Information Technology Policies

Presented to the Bethlehem University Executive Council for Review and Approval

February 2010

Introduction

These Information Technology Policies were prepared as required by a grant from the World Bank to Bethlehem University, Bir Zeit University and An Najah University to establish Institutional Research Units on the three campuses. One component of the grant was the requirement that each of the Universities draft an Information Technology Policy that would govern the gathering, storing, analyzing, and distribution of computerized data at each institution. This document is the result of efforts of an ad hoc group, the Information Technologies Policy Commission at Bethlehem University. The members of the commission were:

Mr. Sami El-Yousef, Vice President for Finances and Planning
Dr. Irene Hazou, Assistant Vice President for Academic Affairs
Mrs. Nihad Jubran, Supervisor of the BU Computer Center
Dr. Fadi Kattan, Dean of the Faculty of Business Administration
Br. Neil Kieffe, Director of Instructional Technology

The draft policies were presented to the Executive Council of Bethlehem University, which is the advisory council to the Vice Chancellor, the CEO of Bethlehem University. After review, the Council and the Vice Chancellor approved the Policies on 15 December 2009.

Those responsible for preparing these policies also recommend the establishment of a permanent Information Technology Policy Commission, which will have the responsibility of addressing needed changes in these policies from time to time, the addition of new policies as required, and for the periodic review of each policy. Each policy included in this document will be reviewed in two years time and experience at that time will determine the frequency of future policy reviews.

The enclosed policies are designed to give the direction and guidelines to those responsible for implementing them. A series of Procedure documents will be required to give the operating departments specific guidelines for the implementation of the policies. Bethlehem University is grateful to the World Bank for the assistance and motivation to prepare these policies. The Commission is recommending that the format developed in this exercise will become the format for University policies in other areas as well.

Print Date: 8 February 2010

Contents

1 Network Account Policy

1.1 Policy Type

Information Technology Policy

1.2 Contact Office

Bethlehem University Computer Center

1.3 Oversight Executive

Director of Instructional Technology

1.4 Implementing Body

Network Administrator and System Administrators

1.5 Applies to

All users of Bethlehem University who have the authorization to access the Network.

1.6 Purpose of the Policy

To establish conditions for use of, and requirements for appropriate security for University Computer and Network Resources.

1.7 Policy Summary

Account usernames and passwords, including e-mail, are issued to individuals (users) for their sole use and are non-transferable. Owners are responsible for all usage of their assigned accounts, usernames, and passwords. Access to the network is a privilege, not a right. With this privilege, there also is a responsibility to use the network solely for educational purposes and not to access inappropriate materials.

The user, by using the account (username and password issued by the Bethlehem University Computer Center Staff), confirms that s/he has read, understands and agrees to adhere to all Bethlehem University regulations and IT Policies. The user also agrees to follow all system messages and instructions.

1.8 Definition of terms

1.8.1 Registered students

Those students who are enrolled in a credit class during the current semester, or the upcoming semester, and whose tuition and fees are up to date.

1.8.2 User

A member of the faculty, staff, students or any person who has permission to access the IT resources and facilities of Bethlehem University.

1.8.3 Network Account

Is a username and a password that allows the user to access the system, local network, internet, and e-mail.

1.8.4 Username

Is a unique code assigned to each user by the Bethlehem University Computer Center Staff. When used with a password chosen by the user, the username allows access to the computing facilities of the University.

1.9 Policy Statement

1.9.1 Creating a Network Account

All of the users listed below will receive a username and a password. This username is unique. For students the username is the student number. For Faculty/Staff the username will usually be the first letter of the individual's name followed by the family name unless it is not unique, in which case another combination is used.

a) Administration: User accounts are issued to all Administrative staff upon employment

b) Students (Full and Part-time: User Accounts will be issued to all registered students for the current semester.

c) Sub-contracted Staff: User accounts are issued to sub-contracted staff upon employment.

d) Volunteers: User accounts are issued to volunteer workers upon their supervisor's request

e) Special Accounts (Visitors): This type of account is issued to visitors to permit them to access the internet in the computer labs.

f) Shared Accounts: Shared accounts will not be used except where absolutely necessary. Persons who wish to use a shared account shall make an application to the Supervisor of the Computer Center

1.9.2 Ownership of Account

Bethlehem University is the official owner of all accounts on University computers.

1.9.3 Acceptable Use Policy

Acceptable use is always ethical, reflects honesty and shows restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of information, system security mechanisms and the individual's rights to privacy and freedom from intimidation, harassment and unwarranted annoyance. Therefore,

a) The user must protect his/her account and the computer system from unauthorized use. The user is responsible for all activities on his/her account or that originate from that account. The username and password together act as an electronic signature for which the user is responsible.

b) The user must access only information that is his/her own, that is publicly available, or to which the user has been given authorized access.

c) The user should select a good choice for a password. That is, it should not contain less than six characters and should contain both upper case and numerical characters. It is the responsibility of the user to keep it secure. It is recommended that the password be changed periodically.

d) The user must report any system security violation (or suspected system security violation) or any behavior that is contrary to the guidelines described in this document to the Bethlehem University Computer Center (BUCC).

e) The user must be responsible at all times for using the BU Systems in a manner that is ethical, legal and not to the detriment of others.

f) Privately owned computer equipment will not have full access to the Bethlehem University network without prior approval by the BUCC.

1.9.4 Unacceptable Network Account Use Policy

In the same way that the actions listed above constitute acceptable use, the following list outlines actions that are not acceptable uses of the Bethlehem University networks and computers. A person who violates one or more of the following unacceptable uses will be severely punished, or may be subject to severe restrictions or the cancellation of the user's privileges.

a) Using another person's account, system, files, or data without permission. Note that permission from an individual user may not be sufficient - some systems may require additional authority.

b) Attempting to gain access to other users accounts and files, or attempting to hack the University network or servers is strictly prohibited. Any violators of this regulation will be severely punished.

c) Altering system software or hacking in any form.

d) Invading the privacy of other individuals.

e) Disobeying computer lab and or system policies, procedures, and protocols (e.g., time limits on workstation usage).

f) Using the network in support of groups outside the University, when such use is not in keeping with the mission of the University, is not allowed.

g) Accessing data or making use of data from the Bethlehem University system or other administrative system's software which is not included in an employee's job responsibilities is not permitted.

h) Creating and/or placing a computer virus on the network or any workstation.

i) Accessing, attempting to access, and/or altering information in restricted areas of any network .

j) Attempting to log on to any network as a system administrator.

Any user, identified as a security risk or having a history of problems with other computer systems, may be subject to severe restrictions or the cancellation of privileges.

1.9.5 Confidentiality

It is not permitted to share passwords. The only person who should ever use an account is the person to whom it belongs. Users are responsible for protecting their own files and data. The user must log out when his/her work is finished.

1.9.6 Authentication and Integrity

Users shall respect the system integrity of campus computing facilities. For example, users shall not intentionally develop or use programs that infiltrate a computing system, or damage or alter the software components of a computing or network system. Authorized personnel routinely monitor the network in order to protect the system and its data.

1.9.7 Removal of Accounts

a) Faculty/Staff or Sub-contracted Staff resigning from Bethlehem University: The resigning faculty or staff member must present his Clearance Form to the BUCC for signature when s/he is leaving the employment of the University. The BUCC will then remove that individual's account.

b) Volunteer Staff: A notice must be sent to the Computer Center Supervisor when a volunteer leaves the University by the immediate supervisor of the volunteer. The BUCC will remove that individual's account upon notification.

c) Faculty & Staff on Study Leave or Sabbatical : Accounts for faculty or staff on study leave or sabbatical will remain active until it is clear that the individual no longer intends to return to the University. When the individual resigns from the University s/he must fill out the Clearance Form which requires the signature of the BUCC. At that time the account will be removed.

d) Students: Dismissed students, graduates and students no longer registered will be removed at the beginning of the following semester.

e) Accounts will be periodically reviewed by BUCC and accounts with a period of inactivity longer than one (1) year will be removed.

1.9.8 Disk Space

a) Staff and students should always save files on the backed-up network drive (H: drive). Work should never be saved on the local computer. Bethlehem University equipment and software backs up all files saved on the H: Drive daily. Files on the local computer are not backed up automatically and must be backed up by the individual user if the user wishes to protect them.

b) Members of the administrative staff have a maximum of 500MB storage, teachers have a maximum of 30MB storage, and students are granted a maximum of 10MB storage on their assigned H: Drives. Faculty members and staff who need additional disk space may apply to the BUCC for a reasonable expansion beyond these limits for special purposes. Beyond these limits the user will not be able to store more files and/or BUCC cannot guarantee back-up or recovery in the event of corruption, lost data and/or hardware/software damage.

c) Storing photos, pictures, software and big files are not allowed on the user's home drive (H: drive), unless they are related to academic work.

1.9.9 Policy Violations

Vandalism is defined as any malicious attempt to harm or destroy the data of another user, networked programs or operating systems that are connected to any of the network infrastructure. This includes, but is not limited to, the uploading or creation of computer viruses, deletion or alteration of other user files or applications, removing protection from restricted areas or the unauthorized blocking of access to information, applications or areas of the network. Vandalism will result in cancellation of network privileges.

Faculty members of staff who violate the terms of this administrative rule or otherwise misuses the network to access inappropriate material will be subject to disciplinary action, from a minimum of losing network privileges, up to and including discharge.

Students who violate the terms of this administrative rule or who otherwise misuse their access to the network will also be subject to disciplinary action from losing network access privileges up to and including dismissal.

1.10 Next Scheduled Review

March 2012

1.11 Approved By

Bethlehem University Executive Council

1.12 Date of Approval

March 2010

1.13 Revisions History

2 E-mail Policy

2.1 Policy Type

Information Technology Policy

2.2 Contact Office

Bethlehem University Computer Center (BUCC)

2.3 Oversight Executive

Director of Information Technology

2.4 Implementing Body

Computer Center Staff

2.5 Applies to

Students, Faculty, Staff and Administrators. This includes all users of Bethlehem University e-mail that ends with @bethlehem.edu. This policy covers appropriate use of any e-mail sent from a Bethlehem University e-mail address and applies to all employees, and agents operating on behalf of Bethlehem University.

2.6 Purpose of the Policy

The purpose of this policy is to ensure that faculty, staff, students and administrators have access to this critical form of communication. This policy ensures that all the above mentioned users can access, and be accessed by, e-mail as needed. This policy sets forth the rules and regulations that govern the use of Bethlehem University e-mail system.

2.7 Policy Summary

This policy provides guidelines for the use of e-mail services to all of its users who must comply with this policy. The University expects that all those who exercise this privilege will do so responsibly, with due care, comply with confidentiality guidelines, authentication and other proper use requirements as detailed in this policy statement. This policy governs the proper use, misuse and penalties thereof.

2.8 Definition of Terms

2.8.1 E-mail

Electronic mail, often abbreviated to e-mail, email, e-post or originally eMail, is a store-and-forward method of writing, sending, receiving and saving messages over electronic communication systems. It is the transmission of information through email software such as Pegasus or Outlook Express. The term ”email” (as a noun or verb) applies to the Internet email system.

2.8.2 Chain e-mail

E-mail sent to successive people. Typically the body of the note has direction to send out multiple copies of the note and promises good luck or money if the direction is followed.

2.8.3 E-mail User

Any user of Bethlehem University e-mail service. It includes all those who have an account that ends with @bethlehem.edu.

2.8.4 Forwarded E-mail

E-mail resent from an internal network to an outside point.

2.8.5 Sensitive Information

Information is considered sensitive if it can be damaging to Bethlehem University or its stakeholders' reputation or market standing.

2.8.6 Virus Warning

E-mail containing warnings about virus or malware. The overwhelming majority of these e-mails turn out to be a hoax and contain bogus information usually intent only on frightening or misleading users.

2.8.7 Unauthorized Disclosure

The intentional or unintentional revealing of restricted information to people, both inside and outside Bethlehem University, who do not have a need to know that information.

2.8.8 Attachment

An e-mail attachment is a computer file which is sent along with an e-mail message. The file is not a separate message, but now it is almost universally sent as part of the message to which it is attached.

2.8.9 Bandwidth

In computer networking and computer science, digital bandwidth or just bandwidth is the capacity for a given system to transfer data over a connection. It is measured as a bit rate expressed in bits/second (bit/s) or multiples of it (kbit/s, Mbit/s, etc.).

2.8.10 Spam

Spamming is the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages to thousands of recipients.

2.8.11 Virus

A computer virus is a computer program that can copy itself and infect a computer without permission or knowledge of the user. The original virus may modify the copies, or the copies may modify themselves. A virus can only spread from one computer to another when its host is taken to the uninfected computer, for instance by a user sending it over a network or the Internet, or by carrying it on a removable medium such as a floppy disk, CD, or USB drive.

2.8.12 Worm

A computer worm is a self-replicating computer program. It uses a network to send copies of itself to other computers on the network and can do so without user intervention.

2.9 Policy Statements

2.9.1 E-mail Acceptable Use Policy

E-mail is a very important resource that the University makes available to/among employees with the understanding that it is used for research, teaching and community services in agreement with the University mission and mandate. It is therefore the responsibility of the user to make appropriate use of this facility. Whatever the usage, the University expects the user to show that the use of these facilities is fully compatible with this guiding principle. In case of doubt it is for the user to prove that the facilities are used properly. Conversely the University has the right to establish that they are being misused.

2.9.2 Students

a) Registered students will be assigned an e-mail account after they finalize registration for their first semester.

b) Passwords will be automatically generated and made available through the computer lab.

c) The account will remain active for the duration of the student's attendance at Bethlehem University.

2.9.3 Faculty, Staff, and Administration

a) Faculty and Staff are assigned an e-mail account at the request of the Personnel Director.

b) The Computer Center creates the employee account and communicates the password directly to the employee.

c) The account will remain active for the duration of employment.

2.9.4 Ownership of Account

The e-mail accounts provided on University servers are institutional property, and those responsible for maintaining these servers are responsible for ensuring that institutional standards for security, user authentication and access control are appropriately applied. However, the security and confidentiality of e-mail cannot be guaranteed. Users are responsible for protecting their own files or data from being read by others using whatever protection mechanisms that are offered by the operating system in use.

2.9.5 Confidentiality

a) The University seeks to preserve privacy and confidentiality in the provision of all IT Services, however confidentiality of electronic mail cannot be assured.

b) Confidentiality may be compromised by unintended redistribution, or because of inadequacy of technologies to protect against unauthorized access. In addition, any confidentiality may be subordinate to the application of law or policy, including this policy.

c) As such, users should assume that the contents of electronic mail might be accessible to persons other than the recipient. Sensitive, libelous or abusive content should never be included in electronic mail.

d) Users should be aware that Network and Systems Administrators, during the performance of their duties, need to observe the contents of certain data, on storage devices and in transit, to ensure proper functioning of the University's IT facilities. On these occasions they may accidentally see the contents of e-mail messages.

e) The University has a reasonable right to capture and inspect any data stored or transmitted on the University's IT facilities (regardless of data ownership), when investigating system problems or potential security violations, and to prevent, detect or minimize unacceptable behavior on those facilities. This includes violations discovered while maintaining system security and integrity, including the management of unsolicited mail and virus protection.

f) The University reserves the right to access e-mail records, including those which have been deleted by the account holder but which may not yet have been deleted centrally. In addition, the University reserves the right to access e-mail records where there are reasonable grounds to believe that those records contain information necessary to the proper functioning of the University's business. Such circumstances would include the absence of an employee where it is not reasonable to obtain the employee's consent. Wherever practical, employees will be notified promptly when their e-mail records have been accessed.

g) Bethlehem University users shall have no expectation of privacy in anything they store, send or receive on the Bethlehem University's e-mail system. Bethlehem University may monitor messages without prior notice. The University is not obliged to monitor e-mail messages.

