BETHEL UNIVERSITY

User Information Security Policy

Jimmy Bomar

731-352-4034
bomarj@bethelu.edu

Table of Contents

1.0 Acceptable Use Policy

1.1.0 Overview

Bethel University’s intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Bethel University’s established culture of openness, trust and integrity. Bethel University is committed to protecting employees, partners and the university from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, system accounts, electronic mail, web browsing, and all other digital communication protocols and services, are the property of Bethel University. These systems are to be used for business purposes in serving the interests of students, clients, and of the University in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every Bethel University employee and affiliate who deals with information and/or information systems. It is the responsibility of every systems user to know these guidelines and to conduct their activities accordingly.

1.2.0 Purpose

The purpose of this policy is to outline the acceptable use of all information systems and equipment at Bethel University. These rules are in place to protect the employee and Bethel University. Inappropriate use exposes Bethel University to risks including but not limited to virus attacks, compromise of network systems and services, and legal issues.

1.3.0 Scope

This policy applies to employees, contractors, consultants, temporaries, and all other workers at Bethel University, including all personnel affiliated with third parties. Additionally, this policy applies to all equipment that is owned or leased by Bethel University.

1.4.0 Policy

1.4.1 General Use and Ownership

1. While Bethel University's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the university systems remains the property of Bethel University. Because of the need to protect Bethel University's network, management cannot guarantee the confidentiality of information stored on any network device belonging to Bethel University.
2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
3. Employees are responsible in making sure that all Bethel University data remains entirely on university systems and equipment. Additionally,

Employees are responsible for making sure that personal data remains entirely on personal equipment.

4. Bethel University recommends that any information that users consider sensitive or vulnerable be stored on university provided shares. For guidelines on information classification, see the *Information Sensitivity Policy*.
5. For security and network maintenance purposes, authorized individuals within Bethel University may monitor equipment, systems and network traffic at any time, per the *Audit Vulnerability Scanning Policy*.
6. Bethel University reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

1.4.2 Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by university confidentiality guidelines, details of which can be found in Human Resources policies. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System and user level passwords should comply with the guidelines defined in the *Password Protection Policy.*
3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less or by logging-off when the host will be unattended.
4. Use encryption of information in compliance with the *Acceptable Encryption Policy*.
5. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the *Mobile Computing and Storage Devices Policy*.
6. Postings by employees from a Bethel University email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Bethel University, unless posting is in the course of business duties.
7. All hosts used by the employee that are connected to the Bethel University Internet/Intranet/Extranet, whether owned by the employee or Bethel University, shall be continually executing approved virus-scanning software with a current virus database. Unless overridden by departmental or group policy.
8. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

1.4.3. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an employee of Bethel University authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Bethel University-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Bethel University.
2. Unauthorized copying of copyrighted material (Copyright Infringement) including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Bethel University or the end user does not have an active license is strictly prohibited. Copyright infringement is the act of exercising, without permission or legal authority, one or more of the exclusive rights granted to the copyright owner under section 106 of the Copyright Act (Title 17 of the United States Code). These rights include the right to reproduce or distribute a copyrighted work. In the file-sharing context, downloading or uploading substantial parts of a copyrighted work without authority constitutes an infringement.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using a Bethel University computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any Bethel University account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless approved by the security specialist for Bethel University.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about, or lists of, Bethel University employees to parties outside Bethel University.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within Bethel University's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Bethel University or connected via Bethel University's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

1.5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Violators are also subject to civil and criminal liabilities.

Penalties for copyright infringement include civil and criminal penalties. In general, anyone found liable for civil copyright infringement may be ordered to pay either actual damages or "statutory" damages affixed at not less than $750 and not more than $30,000 per work infringed. For "willful" infringement, a court may award up to $150,000 per work infringed. A court can, in its discretion, also assess costs and attorneys' fees. For details, see Title 17, United States Code, Sections 504, 505.

Willful copyright infringement can also result in criminal penalties, including imprisonment of up to five years and fines of up to $250,000 per offense.

For more information, please see the Web site of the U.S. Copyright Office at www.copyright.gov, especially their FAQ's at www.copyright.gov/help/faq.

1.6.0 Terms and Definitions

Term	**Definition**
Spam	Unauthorized and/or unsolicited electronic mass mailings.

1.7.0 Revision History

2.0 Password Protection Policy

2.1.0 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen or poorly handled password may result in the compromise of Bethel University's entire university network. As such, all Bethel University employees (including contractors and vendors with access to Bethel University systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.2.0 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

2.3.0 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Bethel University facility, has access to the Bethel University network, or stores any non-public Bethel University information.

