which can sometimes be used to recover documents that have been accidentally corrupted or deleted.

Verification

Backup logs are verified on a monthly basis to make sure that they have completed successfully. Database backups are automatically verified as they are routinely used to create up to date play databases.