2.9.6 Authentication and Integrity

a) A user must access only information that belongs to the user, that is publicly available, or to which the user has been given authorized access.

b) No user may use another person's account, system, files, or data without permission (note that permission from an individual user may not be sufficient - some systems may require additional authority). Users should select a good choice for a password not less than six characters and keep it secure. It is recommended that a password should also include at least one upper-case letter and at least one number. It is recommended that the password be changed periodically.

c) Users should report any system security violation (or suspected system security violation) or any behavior that is contrary to the guidelines described in this document to Computer Center.

d) Attempting to gain access to other users' accounts and computers, or attempting to hack the University network or servers is strictly prohibited. Any violators of this rule will be severely punished.

e) With current technology, the University does not guarantee the authentication or integrity of an e-mail. That is, it cannot guarantee that the sender is indeed the sender nor that the contents are as created by the apparent sender.

2.9.7 Unacceptable E-mail Use

A user may not use Bethlehem University's System to send, receive, store or display communications or files that:

a) infringe any third party intellectual property or publicity/privacy right,

b) violate any law or regulation,

c) are defamatory, threatening, insulting, abusive or violent,

d) might be construed as harassing, insulting, biased or discriminatory based on a person's age, sex, race, sexual orientation, religion, disability, national origin or any other protected classification,

e) are pornographic, harmful to minors, child pornographic, or vulgar,

f) contain any viruses, Trojan horses, worms, time bombs, or other computer programming routines that are intended to damage, detrimentally interfere with, or expropriate any system, data or personal information,

g) are solicitations or advertisements for commercial ventures, religious or political causes, outside organizations or other non-job related activities (Under no circumstances may a user of Bethlehem University e-mail system use it to gain unauthorized access to third party resources),

h) capture and open electronic mail, except as required by authorized employees to diagnose and correct delivery problems,

i) use electronic mail systems for any purpose restricted or prohibited by laws or regulations,

j) ”spoof,” i.e., construct an electronic mail communication so it appears to be from someone else,

k) ”snoop,” i.e., obtain access to the files or electronic mail of others for the purpose of satisfying idle curiosity, with no substantial University business purpose,

l) attempt unauthorized access to electronic mail, attempt to breach any security measures on any electronic mail system, or attempt to intercept any electronic mail transmissions without proper authorization.

2.10 Next Scheduled Review

March 2012

2.11 Approved By

Bethlehem University Executive Council

2.12 Date of Approval

March 2010

2.13 Revisions History

3 Computer Laboratory Use Policy

3.1 Policy Type

Information Technology Policy

3.2 Contact Office

Bethlehem University Computer Centre (BUCC)

3.3 Oversight Executive

Director of Instructional Technology

3.4 Implementing Body

Supervisor of the Computer Center

3.5 Applies to

This policy applies to all users of Bethlehem University's computer labs.

3.6 Purpose of the Policy

The purpose of this policy is to ensure that all users of University computer labs enjoy the service and benefit from the equipment, the connection available, e-mail and computing services in the best possible way.

3.7 Policy Summary

This policy provides guidelines for the acceptable use of computer labs and equipment provided in each one of them. These computer labs are made available for better serving BU faculty and students in their teaching and learning activity. When a lab is not reserved for classes, it may be used by students for acceptable purposes set forth in this policy.

3.8 Definition of terms

3.8.1 Lab Assistant

A lab assistant is a student who is available to assist computer lab users with electronic media, hardware and software issues. The computer lab assistants shall assist with basic applications, internet and printing questions.

3.9 Policy Statements

3.9.1 Lab Goals

The purposes of BU Computer Labs are to provide computing resources (computers, software, network access, etc.) for educational activities, with priority to student use. When not reserved, they may be assigned to ”open” or ”drop-in” use by students and for other uses.

3.9.2 Acceptable Student Use

Use of the University's electronic facilities is a privilege, not a right. The computer laboratory facilities are intended primarily to support the direct instructional purposes of the faculty members. Priority will be given to completion of assignments, exercises, and projects necessary for completion of the requirements of courses.

Use of the facilities is governed by the policies of the University. The use of facilities for purposes that violate University policy, are illegal, or are unethical may result in temporary or permanent loss of privileges or imposition of other sanctions.

The University reserves the right to establish policies and rules as needed for all aspects of use. Specific rules for use of computer laboratory facilities are listed below.

a) Installation of hardware not provided by the University is allowed only with explicit permission of and direct supervision from BUCC staff.

b) Reconfiguration of software is prohibited.

c) Reconfiguration, rearrangement, and removal of hardware are prohibited.

d) Reproduction of copyrighted software is prohibited.

e) Use of the University's facilities for commercial purposes or personal gain is prohibited.

f) If the lab is booked, then classes have first priority. The instructor has the right to ask anyone using the lab, but not in the class, to leave.

g) Users of the University's electronic facilities must comply with directives from BUCC staff regarding appropriate use of facilities. If, at any time, any of the staff feel that an individual is behaving in a disruptive fashion the staff member may instruct the individual to leave the premises. If refused, campus security will be summoned to escort them out of the Lab, and the incident must be reported to the Dean of Students.

3.9.3 Backing Up Data

While all care is taken to protect data, students using the University labs are responsible for backing up their own work.

3.9.4 Software Installation Policy

The University will only install software for which there is a proper and valid license. There are no exceptions to this rule. “Demo” or “evaluation” copies will not be used in these labs.

All software to be installed must be available four weeks prior to the beginning of the semester of use, or the Institute for Community Partnership session. Instructors should test software two weeks prior to use and certify functionality.

To provide adequate lead-time for software testing and installation for special events or demonstrations instructors should notify the Supervisor of Computer Labs of all software needs at the time of reservation.

3.9.5 Instructors' Orientation Before Use

Instructors are encouraged to complete a brief orientation on the features of the Labs before using them. If an instructor uses the Labs for the first time, such an orientation is the best way to familiarize himself/herself with the features of the facilities, such as software, computer hardware and display equipment before the first class meeting. Waiting until after the session begins to do this usually delays the effective use of the lab by the instructor. Instructors are responsible for acquainting themselves with the features of the labs before using them.

3.9.6 Lab Booking Policy

In case a class is scheduled to be given in a computer lab, it is the responsibility of the Registrar's Office to make all necessary reservations. In this case, the Registrar's Office will communicate all schedules to the Supervisor of the computer labs. All other computer lab booking must be made in writing, and should be e-mailed to the supervisor of the Computer Labs. The booking should be made a week prior to the date of the actual use of the Computer Lab. A written confirmation is needed from the Computer Lab Supervisor. Once booking is confirmed, it will not be changed for any other priority.

3.9.7 Cancellation of Booking

To encourage the efficient use of the resources, all users are required to provide at least a three-day notice by e-mail to the Supervisor of the Computer Labs, if they will not be using the labs for an hour or more of their booking.

3.9.8 Computer Configuration

All computers on campus, which are available for students' use, are configured per University standards and may have specialized software as dictated by academic need.

3.9.9 Hourly Schedule of Labs

The hours of each lab are posted on the lab door as well as bulletin boards outside the computer labs. All lab hours and schedules are subject to change. The schedules should be checked regularly for any changes. During holidays and break periods the computer labs will be closed. Special schedules will be announced during the Registration and Admissions periods.

3.9.10 Prohibited Activities

The following activities involving use of Computer Facilities are prohibited.

a) Transmitting, copying, or creating unsolicited information that contains obscene, indecent, or vulgar material or other material that explicitly or implicitly refers to sexual conduct.

b) Transmitting, copying or creating unsolicited information that contains disrespectful language or panders to prejudice, sexism, political purposes or other forms of discrimination.

c) Communicating any information concerning any password, identifying code, personal identification number or other confidential information without the permission of its owner or the controlling authority of the Computer Lab to which it belongs.

d) Creating, modifying, executing or retransmitting any computer program or instructions intended to gain unauthorized access to or make unauthorized use of a Computer Lab, Software or Licensed Software.

e) Creating, modifying, executing or retransmitting any computer program or instructions intended to obscure the true identity of the sender of electronic mail or electronic messages, collectively referred to as "messages", including, but not limited to, forgery of messages and/or alteration of system and/or user data used to identify the sender of messages.

f) Accessing or intentionally destroying Software or Licensed Software in a Computer Lab without the permission of the owner of such Software or Licensed Software or the controlling authority of the Computer Lab.

g) Making unauthorized copies of Licensed Software.

h) Communicating any credit card number or other financial account number without the permission of its owner.

i) Effecting or receiving unauthorized electronic transfer of funds.

j) Violating any laws or participating in any criminal activity or other unlawful or improper purpose.

k) Using the Computer labs in a manner inconsistent with the University's contractual obligation to suppliers or with any published University policy.

3.9.11 Admittance to Computer Labs

a) Admittance to Computer Labs is conditional upon the presentation of a current BU ID, a guest lab pass, or any other acceptable form of ID to the Lab Assistant on duty.

b) The right to use Computer Labs is not assignable. For example, family members or friends are not eligible to use Computer Labs.

c) Users in Computer Labs without a permanent Lab Assistant must be ready to produce identification and/or lab passes when requested.

d) There is a limit of one workstation per person.

e) A workstation left idle for more than 10 minutes may be reassigned to another user.

f) Groups may utilize workstations at Computer Labs as long as such use does not compromise the noise level and work environment of the other users at the Computer Lab.

g) Use of a computer may be limited to one hour during periods of heavy Computer Lab usage, as when there are no available workstations in the lab and students are waiting to obtain a workstation.

h) Computers are available to students when no classes are scheduled in the room.

i) Computers are available on a "first come, first served" basis.

3.9.12 Conduct in Labs

a) Students should be respectful of other lab users, lab equipment and area at all times in the Computer Labs.

b) Computer Lab Assistants are to be respected and their directives responded to immediately at all times.

c) All noise levels (include: talking, music, muffled headphone noise, etc) in the lab should be kept to a minimum so that others are not disturbed. The Computer Labs are to be used as a study environment.

d) No eating or drinking is allowed in the labs.

e) Users are to clean up the area around the computer they used before they leave.

f) Push in all chairs at the end of the class.

g) Any breach of this policy could result in punitive action, including (but not limited to) loss of computer privileges, deletion of account, applicable disciplinary action, suspension or dismissal.

3.9.13 Printing

a) Printers are provided in the Computer Labs for student use. The student pays for printing by means of pre-paid cards. Printing cards are purchased at the University Bookstore.

b) Paper used in the Computer Labs is of the A4 size only. Printing on envelops or transparencies is not allowed.

c) Paper in printers will be refilled by Computer Lab Assistants or Computer Lab staff only.

d) Printing long documents must be done in 50 page sections.

e) Printers at Computer Labs are not photo copying machines. Only one copy of a version of a document may be printed using available printers.

3.9.14 Supervisor of Computer Laboratories

The Supervisor of the Computer Laboratories has the following responsibilities.

1. To maintain the smooth operation of the University Computer Labs and to maintain the labs in good working condition, including computer hardware and software as well as the rooms themselves.
2. To assist registered students and faculty in the use of the Computer Laboratory facilities.
3. To maintain the computers in operable condition by installing on them the image provided by the Computer Center.
4. To manage student and faculty network accounts as assigned by the Computer Center.
5. To distribute the network account sheets for new accounts.
6. To supervise the Lab Assistants by hiring them, laying out their job description, training them and assigning tasks to them and evaluating their performance.

3.9.15 Computer Lab Assistants

The Computer Lab Assistants are students who are available to assist lab users with electronic media, hardware and software issues during lab operating hours. The Computer Lab Assistants shall assist with basic applications, internet and printing questions.

During open lab hours, Computer Lab assistants are responsible for providing end-user support for network access, printing, and use of basic applications. They also oversee the proper operation of the network as far as they are capable. For more complex issues that cannot be resolved by Computer Lab Assistants, they are required to raise the issue to the Supervisor of the Computer Labs or, if necessary, the Computer Center.

Lab Assistants are not an alternative for learning the necessary application. For extensive assistance with specific applications, users should consult the appropriate documentation or see their instructor for assistance.

3.9.16 E-mail Use

Students using e-mail for internal or external communication must follow the standards applicable as set forth by the e-mail policy. Transmission of any inappropriate material that could be construed as harassment or discrimination on the basis of age, race, religion, disability, national origin, or gender) is strictly prohibited.

3.9.17 Internet Use

a) Internet access is provided for educational use. Visiting sites (viewing or printing) of inappropriate nature or that may be considered offensive by other individuals is not considered acceptable use of this service.

b) Sending/Posting harassing messages or repeatedly sending/posting unwanted messages (electronic or paper) to others is prohibited.

c) Users will not post, publish, or display any defamatory, inaccurate, abusive, obscene, profane, sexually-oriented, threatening, racially offensive, sexist or illegal material.

d) Only public domain resources or resources for which the author has given expressed consent for on-line distribution may be uploaded or downloaded.

e) Users will not transmit or download information or software in violation of copyright laws.

3.9.18 Computer/Network Vandalism

a) Transmission of any software having the purpose of damaging computer systems or files (e.g., computer viruses) is prohibited.

b) Users may not share their passwords or accounts with others and must make every effort to safeguard this information from unauthorized users.

c) The privacy of other users must be respected. Users shall not intentionally seek information about, obtain copies of files, modify files, or seek any other information belonging to other users, unless explicitly authorized to do so by those users.

d) Users must not give out personal information such as their passwords, home address, telephone number, or credit card numbers.

e) Users may use the University's mailing address but may not publish the University's phone number as their own personal number.

3.9.19 Equipment Use

No equipment in the Computer Labs is to be removed, modified, relocated, or disassembled. Problems with Computer Lab equipment are to be reported to the lab personnel immediately. Users may not connect any personal computer equipment to the University network without prior authorization.

3.9.20 Closing

Computer Lab Staff shall give users an official warning to finish up work at 15 minutes before closing. At closing, a lab assistant will announce to all remaining users that the lab is now closed. Users should be ready to leave at the posted Computer Lab closing time. In the event users are reluctant to leave the lab after it has closed, members of the Computer Lab Staff may switch printers and computers off without warning.

3.10 Next Scheduled Review

March 2012

3.11 Approved By

Bethlehem University Executive Council

3.12 Date of Approval

March 2010

3.13 Revisions History

4 Printing Policy

4.1 Policy Type

Information Technology Policy

4.2 Contact Office

Bethlehem University Computer Center (BUCC)

4.3 Oversight Executive

Director of Instructional Technology

4.4 Implementing Body

Supervisor of the Computer Center

4.5 Applies to

This policy applies to all computer related printing on the Bethlehem University campus with the exception of that which occurs in the University Print Shop.

4.6 Purpose of the Policy

The purpose of this policy is to provide quality computer related printing services to faculty, staff and students and to minimize unnecessary use and waste.

4.7 Policy Summary

Bethlehem University provides conveniently located printers near faculty and staff desks for the use of employees. For the use of students printers are located in the University Computer Labs and in the Library.

4.8 Definition of terms

4.8.1 Network printer

A printer that is connected to a number of computers, each of which can send print jobs to the printer.

4.8.2 Color laser printer

A printer that can produce color text, drawings and pictures. The cost of color laser pages is considerably more than black and white pages.

4.8.3 Color inkjet printer

A printer that can produce almost photographic quality prints of text, pictures and images. While the quality is excellent it is much slower and much more expensive than images produced by a color laser printer.

4.9 Policy Statement

Printing provides a method of converting electronic images into permanently storable paper copies which can be used for record keeping and dissemination of information. Bethlehem University encourages the printing of documents for which permanent file copies are needed. The University discourages unnecessary printing in order to reduce operating costs and to minimize the use of natural resources. Printers are provided to administrative staff and teachers in locations reasonably close to their desks. Students may make printed copies of electronic materials in the three Computer Labs and in the library. Students pay for printing at a fixed price per copy.

4.9.1 Office Use of Printing

Faculty and administrative staff are provided printers that are easily accessible. The types of printers provided vary to accommodate the speed and quality of printing needed by each office. Most printers provide for black and white printing. Color laser printers are available for special projects. Good judgment must be used in printing. Necessary copies must be made and unnecessary printing should be avoided. Maximum use of means of electronic distribution of information should be used to minimize unnecessary printing.

4.9.2 Printing in Computer Labs

Each of the student Computer Labs has a printer installed that can print documents submitted from any computer in that lab. Students can purchase Printing Cards in the University Bookstore for a fixed price per copy.

4.9.3 Printing in Library

The Printing Cards that are available for printing documents in the University Computer Labs can also be used to pay for printing from computers in the University Library. All the student computers in the Library are connected to one printer.

4.9.4 Access to Printing at Bethlehem University

Some office printers are connected directly to the computer assigned to individuals. Other printers are designated as "network printers" and serve a number of computers located in the same vicinity.

Paper for use in office printers can be obtained from the University Print Shop. Computer printers and photocopy machines use the same type of paper.

Each of the student Computer Labs has a printer installed that can print documents submitted from any computer in that lab. Students can purchase Printing Cards in the University Bookstore for a fixed price per copy. After a card has been purchased the student asks the Computer Lab Supervisor to add the amount to the student's printing balance. As printing jobs are sent to the printer the student's balance is reduced. The student's current printing balance is available on his/her computer screen. It is the student's responsibility to collect her/his printed copies from the printer. Students can also use their printing balance to print materials from the student computers in the library.

Students can print documents in color from the color laser printer located in a Computer Lab. Special computers are used to send documents to the color printer. The cost per sheet for color printing is higher than for black and white.

4.10 Next Scheduled Review

March 2012

4.11 Approved By

Bethlehem University Executive Council

4.12 Date of Approval

March 2010

4.13 Revisions History

5 Notification of Potential Service Interruption Policy

5.1 Policy Type

Information Technology Policy

5.2 Contact Office

Bethlehem University Computer Center (BUCC)

5.3 Oversight Executive

Director of Instructional Technology

5.4 Implementing Body

Supervisor of the Computer Center

5.5 Applies to

This policy applies to all BUCC staff and users of the B.U. computer network.

5.6 Purpose of the Policy

B.U. makes every effort to provide on-line computer services to its users 24 hours per day, 7 days per week. However, there are occasions when there will be planned interruptions as well as unplanned interruptions. This policy outlines steps that are to be taken to minimize the inconvenience to the users and to inform users how they will be notified of an interruption, if there is time to do so.

5.7 Policy Summary

To minimize inconveniences to the users, planned interruptions will take place outside of normal working hours, if possible, and advance notification will be provided. When there are unplanned interruptions, users will be informed with as much advance notice as possible. When unplanned interruptions occur without warning users will be informed if the stoppage will be prolonged.

5.8 Definition of terms

5.8.1 Planned interruption

A pause in computer services which is known and scheduled in advance. These would be things like upgrades to a server, installing programs on a group of computers that require the blocking of user logins, server maintenance in a public lab that causes certain software or functions like printing to be unavailable, or planned activity by the Physical Plant Department that affects electrical or network service to buildings where computer equipment is installed.

5.8.2 Unplanned interruption

A pause in computer service which is not known in advance. Some things, like power cuts from the electric company or accidental disconnection of a network cable, are beyond the control of BUCC and definitely are not planned. However, there can also be unplanned interruptions such as when a network has to be shut down to repair a damaged server.

5.9 Policy Statement

Despite every effort to the contrary, there will occasionally be interruptions of network service to the Bethlehem University campus. To minimize inconveniences to the users, planned interruptions will take place outside of normal working hours, if possible, and advance notification will be provided. When there are immediate, unplanned interruptions, users will be given notification with as much advance notice as possible. Many interruptions, especially those associated with power cuts, do not permit advance notice. In such situations the BUCC will take steps to re-establish service as quickly as possible and will inform users if the interruption will be prolonged.

5.9.1 Implementation of policy

Planned interruptions

Whenever possible, major interruptions in services, such as changing a server, connecting new cables, etc. will take place after working hours on work days or on non-working days. The BUCC will check with the Registrar, the ICP and other offices to make sure that the time selected does not conflict with previously scheduled activities which would require network services. Notification should be made at the beginning of the week in which the interruption will occur.

Unplanned interruption

Occasionally emergencies arise that require network service to be disrupted during the work day. When this occurs users will be notified via “On Screen Notification” that network service will be interrupted at a certain time and is expected to last for a stated period of time.

Unplanned interruption with no opportunity for advance notice

When electrical service is available on the campus but failure of some other equipment causes immediate shutdown of the system that is expected to last for an hour or more the staff of the BUCC will notify users of the situation by telephone. Secretarial staff, such as the switchboard operator and faculty secretaries can be asked to inform users of the situation by telephone.

5.10 Next Scheduled Review

March 2012

5.11 Approved By

Bethlehem University Executive Council

5.12 Date of Approval

March 2010

5.13 Revisions History

6 Computer and Network Security Policy

6.1 Policy Type

Information Technology Policy

6.2 Contact Office

Bethlehem University Computer Center

6.3 Oversight Executive

Director of Information Technology

6.4 Implementing Body

Computer Center and System Administrators

6.5 Applies to

This policy applies to all University personnel with access to University data.

6.6 Purpose of the Policy

Attacks and security incidents constitute a risk to the University's academic mission. The loss or corruption of data or unauthorized access to information on students records, instructional computers, and financial systems could greatly obstruct the activities of University staff, faculty and students. The University also has a responsibility to secure its computers and networks from misuse. Failure to do so may lead to legal or financial liability for damage done by individuals accessing the network from or through the University network. Moreover, other networks and Internet Service Providers may block BU servers and e-mails if BU LAN was compromised or hacked.

The objectives of this policy are to:

a) establish guidelines to protect the University's networks and computer systems from abuse and inappropriate use,

b) establish guidelines that will aid in the identification and prevention of abuse of University networks and computer systems,

c) establish guidelines that will minimize the risks and losses from any security attacks.

6.7 Policy Summary

The Computer Security Policy is intended to protect the integrity of BU network / data, and to establish guidelines that will aid in the identification and prevention of abuse of University networks and computer systems associated with security threats and breaches to campus networks and network resources.

6.8 Definition of terms

6.8.1 Network Resources

Any devices attached to BU network and any services made available over the network. Devices and services include network servers, peripheral equipment, workstations and personal computers (PCs).

6.8.2 Security Incidents

Any type of attack on PC or server that attempts to compromise or damage the equipment. Attacks may range from a simple Virus on a PC to hacking a server.

6.8.3 Local Area Network (LAN)

A computer network (or data communications network) which is confined in a limited geographical area.

6.8.4 Remote Access

Is the ability to obtain access to a computer or a network from a distance.

6.8.5 Firewall

A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both.

6.8.6 VNC (Virtual Network Computing)

A graphical desktop sharing system that uses the network to remotely control another computer. It transmits the keyboard and mouse events from one computer to another, relaying the graphical screen updates back in the other direction.

6.9 Policy Statement

Bethlehem University provides network resources to its divisions, faculties and departments in support of its academic mission. This policy introduces some measures to prevent or at least to minimize the number of security incidents on the campus network.

The responsibility for the security of the University's computing resources and network relies on the System Administrators who manage those resources. The Computer Center will help the system administrators to implement these responsibilities according to this policy.

6.9.1 General Policies

a) Access to any computer connected to BU network must be via a logon process that identifies and authenticates the user, except where read-only access is given to certain systems, such as the library catalog.

b) Shared accounts will not be used except where absolutely necessary. Persons who wish to use shared accounts shall make application to the Supervisor of the Computer Center.

c) Users should never share their account credentials with any other person for any reason.

d) Personal computers or laptops may not be connected to the University network without the prior approval of the Computer Center.

e) All PCs/Laptops connected to BU network should have a valid antivirus program that is updated regularly.

f) Operating systems and applications should always be updated with latest critical updates and patches.

g) Users should always log-off any computer before leaving it.

h) Users must not install nor run software considered as high risk or prohibited (such as: key-generators, hacking tools, packet capturing tools . . .)

6.9.2 Network Security

a) All servers directly connected to the Internet (with real IP addresses) should facilitate the use of Firewalls to prevent any unauthorized access to the servers or LAN.

b) Only needed ports required by running services should be opened. All other ports on all servers must be blocked by default.

c) Unneeded/unnecessary services on the servers should be turned off.

d) Total separation between the Administration and Campus network should be always maintained through physical means.

e) Computers on campus should not be connected to Internet connections (i.e. ADSL or Wireless Internet) other than the one provided by the University. If such connection is required, the Computer Center should be informed and special arrangements will be imposed to protect the security and integrity of the campus LAN.

6.9.3 Attempt to get around or undermine Imposed Security

Users are prohibited from attempting to get around or undermine any system's security measures imposed by the Computer Center or System Administrators. The following list provides examples of practices not allowed on the BU LAN.

a) Password decrypting or cracking tools

b) Denial of service (DoS) or distributed denial of service (DDoS)

c) Harmful activities (e.g. IP spoofing, port scanning, disrupting services, damaging files, or intentional destruction of or damage to equipment, software, or data)

d) Unauthorized access (e.g. using another's account, using a special purpose account, escalating privileges assigned to the user's account)

e) Unauthorized monitoring (e.g. keyboard logging, network packet capturing)

6.9.4 Password Policy

This policy is designed to protect the University resources on the network by requiring strong passwords along with protection of these passwords, and establishing a minimum time between changes to passwords.

This policy applies to any and all personnel who have any form of computer account requiring a password on the campus LAN including but not limited to a domain account and e-mail account.

6.9.5 Password Minimum Requirement

The following password requirements have been set by the Computer Center, and should be observed by all computer users.

a) A minimum length of user password will be 6 characters,

b) All passwords should not be a dictionary word, and should use a combination of lowercase, uppercase, numbers, and/or special characters (!@#$%^&*(){}[]),

c) It is recommended not to re-use old passwords when changing the current one,

d) Its recommended not to use the same password for several services or accounts,

e) It is recommended to change your password every 90 days,

f) Accounts will be automatically locked after 5 failed login attempts. The account will be unlocked after a specified grace period or by the System Administrator,

g) Password protected screen savers should be enabled and should protect the computer within 5 minutes of user inactivity,

h) Computers should not be left unattended with the user logged on unless there is an active password protected screen saver installed.

6.9.6 Password Protection

Never write passwords down, send a password through e-mail, include a password in a non-encrypted stored document, tell anyone your password, or reveal your password over the telephone. Be careful about letting someone see you type your password. If you suspect that someone knows your password, you should change it immediately and contact the Computer Center.

Computer Center staff will not provide a forgotten password to anyone over the telephone or by e-mail. This information will be provided only in person.

6.9.7 Remote Access Security Policy

Ordinarily remote access to servers or the campus LAN from outside the campus is not allowed. Exceptions are granted only when access is contractually obligated to comply with University security policies and practices and it is impossible to get to the campus such as during a snow storm or Bethlehem is occupied. If remote access is necessary the accessed equipment should be isolated from the LAN, if possible, during the access period. In addition, access should also be closely monitored.

The Computer Center and other System Administrators can use the VNC software to access local PCs for maintenance and inspection purposes and in compliance with the System Administrator Policy, Section, 2.9.1.

6.9.8 Logging & Monitoring Policy

a) Networks and computers may be monitored and usage logged. Logs are kept secure and are only available to personnel authorized by the Computer Center and will only be kept as long as needed.

b) Local networks and computers may be monitored and logged for all purposes including, but not limited to:

   i) Protecting against unauthorized access
   ii) Verifying security procedures and policies
   iii) System and operational security
   iv) Detection and prevention of attacks

c) Computer Center Personnel shall monitor in real-time backbone network traffic, as necessary and appropriate, for the detection of unauthorized activity, intrusion attempts and compromised equipment.

d) System Administrators should facilitate, where applicable, the use of intrusion detection systems for the detection of any hacking or attack attempts.

6.9.9 Incident Reporting

Any incidents found or encountered should be immediately reported to the Computer Center with complete details of the incidents and the effected equipment or services.

If a security incident (breach) was detected, the affected device should be immediately disconnected from the campus LAN pending further investigation and action.

6.9.10 Backups and Disaster Recovery

All work related data and files should be saved on one of the available servers and shared folders. Periodic backup will be only performed on designated servers and shared folders.

Backup media will be kept at the Computer Center in a secure and fire resistant cabinet.

The user is responsible for any data and files saved on their computer and local hard drives.

The Computer Center will perform periodic backups on designated servers and shared folders as follow:

a) Daily Incremental Backup: Each day a daily backup is performed to only include modified and new files.

b) Weekly Full Backup: Each Friday a full backup is performed. Weekly backups are kept up to one month.

c) Monthly Full Backup: The last Friday of each month a full backup is performed and saved for one year.

d) Off-Site Backup: A full backup is performed each month to be kept off-site (somewhere on campus).

e) Off-Site Semester Backup: At the end of each semester a full backup is performed, and the media is kept in a secure location outside the campus.

f) Annual Archive: At the end of each academic year a Full Backup will be retired to the permanent archives for historical purposes.

More details on backup and restore policies are available on the "Backup and Restoration of Data Policy" (Section 15).

6.9.11 Networking Implementation and Management

The Computer Center is responsible for planning, implementing, and managing the campus LAN, including wireless connections. The following technologies cannot be added to the LAN without prior approval by the Computer Center: routers, switches, hubs, wireless access points, and other networking technologies.

6.10 Next Scheduled Review

March 2012

6.11 Approved By

Bethlehem University Executive Council

6.12 Date of Approval

March 2010

6.13 Revisions History

7 Protection of Sensitive Data Policy

7.1 Policy Type

Information Technology Policy

7.2 Contact Office

Bethlehem University Computer Center (BUCC)

7.3 Oversight Executive

Director of Instructional Technology

7.4 Implementing Body

Supervisor of the Computer Center

7.5 Applies to

This policy applies to all users of information at the University.

7.6 Purpose of the Policy

To establish a policy for the safeguarding of restricted and sensitive data relating to students and BU personnel that is created, received, maintained or transmitted by the University. This policy is intended to ensure that the information is uniformly used and disclosed in accordance with all University policies and applicable laws. A combination of physical security, personnel security, and system security mechanisms are used to achieve this standard.

7.7 Policy Summary

This policy is intended to create an environment within the University that maintains Information Technology system security, data integrity and privacy by preventing unauthorized access to data and by preventing misuse of, damage to, or loss of data. It sets forth the policy for Data Classification; Data Collection; Data Access; Data Handling and Data Transfer; Storage of Sensitive Data; and Data Retention and Disposal.

7.8 Definition of terms

7.8.1 Archiving/Storage

The act of physically or electronically moving inactive or other records to a storage location until the record retention requirements are met or until the records are needed again.

7.8.2 Institutional Data

Institutional data supports the mission of Bethlehem University. It is a vital asset and is owned by the University. Institutional Data will be protected from deliberate, unintentional or unauthorized alteration, destruction, and/or inappropriate disclosure or use in accordance with established institutional policies and practices. Sensitive Data as defined in this section is a subset of Institutional Data.

7.8.3 Authorized User

Individuals who have been granted access to specific information assets in the performance of their assigned duties are considered Authorized Users (”Users”). Users include, but are not limited to faculty and staff members, trainees, students, volunteers, contractors, or other affiliates of the University.

7.8.4 Electronic Media

All media on which electronic data can be stored, including, but not limited to: hard drives, magnetic tapes, diskettes, CDs, DVDs and USB storage devices

7.8.5 Electronic Messaging

A set of communication processes used to relay information among the users of computers. Electronic Messages take many forms. Examples: Electronic Mail (e-mail), FTP, cell phones, instant messaging and internet chat.

7.8.6 Restricted Data

Data whose access is restricted by University statutes. For purposes of this policy, restricted data is a subset of sensitive data.

7.8.7 Sensitive Data

Data, regardless of its physical form or characteristics, with the highest level of protection including, but not limited to, data protected by law, data protected by legal contracts, or security-related data. It also includes data that is not open to public examination because it contains information which, if disclosed, could cause severe reputation, monetary or legal damage to individuals or the University or compromise public activities. Examples include: passwords, intellectual property, on-going legal investigations, medical or grades information protected by legal or University policies, ID numbers, birth dates, professional research, graduate student work, bank account numbers, income and credit history.

7.8.8 Information

Information is data that has been processed, in contrast to “data” which refers to the raw facts.

7.9 Policy Statement

Institutional data supports the mission of Bethlehem University. It is a vital asset and is owned by the University. Institutional data is considered essential, and its quality and security must be ensured to comply with legal and administrative requirements. Authorization to access institutional data varies according to its sensitivity (the need for care or caution in handling). This administrative policy sets forth the University's standards with regard to the handling of sensitive institutional data.

7.9.1 Data Classification

Any electronic data asset of Bethlehem University shall be classified as Public, Private or Confidential according to the following standards.

a) **Public data** is defined as data that any entity either internal or external to BU can access. Examples are as follows.

1. Employees Information Examples include but not limited to: Name; Job Title; Job Description; Education and Training; Previous work experience; First and last employment; Work location; Work phone number; Honors and awards received.
2. Student Information Examples include but not limited to: Name; Address; Telephone number; e-mail address; Dates of Enrollment; Enrollment Status (full time, part time, not enrolled); Major; Class; Academic Honors and Awards; Degree received.
3. Other Information Examples include but not limited to: Sponsored Academic research; Course Offerings; Academic Calendar.

b) **Private Data** includes information that BU is under legal or contractual obligation to protect. Private information may be copied and distributed within BU only to authorized users. Private information disclosed to authorize external users must be done after the proper clearance is obtained from an authorized supervisor. Examples include:

1. Employees Information Examples include but not limited to: Employee ID number; Employee Birth date; Location of assets; Donors; Gender; Citizenship, Religion; Disability Status.
2. Student Information Examples include but not limited to: Grades; Courses taken; Schedule; Test scores; advising records; Disciplinary actions; Student ID.

c) **Confidential Data** is not to be publicly disclosed. The disclosure, use, or destruction of Confidential Data can have adverse effects on BU and possibly carry significant civil, fiscal, or criminal liability. This designation is used for highly sensitive information whose access is restricted to selected, authorized employees. The recipients of confidential information have an obligation not to reveal the contents to another individual unless that person has a valid need to know the information. Confidential information must not be copied without authorization from the identified owner. Examples of confidential data include: Legal investigations conducted by the University; sealed bids; trade secrets or intellectual property such as research activities; ID numbers; gross salaries, pensions, and retirement benefits; value and nature of fringe benefits; health records; passwords; financial statements.

7.9.2 Data Collection

Users should collect only the minimum necessary institutional/sensitive information required to perform University business.

Department heads must ensure that all decisions regarding the collection and use of institutional data are in compliance with the law and with University policy and procedure.

7.9.3 Sensitive Data Access

a) Only authorized users may access, or attempt to access, sensitive information.

b) Authorization for access to sensitive data comes from the department head, and is typically made in conjunction with an acknowledgement or authorization from the requestor's department head, supervisor, or other official authority.

c) Where access to sensitive data has been authorized, use of such data shall be limited to the purpose required to perform University business.

d) Users will respect the confidentiality and privacy of individuals whose records they access, observe ethical restrictions that apply to the information they access, and abide by applicable laws and policies with respect to accessing, using, or disclosing information.

e) Notification of a user's termination or removal of authorized access to sensitive information must be conveyed immediately to the Supervisor of Computer Center.

7.9.4 Data Handling and Data Transfer

a) Sensitive information must not be transferred by any method to persons who are not authorized to access that information. Users must ensure that adequate security measures are in place at each destination when sensitive data is transferred from one location to another.

b) Sensitive data must be protected from unintended access by unauthorized users. Users must guard against unauthorized viewing of such information which is displayed on the user's computer screen. Users must not leave sensitive information unattended and accessible.

c) Sensitive information must not be taken off-campus unless the user is authorized to do so, and only if approved security precautions have been applied to protect that information.

d) Sensitive data should not be transmitted through electronic messaging even to other authorized users unless security methods, such as encryption, are employed.

e) Physical protection from theft, loss, or damage must be utilized for mobile devices that can be easily moved such as a thumb drive or laptop.

7.9.5 General Security Measures

a) Physical protection must be employed for all devices storing sensitive data. This shall include physical access controls that limit physical access and viewing, if open to public view. When not directly in use, office, lab, and suite doors must be locked and any easily transportable devices should be secured in locked cabinets or drawers.

b) Users of lap-top and other mobile computing devices need to be particularly vigilant and take appropriate steps to ensure the physical security of mobile devices at all times, but particularly when traveling or working away from the University.

c) Computing Services managed servers storing confidential information shall be regularly scanned for vulnerabilities, patched, and backed-up.

d) Systems (hardware and software) designed to store and transfer confidential records require enhanced security protections and must be closely monitored.

e) It is strongly recommended that institutional data not be stored on PCs or other systems in offices or laboratories. Institutional data (including word documents, spreadsheets and databases) that are created on a PC or similar system should be stored on a network drive hosted on a Computer Center managed server.

f) Electronic media storing restricted/sensitive data must be protected by password security. To the extent possible, these devices must employ approved security methods.

7.9.6 Data Retention and Disposal

a) Retention of Records Containing Restricted and Sensitive Data: A "schedule" describing the records and the official retention period should be devised by each department for each type of record created or maintained by the University.

b) Archiving: Institutional records, including sensitive information records, which are not being used for active University business, may be archived until retention requirements have been met.

1. Departments determine the criteria for inactive record status in their areas, based on need for the records and available storage space and any public records law.
2. Storage areas for inactive records must be physically secure and environmentally controlled, to protect the records from unauthorized access and damage or loss from temperature fluctuations, fire, water damage, pests, and other hazards.
3. When appropriate, only primary student records should be archived. The contents of true "Shadow" records should be destroyed after it has been determined that they contain only duplicates of records maintained elsewhere, and do not contain any original materials.
4. Off-site storage facilities or locations for sensitive records as well as the content of the data stored therein must be approved by the Office of Instructional Technology and shall not be disclosed except to the Supervisor of the Computer Center and the Vice Chancellor.

c) Record Disposal: The proper destruction of public records is essential to creating a credible records management program. Records containing restricted/sensitive data shall only be destroyed in the ordinary course of business; no records that are currently involved in, or have open investigations, audits, or litigation pending shall be destroyed or otherwise discarded.

1. No primary records of any type belonging to Bethlehem University may be destroyed until they have met retention requirements established by BU policies and any public records law.
2. When retention requirements have been met, records must be either immediately destroyed or placed in secure locations as described in this section for controlled destruction later.
3. The authorized methods of destruction for non-electronic records are burning, where authorized, or shredding. The authorized methods of destruction for electronic records are wiping or physical destruction of the electronic media.

7.10 Procedures

a) Supervisory Personnel: Every BU employee who has supervisory responsibilities and whose job responsibilities include the maintenance of or use of sensitive data is responsible for implementing and ensuring compliance with this policy and initiating corrective action if needed. In implementing this policy, each supervisor is responsible for the following.

1. Communicating this policy to personnel under their supervision.
2. Ensuring that appropriate security practices, consistent with the data handling requirements in this policy, are used to protect institutional data.
3. Providing education and training in data management principles to employees under their supervision.

b) User Responsibilities: Users who are authorized to obtain data must ensure that it is protected to the extent required by law or policy after they obtain it. All data users are expected to:

1. access institutional/sensitive data only in their conduct of University business.
2. request only the minimum necessary confidential/sensitive information necessary to perform University business
3. respect the confidentiality and privacy of individuals whose records they may access.
4. observe any ethical restrictions that apply to data to which they have access.
5. know and abide by applicable laws or policies with respect to access, use, or disclosure of information.

c) Compliance with this data protection policy is the responsibility of all members of the Bethlehem University community. Violations of this policy are dealt with seriously and include sanctions up to and including termination of employment or dismissal. Users suspected of violating these policies may be temporarily denied access to BU's information technology resources during investigation of an alleged abuse. Violations can also be subject to prosecution by law.

7.11 Next Scheduled Review

March 2012

7.12 Approved By

Bethlehem University Executive Council

7.13 Date of Approval

March 2010

7.14 Revisions History

8 Information Access through Computer Networks Policy

8.1 Policy Type

Information Technology Policy

8.2 Contact Office

Bethlehem University Computer Center (BUCC)

8.3 Oversight Executive

Director of Instructional Technology

8.4 Implementing Body

Supervisor of the computer Center

8.5 Applies to

Faculty, staff, administrators, and students and others engaged on the University's behalf.

8.6 Purpose of the Policy

This policy establishes principles for appropriate access to computer based University information among its staff, faculty, administrators, and students and others engaged on its behalf in the course of conducting its business and to safeguard its information assets against loss by theft, fraud, malicious or accidental damage, or breach of privacy or confidence.

8.7 Policy Summary

This policy establishes the rules for basic use, protection and preservation of all University information subject to the principles of academic freedom, professional integrity, protection of privacy, and confidentiality.

8.8 Definition of terms

8.8.1 Access

Permission, privilege or ability to read, enter, update, manage or administer computer information in some manner. The level of access is determined by the specific job of the user. For example, a user might be granted read access to a file, meaning that the user can read the file but cannot modify or delete it. Most operating systems have several different types of access privileges that can be granted or denied to specific users or groups of users.

8.8.2 Custodian of Data and Information

A university official or entity which has physical control over University information resources.

8.8.3 Steward

A University official who has responsibility for the data generated by his or her unit.

8.9 Policy Statement

Bethlehem University seeks to protect the privacy of information about students, staff and faculty and the confidentiality of University information. The University recognizes that all employees must have access to appropriate information in order to fulfill their jobs responsibly. Rules and procedures are put in place to enable members of staff to obtain authorized access to the information they need, in a manner that enables them to carry out their work effectively and efficiently. Violation of these rules will lead to disciplinary action by the University.

8.9.1 Authorization

The following University officials are authorized to grant or revoke access to University information.

Type of Information	**Executive Officer Authorized to Grant Access**
Academic and educational information; student and graduate academic information; information on faculty	Vice President for Academic Affairs
Financial information, such as purchasing, budget, financial statements, audits, facilities	Vice President for Finances and Administrative Affairs
Human Resources Information	Director of Personnel Management
Information on donors, alumni	Vice President for Development

8.9.2 Principles

The Information Access Policy operates on the basis of the following principles.

a) All information created or acquired through university funds or as part of employment with the University is owned by the University.

b) The Computer Center is the designated custodian of all university electronic information and data and should be responsible for its operational integrity and for implementing the Information Access Policy.

c) Rights of access to information are balanced by responsibilities. Only those individuals who have legitimate need to know can access information that is relevant to their work and essential to performing their duties.

d) No individual may download and transport off-campus on laptops, cds, dvds, flash drives, paper copies, or other portable media any data from the University's information systems without the specific permission of the executive officer listed in Section 8.9.2.

e) Staff in the Computer Center who are responsible for providing access to data through assigning passwords, keys, etc. are held responsible for any error that may result in unauthorized access.

f) Individuals who have erroneously received access to information that they should not possess must report this to the executive officer with the authority to grant them access.

g) An individual who uses information, to which he/she has no right to access, even if access was granted in error, will be subject to disciplinary action up to and including termination of employment or dismissal.

h) An individual seeking deliberate access to unauthorized information, using University information for personal action, destroying information to impede work or sabotaging information systems will be subject to disciplinary action up to and including termination of employment.

i) When an individual's duties at the University are changed, then his/her access should also change to reflect this.

j) When an individual leaves employment, all access to University information must be terminated immediately.

k) If, as a result of an individual using information to which s/he has no right and which results in a financial loss or damage to the reputation of the University, the University may seek legitimate financial compensation.

8.9.3 Implementation

a) Each computer application will have a designated person (data steward) responsible for its contents.

b) Each head of a department or unit will identify requirements for information access in their area and these will be registered by the appropriate data steward. He/she must specify the level of access (read-only or read/write) to each individual in his/her department.

c) Request for authorization for access of data is submitted to the relevant executive officer authorized to grant access for approval.

d) Staff within a department or unit may only obtain access through this procedure. Staff may not pass on information to another staff without consent of the relevant head of the department.

e) The Computer Center generates access capacity and can only do so upon written instructions from an executive officer with the authority to grant access.

8.10 Next Scheduled Review

March 2012

8.11 Approved By

Bethlehem University Executive Council

8.12 Date of Approval

March 2010

8.13 Revisions History

9 Monitoring of Employee Electronic Communications Policy

9.1 Policy Type

Information Technology Policy

9.2 Contact Office

Bethlehem University Computer Center (BUCC)

9.3 Oversight Executive

Director of Instructional Technology

9.4 Implementing Body

Supervisor of the Computer Center

9.5 Applies to

To all users and uses of electronic information owned or managed by the University.

9.6 Purpose of the Policy

To define a university policy on the circumstances for the monitoring and review of the content of employees electronic communication files.

9.7 Policy Summary

This Policy establishes monitoring and review principles, rules, and procedures applying to all members of the University community to ensure consistent application.

9.8 Definition of terms

9.8.1 Electronic communication

All communication via telephone, phone-mail, e-mail or computer files that traverse the University network or is stored on University equipment.

9.9 Policy Statement

Bethlehem University respects the privacy of electronic communication, upholds the principles of academic freedom and free expression while seeking to ensure that University administrative records are accessible for the conduct of University business. BU will not monitor and examine employees' electronic communication files in most instances except under certain circumstances that are deemed not in compliance with university policies.

9.9.1 Review with Consent

The consent of the holder of an electronic communication is obtained by the University prior to any access for the purpose of examination or disclosure of the contents of University communications records in the holder's possession.

9.9.2 Review without Consent

In the following circumstances consent to review the content of the electronic communication of an employee is not needed:

a) when required by and consistent with law

b) when there is substantiated reason to believe that there is a violation of law or University policies

c) in case of an urgent and sufficiently serious issue of health or safety

d) in case the employee is unexpectedly unavailable and when records to be accessed are of sufficient importance to justify their review when employee is unable to give consent for that review.

9.9.3 Authorization

Authorization to review an employee's electronic communication may be granted by the Vice President responsible for the affected employee, or in the absence of the Vice President by the Vice Chancellor.

9.9.4 Circumstances not requiring authorization

The University or some of its units might conduct routine monitoring or examination of employee electronic communications and files as part of the work environment and affected employees must be informed in advance of such monitoring. Such routines must be approved by the relevant Vice President. In the process, staff undertaking the monitoring or examination might observe certain transactional information or the content of electronic communication. They are not though permitted to seek out transactional information or content of electronic communication when not germane to system operations and support, or to disclose or otherwise use what they have observed. Technical staff that is operating in good faith in resolving technical problems may inadvertently see or hear content in communication and files which is potentially illegal or contrary to University policy. They are required to report what they have seen or heard to appropriate authorities.

9.9.5 Implementing this policy

Requests for authorization to monitor or review the electronic communication files of an employee usually originate with the supervisor or an investigatory authority; for example: the Disciplinary Committee, Council of Personnel Affairs, or a law enforcement agency. The request must be made in writing to the relevant Vice President. The University expects that the Vice Chancellor and the Vice Presidents to maintain confidentiality and to consult with the Executive Council / University lawyer to determine whether to authorize monitoring or review and in determining if the affected employee or anyone else should be notified that the monitoring or review is taking place.

9.10 Next Scheduled Review

March 2012

9.11 Approved By

Bethlehem University Executive Council

9.12 Date of Approval

March 2010

9.13 Revisions History

10 Website Policy

10.1 Policy Type

Information Technology Policy

10.2 Contact Office

Bethlehem University Computer Center (BUCC)

10.3 Oversight Executive

Director of Instructional Technology

10.4 Implementing Body

Bethlehem University Web Administrator

10.5 Applies to

This policy applies to staff who contribute to the Bethlehem University Website and its various components, in particular to members of the University Website Committee and the website assistants.

10.6 Purpose of the Policy

To establish a policy for governing the nature, content, format, maintenance, timeliness and ownership of information contained on the official pages of the Bethlehem University Website.

10.7 Policy Summary

The Bethlehem University website is an invaluable tool that offers opportunities for communicating information about Bethlehem University to a worldwide audience. The University Website Committee will be responsible for setting policies governing the nature, content, format, maintenance, timeliness and ownership of information contained on the official pages of the Bethlehem University website.

10.8 Definition of Terms

10.8.1 Website Committee

A committee established to oversee the B.U. Website, composed of the Web Administrator as chairperson, two faculty members, and representatives of the Public Relations, and Academic Offices.

10.8.2 Website Structure

Pages within the website will be designated by the Web Administrator as either official (University) or personal sites.

10.9 Policy Statement

The Bethlehem University Website is an official publication of the University. Its mission is to promote the University and provide accurate, up-to-date information about it in an accessible and attractive manner to audiences inside and outside the Bethlehem University community.

10.9.1 Official University Web Pages

Official web pages represent the University and its offices, divisions and departments, to the University's various audiences: potential students, current students, employees, friends, and visitors. Official pages must conform to the design styles adopted by the Committee to give the site unity, coherence, functionality and readability.

a. The contents of all official pages must reside on the Bethlehem University server.

b. All official pages will be built using template pages supplied by the Web Administrator and will be maintained and regularly updated by the University offices or departments responsible for them.

c. Each official page within the Bethlehem University web site will be readily identifiable as a part of its site by the use of the University logo or logotype, a specific palette of colors and specific typefaces.

d. Each official page will carry the e-mail address of the department or office responsible for its upkeep. Each Web Assistant will be responsible for regularly checking the e-mail and responding.

e. Official pages will be accurate, well-written, concise, free of spelling and grammatical errors and will otherwise present the University, its mission and values in a positive light.

f. All official pages will be regularly monitored by the Web Administrator to ascertain that material is correct and current. Those with outdated materials will be notified to update their page or remove the outdated material within five working days.

10.9.2 Personal Web Pages

Personal web pages are the home pages of any member of the faculty or staff of Bethlehem University. They are provided so that members of the staff can provide a brief biography and list their areas of academic interests. A personal page will be no larger than one A4 page.

However, space on this resource is a privilege, and all users are expected to follow the established website policy.

a. Personal pages will be governed by the Bethlehem University's acceptable use policy and all other applicable policies of the University. Anyone violating University policy on a web page will be subject to the appropriate disciplinary actions described in the relevant policy.

b. Personal web pages may not be used for commercial uses, sales or money-making ventures except those authorized by the University Administration.

c. In order to be given the privilege of a personal page, the author must sign a form agreeing to comply with the University's Website Policy.

10.9.3 Web Authoring of Official Pages

1. One person will be designated by each academic or staff unit to be ultimately responsible for the pages pertaining to it. This person will be designated as a "Web Assistant." Other employees within the academic or staff unit may help build, add to, maintain and/or update that unit's web pages, but the Web Assistant will be responsible for checking materials for their accuracy and conformance with web standards and for working with the Web Administrator prior to the publication of the material on the site. The Web Assistant will prepare the page using the template and pass it to the Web Administrator who will check the contents for compliance with University standards and will then post it on the website. Ultimate responsibility for the intellectual content of each section lies with the member responsible for each section.

    - **Website assistant positions are:**
        (a) Alumni
        (b) Audio-Visual Center
        (c) Computer Center
        (d) Computer Labs
        (e) Dean of Students
        (f) Digital Media Center
        (g) Faculty of Arts
        (h) Faculty of Business
        (i) Faculty of Education
        (j) Faculty of Nursing
        (k) Faculty of Science
        (l) Hereditary Research Center
        (m) Institute for Community Partnership
        (n) Institute for Hotel Management
        (o) Institutional Research Unit
        (p) Library
        (q) Office of Assistant Academic Vice President
        (r) Office of Personnel Management
        (s) Office of the Vice Chancellor
        (t) Office of the Vice President for Academic Affairs
        (u) Office of the Vice President for Development

(v) Office of the Vice President for Finance
(w) Public Relations
(x) Registrar's Office
(y) UNESCO Biotechnology Center
(z) Water and Soil Research Center

2. All Web Assistants must be employed by the University as members of the faculty or staff. Web Assistants may not be students, alumni, volunteers or hired professionals, although people in any of these categories may help the Web Assistant with his or her task.

3. Those appointed as "Web Assistants" will be provided with appropriate software, hardware and workshop training, as well as individual assistance in mastering software and style for the website.

4. Web Assistants may choose from a selection of official University templates, colors and photos for composing pages representing their office(s) or department(s). These will be stored in a website library maintained by the Digital Media Center.

5. All web pages for the University's official pages will be constructed using the Bethlehem University official approved software to eliminate compatibility problems and to enable those working within the site to check, change and maintain hyperlinks more easily.

6. All slightly changed or updated material for official pages will be reviewed prior to publication by the Web Administrator. All new or substantially changed official material will be reviewed by both the Web Administrator and the Website Committee prior to publication on the University website.

10.9.4 Graphic Elements and Photographs on Official Pages

Official pages within the University's website have been designed with several factors in mind. The main ones being: building and maintaining the University's image, supporting its image, keeping the site easy to maintain, making the site accessible to those viewers without state-of-the-art Internet access, and striving to make the site accessible to persons with disabilities. With these factors in mind, the following graphic standards have been developed.

a) Graphics will be limited in size to no larger than 75 k., with 50 k or less recommended.

b) Graphics to be used will be saved as .gif or .jpeg. files.

c) Only colors within the designated color palette will be used for graphic images.

d) The official Bethlehem University logo/logotype will be used only on official University pages and is not to be changed in any way.

e) Graphics and photographs will be chosen to enhance the informational content of the page.

f) The Digital Media Center (DMC) will be responsible for maintaining an approved library of graphic elements and photographs for use by Web Assistants on the official template pages. Web Assistants who have photos other than those in the file they wish to use can bring them to the DMC for approval and scanning. The DMC also will approve new graphics or help assistants develop new graphics as necessary for addition to the website library.

10.9.5 Approval Process for New and Changed Materials on the Official Website

Materials will be developed, changed and tested on the developmental web server, a test site that will enable Web Assistants to complete their work prior to its publication on the University's public server.

All new, changed or updated materials to official University pages then will be reviewed prior to publication on the University website by the Web Administrator. If the material is new or substantially changed, it also will be reviewed by the Website Committee. The review process will check for text style and accuracy, conformance with design standards and technical function. The Web Administrator may edit textual and design elements to bring them in line with established style and professional standards used in other official Bethlehem University publications. Alternatively, the material may be returned to the Web Assistant for additional work if necessary. When the material is approved by the Web Administrator and, if necessary, by the Website Committee, it will be published on the official website.

Major changes in the University website will be recommended by the Web Committee and approved by the Executive Council.

10.9.6 Website Access and Responsibility for Protecting Website Security

a) A system of permissions will be adopted and used to protect the security of the University website.

b) Those with full permissions to administer the site will be limited as necessary to maintain the site. The Web Administrator and Computer Center staff, will be the only employees with full permission to the official University website.

c) All employees with permission to the University website are responsible for taking all reasonable precautions to protect both the public and developmental website areas from vandalism, hacking and accidental alteration. This includes not sharing computer account information or passwords with others at the University and carefully monitoring access to personal computers in shared work areas.

d) Outside consultants must be approved by the Director of Instructional Technology and the Web Administrator. Each consultant must sign the University's Acceptable Use Policy for computers.

10.9.7 University Website Committee Responsibilities

a) The University Website Committee will be responsible for interpreting, implementing and revising current website policy.

b) The University Website Committee will be responsible for recommending new policy necessary to respond to new technology or emerging issues pertaining to website operation in general or to the University website in particular.

c) The committee will meet as necessary to resolve any questions, problems or grievances concerning website policy, management or other issues that may arise concerning website maintenance and operation. If deemed necessary, the committee will ask for the guidance or instruction of the University Administration in resolving an issue of importance.

10.9.8 Grievance Policy

a) Issues or grievances may be brought to the Website Committee for resolution by contacting either the Web Administrator or any member of the Website Committee.

b) The committee member contacted will be responsible for calling a meeting within two weeks and sharing the individual's concern with the committee. The individual with the concern may choose to present his/her issue to the committee for discussion and/or resolution or to have it presented to the group by another party.

c) The committee will discuss the matter and then decide on an appropriate course of action to address the issue or concern, if necessary.

d) If expedient, the issue may be tabled for a reasonable time pending further research and study by the committee.

e) If the committee decides it cannot resolve a grievance or problem, or, in the case of a conflict of interest, it is not the appropriate body to resolve the grievance, it may refer the issue to the University Administration for resolution.

10.10 Next Scheduled Review

March 2012

10.11 Approved By

Bethlehem University Executive Council

10.12 Date of Approval

March 2010

10.13 Revisions History

11 Information Release Policy

11.1 Policy Type

Information Technology Policy

11.2 Contact Office

Institutional Research Unit

11.3 Oversight Executive

Director of Instructional Technology

11.4 Implementing Body

Institutional Research Unit

11.5 Applies to

All Bethlehem University employees.

11.6 Purpose of the Policy

Various offices at Bethlehem University receive requests for institutional information from members of the University community as well as from agencies and organizations outside the University. This policy is meant to provide guidelines to respond to such requests.

11.7 Policy Summary

Bethlehem University is committed to high standards in the management of its information resources. This policy sets standards and guidelines to manage release of information without compromising the security of either University information assets or the confidentiality and privacy of personal records of students, staff, faculty, and administrators.

11.8 Definition of terms

11.8.1 University Public Records

All University records pertaining to the conduct of the administrative business of the University, such as the University Catalog, the Academic Staff Handbook, The Administrative Support Staff Handbook, and any information posted on the University's main Website.

11.8.2 Student's Academic Records

Any records (on computer, electronic, print, or handwriting) maintained by the Registrar's Office that relate directly to the student. By contrast, student records maintained by the advisor for advising purposes, medical records kept at the University Clinic for treatment purposes, and records pertaining to the employment of the student in the University do not constitute part of the student's academic records.

11.8.3 Student's Financial Records

All records pertaining to the student's financial status in the University maintained by the Finance Office.

11.8.4 Employee's Records

All information pertaining to non-academic staff as maintained by the Office of Personnel Management and to academic staff as maintained by the Office of the Vice President for Academic Affairs.

11.8.5 Donor Information

All information related to donor such as name of donor, address, telephone numbers, gift history or any other information pertaining to the donor and maintained by the Development Office or any other unit of the University directly dealing with the donor.

11.8.6 Alumni Information

All information maintained by the Development Office pertaining to graduates of the University such as names, degrees, program(s) attended, years attended, graduation date(s) and all other information gathered by the University after the person is no longer enrolled as student.

11.9 Policy Statement

11.9.1 Public Records

University public records that are in the public domain can be disclosed without prior consent.

11.9.2 Student Academic Records

Students' Academic Records are maintained by the Registrar's Office and information in them is classified as either directory information or non-directory information as follows.

Directory Information

Bethlehem University considers as "directory information" all information whose disclosure is generally not considered harmful or an invasion of privacy. The following information on students is designated as directory information and can be released without the student's prior consent unless the student has specifically requested restriction on its release: student name, address, telephone number, dates of attendance, major/minor fields of study, classification (freshman, sophomore, etc.), status (full-time, part-time) awards (scholarships and honors), degrees conferred.

Non-Directory Information

Information classified as non-directory pertains to: student's grades, GPAs, academic status (probation, suspension, and dismissal), transcript, financial status, ID number, birth date, disciplinary records. Student's consent is not needed for release of this information if done:

a) in response to requests by University officials for University use and who have legitimate educational interest in this information,

b) in response to officials in other institutions to which student is seeking enrollment,

c) in compliance with a law order,

d) in response to parent's requests, if the student is still a dependent as defined by the legal age.

Otherwise, release of such information requires the consent of the student. If non-directory information is requested for groups of students by officials from the University or outside and who have legitimate need for it, the consent of the Vice President for Academic Affairs is required for its release.

Ambiguous Information

If it is not clear whether the information requested falls under directory or non-directory, the Vice President for Academic Affairs must be consulted and his approval for the release must be secured.

11.9.3 Student Medical Records

Such records are maintained by the University Clinic and can be made available only to those persons providing the treatment. Disclosure of such records to any other party requires the consent of the student. It is the responsibility of the doctor or nurse to secure the consent of the student.

11.9.4 Student Financial Records

Students financial records are maintained by the Finance Office and any release of information therein to University officials and external parties must be authorized by the Vice President for Financial and Administrative Affairs.

11.9.5 Employee Records

Records of employees on non-academic contracts are maintained by the Office of Personnel Management while records of employees on academic contracts are maintained by the Office of the Vice President for Academic Affairs. The information in these records is classified as either personal or non-personal as follows.

Non-personal Information

The University has determined that the following information about University employees is non-personal: name, date of hire or separation, current position title, rank and step, organization unit assignment, office address & telephone number, current job description, full time or part time, probationary status, prior non-University employment, and any additional information deemed necessary to release to the public by the University administration. The University will disclose all non-personal information without the employees consent in response to any request by a party who has a legitimate interest in the information.

Personal Information

The University will use the term ”personal information” to mean all information that identifies or describes an individual the disclosure of which would constitute an unwarranted invasion of personal privacy. Examples of this kind of information are: birth date, citizenship, ID number, home address and home telephone number, performance evaluations or letters of corrective actions, spouse's or other relatives' names, medical history. The University will not disclose any personal information in a manner that would link the information disclosed to the individual to whom it pertains without the consent of the employee unless the disclosure is:

1. for University use to University officials who have legitimate interest in this information,

   (a) to appropriate parties in a medical or safety emergency,

   (b) to comply with a law order.

In all cases as seen appropriate the University will inform the employee of the disclosure.

11.9.6 Alumni Information

Only University employees who have a need to know in order to perform their duties may access alumni information. Information about alumni that can be released without their prior consent may include forwarding contact information about an alumnus to another alumnus; information to organizations associated with the University to serve a University function, and to alumni directories. Other circumstances for release of alumni information require the prior consent of the alumnus, if possible, otherwise the consent of the Vice President for Development is required.

11.9.7 Donor Information

Only University officials who are authorized and have a need to know to perform an authorized University function may access donor information. Donor information shall be used solely for development purposes. Each unit is responsible to maintain confidentiality of its donor information. The names and addresses of donors who donate in memory or in honor of someone may be released to the appropriate family member.

11.9.8 Solicitation for Business Purposes

Under no circumstance will the University release a listing of its employees, students or alumni to individuals or organizations for soliciting business or promotion of commercial products.

11.9.9 How to Request Information

Students have the right to inspect their records if they suspect inaccuracies or violation of privacy. The request for inspecting their records must be done in writing to the Registrar if the request pertains to their academic records and to the Financial Vice President if the request is in relation to their financial records.

11.9.10 Government Officials and Others Outside the University

The University releases information upon the request of officials in the Palestinian governmental offices such as the Ministry of Education and Higher Education, Palestinian Bureau of Statistics, Ministry of Labor, with the understanding that the information released is used by these offices to carry out their functions. The Institutional Research Unit is the office responsible for providing the information.

11.9.11 Release of Information for Research Purposes

The University will release information to individuals or organizations conducting certain studies or research on behalf of the University with the understanding that the information will not be released to a third party without the necessary authorization. Information for such purposes can only be released by the Institutional Research Unit in an agreed-upon format.

11.9.12 Implementation

It is the supervisors' responsibility to ensure that their employees are made aware of this policy. Any employee disclosing information in his/her area must do so in compliance with this policy. When in doubt the employee must seek advice of the supervisor and ultimately the approval of the relevant vice president.

11.10 Next Scheduled Review

March 2012

11.11 Approved By

Bethlehem University Executive Council

11.12 Date of Approval

March 2010

11.13 Revisions History

12 Standard Operating Environment Policy

12.1 Policy Type

Information Technology Policy

12.2 Contact Office

Bethlehem University Computer Center

12.3 Oversight Executive

Director of Instructional Technology

12.4 Implementing Body

Computer Center

12.5 Applies to

This policy applies to all departments and faculties of Bethlehem University.

12.6 Purpose of the Policy

A Standard Operating Environment (SOE) provides a high level of productivity in a cost-effective manner. It also reduces complexity, improves operational effectiveness, and assures a continuous availability of services.

The adoption of SOE reduces cost through more effective use of BUCC support staff as well as increased productivity from using compatible file formats among all faculties and departments.

12.7 Policy Summary

This policy establishes a Standard Operating Environment (SOE) for all computer users at the University.

12.8 Definition of terms

12.8.1 Standard Operating Environment

A Standard Operating Environment (SOE) comprises the following components: a software base image that is used for deployment across University staff desktop computers. The image includes the operating system, the standard connection software and security settings used and a predefined set of University enterprise wide applications.

12.8.2 Application Software

Computer software is designed to help the user perform a particular task. Such programs are also called software applications, applications or apps. Typical examples are word processors, spreadsheets, media players and database applications.

12.9 Policy Statement

To make the most efficient use of University resources, all computers acquired by the University will conform to the University minimum standards. Exceptions to standards may be considered when a non-conforming technology is essential to fulfill a department's needs.

The Computer Center is the body responsible for selecting which Operating system (OS) or Software to be installed on each user's computer based on his/her needs.

12.9.1 Standard Operating Systems

After study the Computer Center selects the operating system to be used on the individual workstations of the University to facilitate efficiency in use and ease of maintenance.

12.9.2 Anti-Virus Controls

All computers should have appropriate software installed for virus protection and for spyware protection.

12.9.3 Office Applications

Word processing, spreadsheet and presentations software will be installed on all University computes based on the existing operating system and the hardware.

12.9.4 Internet Browsers

Approved internet browsers will be installed on all University computers.

12.9.5 Other Software

Other needed software such as graphics, programming, media development, etc. will be deployed according to user/department needs and based on the Computer Center decision.

12.9.6 Software that are Not Permitted

The following types of software are not allowed because they unnecessarily use network facilities and the time of University personnel:

a) Peer-to-Peer software

b) Proxy and firewall by-pass

c) Games

d) Browser messengers or toolbars

e) Voice over IP

f) Screensavers

g) Any software that downloads huge amounts of data

h) Any other software that is not work related.

12.9.7 Software Development Policy

The purpose of this policy is to describe the requirements for developing and implementing any new software at Bethlehem University.

The Computer Center is responsible for developing, maintaining, and participating in a System Development Life Cycle (SDLC).

A complete and documented system analysis for the requested software should be conducted by the Computer Center and the requesting department prior to any decision on procurement or development of the software.

The programming language used for software development should be based on the Computer Center's recommendations.

There must be more than one staff other than the programmer for analyses, developing, testing, writing documentation and implementing the new software.

All production systems must have an access control system to restrict who accesses the system as well as restrict the privileges to those users. A Control Administrator must be assigned for the new systems.

There must be a separation between production, analysis, development and testing environment.

12.9.8 Software Purchase Policy

Computer Center Staff will review Purchase Requisitions to ensure both the technical adequacy of the proposed expenditure and compliance with the specifications and regulations. They may refer proposals to appropriate committees. After review, they will send proposals to the Purchasing Manager.

In selecting software Open-Source software should be used whenever possible. After purchase, the Computer Center will install the software on a computer for testing. Testing should involve users from the requesting department.

12.9.9 Software Installation Policy

Offices and Support Departments

a) Employees, other than Computer Center Staff, are not allowed to install software on Bethlehem University's computing devices operated within Bethlehem University network.

b) Software must be provided to the Computer Center for testing and maintenance. This is to minimize the risk of loss of the operating system.

Computer Labs & Class Rooms

a) Each semester a notice will be sent to all departments asking about their need to add, update or remove software on the classroom and laboratory computers.

b) It is the department's responsibility to provide any new software to the Computer Center to install.

c) The Computer Center will install new software on one computer from each lab. The department/teacher should test the new software before the Computer Center installs it in all labs.

d) New software will be installed in the computer labs, laptops and class rooms one week before the beginning of the semester. Software cannot be installed in the labs during the semester unless there is an emergency.

12.9.10 Policy for Program Changes and Amendments

Faculty must provide the Computer Center with the reasons to change any software. It is the Computer Center's decision to do so based on the existing hardware and the information.

12.10 Next Scheduled Review

March 2012

12.11 Approved By

Bethlehem University Executive Council

12.12 Date of Approval

March 2010

12.13 Revisions History

13 System Administrator/Instructional Technology Staff Policy

13.1 Policy Type

Information Technology Policy

13.2 Contact Office

Bethlehem University Computer Center

13.3 Oversight Executive

Director of Information Technology

13.4 Implementing Body

Computer Center and System Administrators

13.5 Applies to

This policy applies to all system administrators at all departments and other locations of Bethlehem University.

13.6 Purpose of the Policy

The policy is intended to protect the wide range of information technology resources that are supported by System Administrators.

13.7 Policy Summary

This policy governs and provides guidelines to employees of Bethlehem University who have administrative access and rights to Information Technology Resources, local area network, shared folders, or files of BU community members.

System Administration must be accomplished in a professional and timely manner with the goal of protection of University assets and the broad range of Information Technology Resources in use at the University. System Administrators have responsibilities to the University and must use all reasonable efforts to comply with all IT and University Policies and guidelines to ensure the availability, confidentiality and integrity of data and information.

13.8 Definition of terms

13.8.1 Information Technology Resources

Includes the use of University computer networks, the Internet, e-mail, shared folders, electronic documents, servers, and other devices used for storing or transmission of electronic data.

13.8.2 System Administrator

Any individual who has full access/rights to any Information Technology Resource at Bethlehem University.

13.8.3 System Administration

System Administration refers to specific responsibilities and assigned tasks of the System Administrator. Such tasks include, but are not limited to: installing, supporting, and maintaining operating systems, database management systems, application software and hardware; planning for, troubleshooting and responding to system problems or outages; and providing knowledgeable facts about the use of the system in the organization.

13.9 Policy Statement

13.9.1 Main Duties

The main duties of the System Administrators are to ensure proper operation of the various Information Technology Resources under their responsibilities including, but not limited to, servers, routers, applications, and network. Duties also include ensuring the confidentiality, integrity, and availability of various information and data used by University community.

13.9.2 Investigation of Possible Misuses and System Logs

System Administrators are assigned to:

a) monitor system logs for possible abuse and misuse,

b) check application log for warning and error messages for service startup errors, application or database errors and for unauthorized application installations,

c) check security log for warning and error messages for invalid logons, unauthorized user creating, opening or deleting files,

d) check system log for warning and error messages for hardware and network failures,

e) check web/database/application logs for warning and error messages,

f) check directory services logon domain controllers.

13.9.3 Data and Systems Backup Services

System Administrators must perform regular and complete backup services for all systems they administer, such as:

a) running and/or verifying that a successful backup of system and data files has been completed successfully,

b) performing periodic tests to the backup/restore system by restoring backup files to a test system to verify procedures and files,

c) performing a complete disaster recovery simulation on main servers,

d) ensuring that backup sets are kept in a secure place,

e) ensuring that offsite backups are performed periodically and according to the instructions of the Computer Center.

13.9.4 User Account Integrity

a) System Administrators will manage User Accounts on a timely basis, providing new accounts and removing old accounts in a prompt manner. All User Accounts are authenticated using individually assigned unique usernames and passwords. Accounts will be created with minimum privileges.

b) System Administrators will ensure that all User Accounts are disabled immediately upon employment termination unless otherwise approved in advance.

c) System Administrators will ensure that good passwords are used and those passwords are changed frequently according to BU Computer Security Policy.

13.9.5 Obligation to Maintain the Confidentiality of Accessed Communications

a) A Systems Administrator shall not read, listen to or otherwise view the confidential contents of any Information Technology Resources unless approved by University Administrators for special purposes.

b) A System Administrator who improperly reads, disseminates, or otherwise compromises the confidentiality of electronic mail or other data, files or records will be subject to disciplinary action, including dismissal.

13.9.6 Ensuring Data and Services Availability and Integrity

System Administrators will:

a) implement adequate protections of Confidential Data including identification of appropriate storage locations, encryption processes, and user access control,

b) Track/monitor system performance and activity by checking for memory usage, CPU usage, and hard-drive space,

c) perform physical checks of systems by visually checking the equipment for alert lights, alarms, etc. and taking appropriate action when needed,

d) install and maintain all aspects of system integrity, including obtaining releases and fixes to ensure the currency of operating system upgrades, installing patches, and managing releases,

e) verify that vendor default passwords are disabled or changed immediately upon installation of new software,

f) update Server Anti-Virus signature file and software daily,

g) run periodic Anti-Virus scans on servers and clean any virus or malware found,

h) disable any unnecessary system services running on servers,

i) block unneeded ports on servers,

j) keep software up-to-date by downloading any updates or upgrades,

k) make sure that the internet line and bandwidth is utilized in a matter that best serves the University community members and mission by:

- blocking access to specific sites,
- limiting bandwidth usage to specific sites,
- prohibiting the use of unnecessary software with high Internet bandwidth consumption,
- scheduling software and large file downloads during the night or during off-peak hours.

13.9.7 Third Party Access

Third parties should not be given access to University information technology resources. If such access is to be granted,

a) it must be contractually obligated to comply with University security policies and practices,

b) the accessed equipment should be isolated from the LAN (if possible) during the access period,

c) access should also be closely monitored and only provided when needed.

13.9.8 Remote Access

System Administrators will facilitate the use of Remote Access applications (i.e. SSH, VNC, Remote Desktop) to maintain various devices or to remotely provide services to users. Remote access connections must be handled through secured and encrypted communications. Other security measures must be used such as using good encrypted passwords, requiring user acceptance for remote connections, and limiting remote access to specific IP addresses.

13.9.9 Policy Violations and Criminal Activity

a) System Administrators should immediately report any violations to Bethlehem University policies, local relevant policies, or any security breaches to the Supervisor of the Computer Center.

b) If a security breach is found, immediate actions should be taken to minimize the damage to University Information Technology Resources. Actions such as disabling user accounts, disconnecting devices from network, or taking a system/website off the Internet should be taken until the issue has been resolved.

13.9.10 Enforcement

The Computer Center will audit the security of systems that is connected to the University network. The Computer Center may scan or examine systems for compliance and may disconnect any non-compliant system from the University network until the system is brought into compliance. In accordance with this policy, violators may be denied access to University computing resources and may be subject to other penalties and disciplinary action according to University disciplinary procedures and policies.

13.10 Next Scheduled Review

March 2012

13.11 Approved By

Bethlehem University Executive Council

13.12 Date of Approval

March 2010

13.13 Revisions History

14 Purchase and Disposal of Equipment Policy

14.1 Policy Type

Purchasing Policy

14.2 Contact Office

Office of Purchasing and Auxiliary Enterprises Management

14.3 Oversight Executive

Vice President for Finances and Administrative Affairs

14.4 Implementing Body

Purchasing and Auxiliary Enterprises Manager

14.5 Applies to

This policy applies to the purchase of items from all sources of funds administered by the University. This policy applies to all University activities including foundations, centers, associations and institutes.

14.6 Purpose of the Policy

The purpose of this policy is to ensure that all purchases of materials and equipment are made in accordance with a set of clear policies and procedures. It attempts to administer buying practices so that all suppliers are considered and dealt with ethically, effectively and efficiently.

14.7 Policy Summary

This policy provides guidelines for the steps to be followed when purchasing any item, whether for materials or equipment. All University purchases should be made in accordance with the policy set forth in this document. The Vice Chancellor, Vice President for Finances and Administrative Affairs, and the Purchasing Manager are the only persons authorized to obligate the University. Without definite and prior written permission, no University department may order directly by letter, telephone, fax, or in any other manner. The University will assume no obligation except by a previously issued and duly authorized purchase order that follows this policy.

14.8 Definition of terms

14.8.1 Capital outlay

The cost of acquiring plant assets, adding to plant assets, and adding utility to plant assets for more than one accounting period.

14.8.2 Equipment

Moveable tangible property such as research equipment, vehicles, machinery, and office equipment that meets the institution's capitalization policy for capital assets.

14.9 Policy Statement

14.9.1 Principles of Purchasing

The principles that govern purchasing are:

a) value for money, being the benefits achieved compared to the costs incurred. This could include measures such as price, quality, reliability, service, delivery, payment terms, and strategic suppliers,

b) quality, efficiency and effectiveness,

c) transparency,

d) effective competition, including fair dealing,

e) free from fraud and conflict of interest.

It is crucial that comprehensive and well-documented records are maintained on all acquisitions of goods and services.

14.9.2 Purchasing and Auxiliary Enterprises Manager

Bethlehem University has a purchasing manager who is responsible for ensuring that the University achieves best value for money in all University procurement activities. The Manager is responsible for:

a) soliciting bids

b) approving all quotations,

c) approving all advertisements for tenders, and

d) signing all purchasing orders.

14.9.3 Justification for the Purchase

Prior to the purchase of any item, there must be sufficient justification to demonstrate that there is a need for the goods and services to be provided and that funding is available.

14.9.4 Role of the Computer Center in Purchasing

Computer Center staff will review Purchase Requisitions to ensure both the technical adequacy of the proposed expenditure and compliance with the specifications and regulations. They may refer proposals to appropriate committees. After review, they will send proposals to the Purchasing Department.

14.9.5 Specifications

To provide a common basis for bidding, specifications should set out the essential characteristics of the items being purchased, so that all bidders know exactly what is wanted and can accurately compute their bids. If some essential requirement is left out, the award may be made without determining whether the successful bid meets the needs. The unsuitability of the product purchased may not become apparent until much later. Requiring unnecessary features can also result in restrictive specifications. It can also be defeating. Select wording carefully. Use ”shall” when specifications express a requirement binding on either the contractor or the purchaser. Use ”should” and/or ”may” to express non-mandatory provision.

The three types of specifications are as follows.

a) Material Specification - (also referred to as design or descriptive specifications). It specifies what the product must be. (i.e., all of the physical characteristics of the product; height, weight, storage capacity, RAM specifications, voltage, etc.)

b) Performance Specification - (also referred to as a functional specification). It specifies what the product must do. (i.e., all of the performance characteristics of the product without regard to how it is constructed, what size it is, etc.)

c) Combination of Material and Performance Specifications. In many cases, a bid specification falls somewhere in between the performance related and design oriented.

- All specifications must:
  identify the minimum requirements,
  allow for competitive bidding, and
  provide for a just and fair award at the lowest possible cost.

14.9.6 Quotation and Tender Requirements

The following quotation and tender requirements are the minimum needed. Additional quotations or undertaking a tender process should be considered where the nature of the goods or services being acquired warrants it.

Value of Order/Agreement	Requirement
Should circumstances require	Tendering process & Tender Board approval required
$20,000 and above	3 written quotations
$1,001 to $19,999	2 written quotations
$1,000 or less	Quotations could be waived

Note: Values above and elsewhere in this policy are gross costs, including all taxes and duties.

Transactions must be valued as a total transaction and not split into components or parts such as installments or individual items.

Regular or periodic orders for the same goods or service should be assessed as a minimum at the annual transaction value.

The need to obtain quotations or tenders may be waived in the following circumstances.

a) Exceptional circumstances where it is impractical to devote the time or other resources to obtaining quotations or tenders; or

b) The equipment or service is available from only one supplier.

14.9.7 Purchase Requisitions are not to be Artificially Divided

It is a violation of policy to split individual orders into multiple smaller orders for the purpose of circumventing this policy.

Artificial division of purchases can be outlined as follows.

a) Department submitting two or more requisitions to the same vendor, similar vendors, or for like or similar commodities in order to avoid bid requirements or to avoid the formal solicitation of sealed bid.

b) Multiple requisitions received in the Purchasing Office on the same day, or within the same week or month to the same vendor, similar vendors or for like or similar commodities.

c) Multiple requisitions staggered to arrive in the Purchasing Office with the same requisition date and/or sequential requisition numbers to the same vendor, similar vendors or for like or similar commodities.

d) Recurring pattern of requisitioning over the course of a fiscal year for like commodities from the same vendor or similar vendors.

Individual departments will be held accountable for violations of these regulations.

The Purchasing Office will attempt to enforce these regulations by combining requisitions it interprets as possible violation of the policy. If requisitions are combined by the Purchasing Office, the necessary bids will be solicited unquestioned, unless the requisition is accompanied by a suitable explanation for dividing a purchase.

In a few cases, there are daily or weekly recurrences of small noncompetitive purchases necessary to perform unanticipated remedial maintenance.

14.9.8 Purchase Requisitions

Requisition Forms are available at the Purchasing Office. These forms are used to request that the Purchasing Office procure materials or services.

14.9.9 Rejection of forms

The Purchasing Office normally will reject requisitions when:

a) The items are not relevant to the effective operation of the University.

b) The forms have insufficient information, such as:

1. required signatures
2. required attachments
3. incomplete specifications
4. proper account number.

c) There are insufficient funds in the departmental budget.

14.9.10 Tendering

Tendering is done by the calling of an Expression of Interest that results in an assessed list of suitable bidders.

The Purchasing Manager must approve all advertisements for the expression of Interest.

Selective Tendering may be used instead in special circumstances. Selective tendering occurs when specific suppliers are invited to tender for the goods or services rather than the tender being open to all suppliers.

Selective tendering will generally be used following an Expression of Interest. The Purchasing Manager along with the Vice President for Finance and Administrative Affairs must approve all Selective Tender proposals.

14.9.11 Bid Evaluation Process

The requisitioning department usually evaluates its own bids and makes recommendations as to the bid award, but the final decision will be by the Purchasing Office.

Beginning with the lowest bid, a determination must be made if criteria were met and the bid is acceptable. If the low bid meets specifications and is acceptable, an indication is made on the summary sheet and the bid can then be awarded.

If the low bid is not acceptable, reasons must be documented and the process is repeated for the next low bid. Red is used to note reasons for rejecting a bid on the summary sheet. A separate memo may also be attached.

14.9.12 University Purchase Order

University Purchase Orders are to be issued for all purchases.

14.9.13 Receipt of Goods and/or Services

The authorized person taking delivery of the goods and/or service will certify (sign and date) the invoice that all of the goods were received in good order and condition or all of the service was satisfactorily performed. Where goods and/or services were found to be faulty, improperly performed or not as specified the supplier must be immediately contacted and details noted on the invoice or order. If goods are returned to the supplier, details must be noted on the invoice and order and the supplier should not be paid for the returned goods.

14.9.14 Payment for Goods and/or Services

The Purchasing Office will not authorize payment for goods or services if:

a) A statement, packing slip, or acknowledgment is attached rather than an invoice,

b) The invoice is not an original,

c) The attached invoice is made out to an individual. Invoices must read Bethlehem University/ Department of _____.

14.9.15 Service or Maintenance Agreements

Maintenance or service agreements may be obtained for any equipment or software, which requires regular maintenance or service for continuous, efficient operation. Equipment typically covered by service agreements includes such items as office equipment, computing equipment and software, and specialized research equipment. In case an office needs a certain service for office equipment, the Computer Center staff should be first approached. In case that the Computer Center staff cannot fix a problem, the purchasing procedure should be followed through the Office of the Purchasing Manager to locate an external vendor for such a service.

14.9.16 Disposal of equipment

Any department or division within the University, upon determining that an item is surplus to its needs, shall report this to the Purchasing Manager.

The department chairperson or administrative head shall be responsible for preparing the surplus property for disposal.

Sale within the University The Purchasing Office shall offer surplus items to other departments/divisions within the University. Sale price shall be as agreed upon by the Purchasing Office and the buying and selling departments.

Sale outside the University If no need exists in other departments or divisions, the value of the item will be determined by the Purchasing Office, and the property will be disposed of by either of the following methods.

a) Items valued at less than $100 may be sold by the Purchasing Office by direct sale, auction or sealed bids.

b) Items valued at more than $100 will be sold by public auction or sealed bids unless the purchasing manager it is in the best interests of the University to sell by other methods.

Donating Assets: Assets that are not of use to Bethlehem University may be donated to organizations that might need them upon the recommendations of the department involved and the approval of the Vice President for Finances and Administrative Affairs.

Procedures to be Followed: University assets may not be sold externally without publicly advertising their availability. The sale of an asset to a staff member is considered to be an external sale, and staff members are required to bid for items in response to a tender advertisement. Exception to this policy may exist where the cost of advertising externally will not show an appropriate return to cover the costs. In this instance the Financial Vice President may approve in lieu of the advertising for tender, the internal sale to staff members. Justification for this deviation is to be documented in writing. Once approved all staff of the University must have the opportunity to bid having been advised of the items for sale through the University Intranet.

When selling an asset externally the procedure is as follows.

a) Place an advertisement in the local newspaper (or intranet) and any other publications appropriate to the type and value of equipment to be sold. The following details must be included.

   1. Information regarding the model/year, condition and number of items to be disposed of.
   2. A contact name and telephone number to arrange inspection of the items available, or to obtain a written specification for items of a more complex nature.
   3. The closing date for quotations/tenders must be a minimum of fourteen (14) days following the date of advertising.
   4. Indication that the quotation /tenders are to be addressed to the Vice President of Finances and Administrative Affairs and clearly marked with the name and the number of the tender advertisement.
   5. Include the following statement in the advertisement. “The University is not obliged to accept the highest quote or any quote.” This statement may be deleted if it is already been included in the specifications.

b) Forward to the Purchasing Manager a copy or draft of the advertisement for approval with details of the Asset Identification Numbers of the items if they are not included in the advertisement.

c) At the closing time and date the responses will be opened in the Finance Office in the presence of two (2) finance officers.

d) Members of the Faculty/Division selling the items may attend.

e) The responses will be date stamped and recorded and then forwarded to the Faculty/Division for analysis.

f) When a decision is reached as to acceptance of any of the quotations, notify the Purchasing Manager of details of the successful tender. Advice to the party offering the successful tender may be verbal or written depending on the nature and value of the items. Those who made the unsuccessful tenders may then be advised.

14.9.17 Inventory Records

Bethlehem University must maintain official inventory records for all non-expendable, movable property and equipment which has a single item cost of $1,000 or more, or is a gift with equal value, and:

a) has an expected useful life of one (1) year or more;

b) is self-contained for its primary function (not a component part of any other piece of equipment); and

c) has sufficient individuality and size to make control feasible by means of identification tag, number and/or manufacturer's serial number marked thereon.

Responsibilities

Purchasing Office

The Purchasing Office is responsible for:

a) establishing and maintaining the records and procedures necessary for the accountability of the University property and equipment inventory,

b) providing a list of all inventoried items to each department chairperson or administrative head on an annual basis, and providing a similar list to the Accounting Department on June 30 of each year,

c) determining the items to be inventoried and the numbers assigned,

d) affixing the inventory tag to the property or equipment,

e) proving equipment, which has been acquired through grants, with a unique designator as part of its inventory record to indicate its source.

Unit Supervisor

Each department chairperson or administrative head is responsible for:

a) all property and equipment purchased or constructed for and assigned to the department,

b) reporting any transfers or loss of inventoried property to the Purchasing Department,

c) establishing appropriate controls for all products purchased with University funds, and maintaining records and controls for equipment such as cameras, computers, printers, pocket calculators, etc.,

d) notifying the Purchasing Office of equipment that has been obtained from donations. Items received shall be entered on the records at fair market value,

e) verifying inventory records provided by the Purchasing Department annually. Specifically each chairperson must:

    1. check the accuracy of the inventory account list,
    2. certify that the equipment listed is on hand, usable, useful and needed,
    3. return the corrected inventory lists by the prescribed deadline.

Note: University property shall not be donated, destroyed or otherwise disposed of without the permission of the Vice President of Finances and Administrative Affairs.

14.10 Next Scheduled Review

March 2012

14.11 Approved By

Bethlehem University Executive Council

14.12 Date of Approval

March 2010

14.13 Revisions History

15 Data Backup and Restoration Policy

15.1 Policy Type

Information Technology Policy

15.2 Contact Office

Bethlehem University Computer Center(BUCC)

15.3 Oversight Executive

Director of Instructional Technology

15.4 Implementing Body

Computer Center Staff

15.5 Applies to

This policy applies to all electronic data which is stored on Bethlehem University servers and University data and information which is stored on local drives of computers owned by the University and used by B.U. employees.

15.6 Purpose of the Policy

The purpose of this policy is to define the process of backup and restoration of University data. The backup system is primarily for the restoration of files in a disaster recovery situation but may also be used for restoration of lost or damaged user and system files.

15.7 Policy Summary

Bethlehem University backs up data on its servers on a daily basis. This includes all of the data which individual users (students, faculty, staff and administrators) store on their personal "H-Drive." Computer Center staff are responsible for preserving this data for emergency and archival purposes. Users are responsible for keeping essential information on their "H-Drive" where it is backed up regularly or taking the necessary steps to insure that there is a backup copy of all necessary information. Administrators are responsible for making sure that all critical data for their area of responsibility is kept on a computer and backed up on a regular basis.

15.8 Definition of terms

15.8.1 Backup

A process by which server files are copied from disk to tape and/or disk to disk.

15.8.2 Backup Verify

A comparison of data collected by the backup to the source data. Full Backup will include all files selected on the backup selection list for each server.

15.8.3 Duplicate Backup

A complete copy of a Full Backup

15.8.4 Full Backup

A copy of the files on each server including all data files and all programs, both locally produced and purchased

15.8.5 Incremental Backup

Includes all files changed since the last Full or Incremental Backup

15.9 Policy Statement

It is the responsibility of the Computer Center Staff to ensure that all University data that is kept in electronic format is available for use when it is needed. For that reason this policy outlines the University backup and retention process. University operating information as well as the on-going computer work of all employees will be backed up and available for restoration in case of a loss of data due to small scale hardware malfunction, human error or a catastrophic event. Student data will be backed up and restored as a courtesy to the students. However, it is the student's responsibility to systematically backup his/her own work.

15.9.1 Backup Implementation

Full backups of all programs in use, data from the Academic, Development, Finance and Personnel Offices as well as the data currently on the H-Drives of individual users will be made on a regular basis and kept in safe locations as described in this policy. Data restoration is available from the Bethlehem University Computer Center in the event of a computer failure or accidental erasure of files.

15.9.2 Data Backup Policy

The Computer Center will perform periodic backups on designated servers and shared folders as listed below.

a) Daily Incremental Backup: Each day a daily backup is performed to only include modified and new files.

b) Weekly Full Backup: Each Friday a full backup will be performed. Weekly backups are kept up to one month.

c) Monthly Full backups: The last Friday of each month a full backup is performed and saved for one year.

d) Off-Site Backup: a full backup will be performed each month to be kept off-site (somewhere on campus).

e) Off-Site Semester Backup: At the end of each semester a full backup will be performed, and the media will be kept in a secure location outside the campus.

f) Annual Archive: At the end of each academic year a Full Backup will be retired to the permanent archives for historical purposes.

15.10 Next Scheduled Review

March 2012

15.11 Approved By

Bethlehem University Executive Council

15.12 Date of Approval

March 2010

15.13 Revisions History

16 Data Retention and Removal Policy

16.1 Policy Type

Information Technology Policy

16.2 Contact Office

Bethlehem University Computer Center (BUCC)

16.3 Oversight Executive

Director of Instructional Technology

16.4 Implementing Body

Supervisor of the Computer Center

16.5 Applies to

This policy applies to all electronic data which is stored on Bethlehem University servers and University data and information which is stored on local drives of computers owned by the University and used by B.U. employees.

16.6 Purpose of the Policy

The purpose of this policy is to provide a consistent guide for managing disk space and protecting electronically stored data on Bethlehem University's (BU) network servers. By implementing and maintaining a data retention policy, the University will be able to better manage disk space, keep backup times acceptable and ensure the protection of Bethlehem University's data. This policy applies to all B.U. employees and students. Employees or students who violate this policy shall be subject to disciplinary action. This policy applies to all computer systems utilized by B.U.

16.7 Policy Summary

This policy provides specific information about where official University records should and should not be kept. It also provides requirements for the storing of and removal of data and specifies the period that data will be retained on the University servers.

16.8 Definition of terms

16.8.1 Data

Electronic information that is stored on any disks or tapes, including hard drives, magnetic tapes, floppy disks/removable media, CD/DVD, optical disks and USB flash drives.

16.8.2 Server Data

Any data that is stored on an B.U. owned server.

16.8.3 Client Data

Any data that is not stored on an B.U. owned server,

16.8.4 Confidential Business Related Data

Any data that pertains to student records, employee information or financial data.

16.9 Policy Statement

Confidential business related data may only be stored on B.U. servers and not on client computers, for example, student records may not be stored on desktop or laptop computers. All B.U. information should be stored on University servers (G: or H: drives).

Employees: Network file storage is to be used for institutional documents only. Institutional documents and network file servers are the property of B.U. and employees should have no expectation of personal privacy associated with the information they store on these systems. B.U. will refrain from accessing system user's data unless there is a reasonable cause for doing so, B.U. may review data for any system user at any time for business, policy, security, legal or personnel actions. In the event that non-institutional related data or applications are found on a user's network file share, the user will be notified and will be expected to delete it within 5 business days of notification. If the user is on vacation or "out of the office," the user's supervisor will be contacted.

When administrators or members of the staff leave the University the computer that they are using will normally be transferred to their successor. Since most of the University business and correspondence should be on the departing employee's H:-drive the departing employee should contact the BUCC and make arrangements for the transfer of the H:-drive data to the account of the replacement employee.

Other employees who leave B.U. will have their home directories written to CD within 10 days of the Computer Center's notification of their termination date. This CD will be delivered to the employee's supervisor. The supervisor is then responsible for the use or disposal of said data.

The departing employee should remove all personal materials from the computer and his/her H:-drive prior to leaving the University.

Students: Students will be given network file storage space on a B.U. owned server. This data is the property of B.U. and every attempt to protect privacy will be maintained, but observation of traffic flow and content may be necessary at the University's discretion for security and legal reasons. B.U. will refrain from accessing student's data unless there is a reasonable cause for doing so. Previous students who are no longer registered at the University will have their accounts removed within 30 days after the beginning of the semester after their departure.

E-Mail Retention: The e-mail system's capacity and performance is designed to provide an effective messaging system. Many of the messages that traverse through the e-mail system are temporary or time-sensitive messages that should be discarded routinely. However, depending on the content of the e-mail, it may be necessary to retain e-mail messages for a longer period of time. B.U. employees are asked to periodically delete unnecessary messages to keep within the allocation for each employee. Messages determined by employees and students to be necessary to keep for historical or other purposes should be archived and backed up by the employee or student in order to retain this data.

16.9.1 Disk Space Policy

Employees are given fixed amount of network file storage space for their use (H:-drive). Employees who have a requirement for additional space may contact the BUCC for a larger allocation, which will be provided, if space is available.

Students are given a smaller fixed amount of storage for their personal account.

16.9.2 File Restore Policy

File restore requests are made via the Computer Center On-line Support Form. Data restores will normally be performed within 24 hours of request in alignment with the retention periods. Files will be restored to the state they were in at the time of the most recent backup or as close to the requested date as possible.

16.9.3 Implementation

Daily: BUCC staff will make backup tapes of each server after the conclusion of each working day. The daily tapes will be kept for 7 days before they are recycled in sequence.

Monthly: Full backups of all servers are made on the last working day of each month and provided to the Director of Instructional Technology who keeps the tapes in a location outside the Computer Center. The monthly tapes are recycled in sequence.

Semester: One full backup copy is provided to the Director of Instructional Technology after the academic records for each of the Spring and Fall semesters have been finalized for storage at a site outside of Bethlehem University.

Annual: At the end of each academic year a Full Backup will be retired to the permanent archives for historical purposes.

16.10 Next Scheduled Review

March 2012

16.11 Approved By

Bethlehem University Executive Council

16.12 Date of Approval

March 2010

16.13 Revisions History

17 Appendix

Glossary Terms

Term	Definition
Access	Permission, privilege or ability to read, enter, update, manage or administer computer information in some manner. The level of access is determined by the specific job of the user. For example, a user might be granted read access to a file, meaning that the user can read the file but cannot modify or delete it. Most operating systems have several different types of access privileges that can be granted or denied to specific users or groups of users.
Alumni Information	All information maintained by the Development Office pertaining to graduates of the University such as names, degrees, program(s) attended, years attended, graduation date(s) and all other information gathered by the University after the person is no longer enrolled as student.
Archiving/Storage	The act of physically or electronically moving inactive or other records to a storage location until the record retention requirements are met or until the records are needed again.
Attachment	An e-mail attachment is a computer file which is sent along with an e-mail message. The file is not a separate message, but now it is almost universally sent as part of the message to which it is attached.
Authorized User	Individuals who have been granted access to specific information assets in the performance of their assigned duties are considered Authorized Users (”Users”). Users include, but are not limited to faculty and staff members, trainees, students, volunteers, contractors, or other affiliates of the University.
Backup	A process by which server files are copied from disk to tape and/or disk to disk.
Backup Verify	A comparison of data collected by the backup to the source data.
Bandwidth	In computer networking and computer science, digital bandwidth or just bandwidth is the capacity for a given system to transfer data over a connection. It is measured as a bit rate expressed in bits/second (bits/s) or multiples of it (kbit/s, Mbit/s, etc.).
Chain E-mail	E-mail sent to successive people. Typically the body of the note has direction to send out multiple copies of the note and promises good luck or money if the direction is followed.
Client Data	Any data that is not stored on an B.U. owned server

Term	Definition
Color Inkjet Printer	A printer that can produce almost photographic quality prints of text, pictures and images. While the quality is excellent, it is much slower and much more expensive than images produced by a color laser printer.
Color Laser Printer	A printer that can produce color text, drawings and pictures. The cost of color laser pages is considerably more than black and white pages.
Confidential Business Related Data	Any data that pertains to student records, employee information or financial data
Custodian of Data and Information	A university official or entity which has physical control over University information resources.
Data	Electronic information that is stored on any disks or tapes, including hard drives, magnetic tapes, floppy disks/removable media, CD/DVD, optical disks, or USB flash drives.
Data Steward	A University official who has responsibility for the data generated by his unit
Donor Information	All information related to donor such as name of donor, address, telephone numbers, gift history or any other information pertaining to the donor and maintained by the Development Office or any other unit of the University directly dealing with the donor.
Duplicate Backup	A complete copy of a Full backup
Electronic Communication	All communication via telephone, phone-mail, e-mail or computer files that traverse the University network or is stored on University equipment.
Electronic Media	All media on which electronic data can be stored, including, but not limited to: hard drives, magnetic tapes, diskettes, CDs, DVDs and USB storage devices
Electronic Messaging	A set of communication processes used to relay information among the users of computers. Electronic Messages take many forms. Examples: Electronic Mail (e-mail), FTP, cell phones, Instant Messaging and internet chat.
E-mail	Electronic mail, often abbreviated to e-mail, email, e-post or originally eMail, is a store-and-forward method of writing, sending, receiving and saving messages over electronic communication systems. It is the transmission of information through e-mail software such as Pegasus or Outlook Express. The term ”e-mail” (as a noun or verb) applies to the Internet e-mail system.
E-mail User	Any user of Bethlehem University e-mail service. It includes all those who have an account that ends with @bethlehem.edu

Term	Definition
Employee's Records	All information pertaining to non-academic staff as maintained by the Office of Personnel Development employee and to academic staff as maintained by the Office of the Vice President for Academic Affairs.
Firewall	A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both.
Forwarded e-mail	E-mail resent from an internal network to an outside point.
Full Backup	Will include all files selected on the backup selection list for each server.
Incremental Backup	Will include files changed since last Full or Incremental backup.
Information Technology Resources	Includes the use of University computer networks, the Internet, e-mail, shared folders, electronic documents, servers, and other devices.
Institutional Data	Institutional data supports the mission of Bethlehem University. It is a vital asset and is owned by the University. Institutional Data will be protected from deliberate, unintentional or unauthorized alteration, destruction, and/or inappropriate disclosure or use in accordance with established institutional policies and practices. Sensitive Data as defined in this section is a subset of Institutional Data.
Local Area Network (LAN)	A computer network (or data communications network) which is confined in a limited geographical area.
Network Account	is a username and a password that allows the user to access the system, local network, internet, and e-mail.
Network Printer	A printer that is connected to a number of computers, each of which can send print jobs to the printer.
Network Resources	Any devices attached to BU network and any services made available over the network. Devices and services include network servers, peripheral equipment, workstations and personal computers (PCs).
Planned Interruption	A pause in computer services which is known and scheduled in advance. These would be things like upgrades to a server, installing programs on a group of computers that require the blocking of user logins, server maintenance in a public lab that causes certain software or functions like printing to be unavailable, or planned activity by the Physical Plant Department that affects electrical or network service to buildings where computer equipment is installed.
Registered Students	Those students who are enrolled in a credit class during the current semester, or the upcoming semester, and whose fees are up to date.
Remote Access	Is the ability to get access to a computer or a network from a distance.

Term	Definition
Restricted Data	Data whose access is restricted by University statutes. For purposes of this policy, restricted data is a subset of sensitive data.
Security Incidents	Any type of attack on PC or server that attempts to compromise or damage the equipment. Attacks may range from a simple Virus on a PC to hacking a server.
Sensitive Data	Data, regardless of its physical form or characteristics, with the highest level of protection including, but not limited to, data protected by law, data protected by legal contracts, or security-related data. It also includes data that is not open to public examination because it contains information which, if disclosed, could cause severe reputation, monetary or legal damage to individuals or the University or compromise public activities. Examples include: passwords, intellectual property, on-going legal investigations, medical or grades information protected by legal or University policies, ID numbers, birth dates, professional research, graduate student work, bank account numbers, income and credit history.
Sensitive information	Information is considered sensitive if it can be damaging to Bethlehem University or its stakeholders' reputation or market standing.
Server Data	Any data that is stored on an B.U. owned server
Spam	Spamming is the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages to thousands of recipients.
Student's Academic Records	Any records (on computer, electronic, print, or handwriting) maintained by the Registrar's Office that relate directly to the student. By contrast, student records maintained by the advisor for advising purposes, medical records kept at the University Clinic for treatment purposes, and records pertaining to the employment of the student in the University do not constitute part of the student's academic records.
Student's Financial Records	All records pertaining to the student's financial status in the University maintained by the Finance Office.
System Administration	System Administration refers to specific responsibilities and assigned tasks of the System Administrator. Such tasks include, but are not limited to: installing, supporting, and maintaining operating systems, database management systems, application software and hardware; planning for, trouble-shooting and responding to system problems or outages; and providing knowledgeable facts about the use of the system in the organization.

Term	Definition
System Administrator	Any individual who oversees or has administrative access/rights to any Information Technology Resource at Bethlehem University.
Unauthorized Disclosure	The intentional or unintentional revealing of restricted information to people, both inside and outside Bethlehem University, who do not have a need to know that information.
University Public Records	All University records pertaining to the conduct of the administrative business of the University, such as the University Catalog, the Academic Staff Handbook, The Administrative Support Staff Handbook, and any information posted on the University's main Website.
Unplanned Interruption	A pause in computer service which is not known in advance. Some things, like power cuts from the electric company or accidental disconnection of a network cable, are beyond the control of BUCC and definitely are not planned. However, there can also be unplanned interruptions such as when a network has to be shut down to repair a damaged server.
User	Members of the faculty, staff, students or any person who has permission to access the IT resources and facilities of Bethlehem University.
Username	Is a unique code assigned to each user by the Bethlehem University Computer Center. When used with a password chosen by the user, the username allows access to the computing facilities of the University.
Virus Warning	E-mail containing warnings about virus or malware. The overwhelming majority of these e-mails turn out to be a hoax and contain bogus information usually intent only on frightening or misleading users.
Virus	A computer virus is a computer program that can copy itself and infect a computer without permission or knowledge of the user. The original virus may modify the copies, or the copies may modify themselves. A virus can only spread from one computer to another when its host is taken to the uninfected computer, for instance by a user sending it over a network or the Internet, or by carrying it on a removable medium such as a floppy disk, CD, or USB drive.
VNC (Virtual Network Computing)	A graphical desktop sharing system that uses the network to remotely control another computer. It transmits the keyboard and mouse events from one computer to another, relaying the graphical screen updates back in the other direction.
Worm	A computer worm is a self-replicating computer program. It uses a network to send copies of itself to other computers on the network can do so without user intervention.