2.4.0 Policy

2.4.1 General Rules

System and user level passwords should comply with the guidelines defined below:

- All system-level passwords (e.g., root, enable, admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All production system-level passwords must be part of the administered global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every four months.
- User accounts that have system-level privileges granted through group memberships must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication unless they are being used as a one-time pass with enforced password change upon first login.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- All user-level and system-level passwords must conform to the guidelines described below.

2.4.2 General Guidelines

- Passwords are used for various purposes at Bethel University. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

- Poor, weak passwords have the following characteristics:
    - The password contains less than eight characters
    - The password is a word found in a dictionary (English or foreign)
    - The password is a common usage word such as:
        - Names of family, pets, friends, co-workers, fantasy characters, etc.
        - Computer terms and names, commands, sites, companies, hardware, software.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Any of the above spelled backwards.
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)
- Strong passwords have the following characteristics:
    - Contain both upper and lower case characters (e.g., a-z, A-Z)
    - Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
    - Are at least eight alphanumeric characters long.
    - Are not a word in any language, slang, dialect, jargon, etc.
    - Are not based on personal information, names of family, etc.
    - Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

2.4.3 General Use

- Do not use the same password for Bethel University accounts as for other non Bethel University access (e.g., personal ISP account, option trading, benefits, etc.).
- Where possible, don't use the same password for various Bethel University access needs. For example, select one password for the email system and a separate password for the portal. Also, select a separate password to be used for a Microsoft account versus a UNIX account.
- Do not share Bethel University passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential Bethel University information.

2.4.4 Restrictions

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation or for any other reason

If someone demands a password, refer them to this document or have them call someone in the Information Technology Department.

Do not use the "Remember Password" feature of applications (e.g., Gmail, Google+).

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including iPads or similar devices) without encryption.

Change passwords at least once every four months (except system-level passwords which must be changed quarterly).

If an account or password is suspected to have been compromised, report the incident to IT and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by IT or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

2.4.5 Application Development Standards

Application developers must ensure their programs contain the following security precautions.

Applications:

- Should support authentication of individual users, not groups.
- Should not store passwords in clear text or in any easily reversible form.
- Should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- Should support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

2.4.6 Guidelines for Remote Access Users

Access to the Bethel University Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase or password.

Passphrases: Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks." A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

2.5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

2.6.0 Terms and Definitions

Term	**Definition**
Dictionary Attack	A Dictionary Attack is a form of Brute Force. An attacker obtains A username and then tries commonly used passwords, which can be pulled from a dictionary database.

2.7.0 Revision History

3.0 Acceptable Encryption and Hashing Policy

3.1.0 Purpose

The purpose of this policy is to provide guidance that limits the use of encryption and hashing to those algorithms that have received substantial public review and have been proven to work effectively. This policy also explicitly denies the use of encryption or hashing within the university unless reviewed and permitted by Bethel University's designated security specialist. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

3.2.0 Scope

This policy applies to all Bethel University employees and affiliates.

3.3.0 Policy

Proven, standard algorithms should be used as the basis for encryption and hashing technologies. These algorithms represent the actual cipher used for an approved application. Examples of approved standard algorithms are listed below:

Encryption
Data Encryption Standard (DES)
Triple Data Encryption Standard (TDES)
International Data Encryption Algorithm (IDEA)
Advanced Encryption Standard (AES)
Blowfish
RSA
RC4
RC5
Deffie-Hellman

Hashing
MD5
Secure Hashing Algorithm (SHA)
Keyed-Hashing for Message Authentication (HMAC)
Universal Hash Function (UHASH)

Symmetric cryptosystem key lengths must be at least 56 bits. Asymmetric cryptosystem keys must be of a length that yields equivalent strength. Bethel University's key length requirements will be reviewed annually and upgraded as technology allows.

Use of encryption or hashing within the university is explicitly prohibited unless reviewed and permitted by Bethel University's designated security specialist. The use of proprietary encryption or hashing algorithms is not allowed for any purpose unless reviewed and permitted by Bethel University's designated security specialist.

Be aware that the export of encryption technologies is restricted by the U.S. Government. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

3.4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

3.5.0 Terms and Definitions

Term	**Definition**
Hashing	A mathematical summary that can be used to provide message integrity.
Encryption	The process of coding data so that a specific code or key is required to restore the original data.
Proprietary Encryption	An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.
Symmetric Cryptosystem	A method of encryption in which the same key is used for both encryption and decryption of the data.
Asymmetric Cryptosystem	A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (e.g., public-key encryption).

3.6.0 Revision History

4.0 Mobile Computing and Storage Devices Policy

4.1.0 Overview

With advances in computer technology, mobile computer and storage devices have become useful tools to meet the needs of Bethel University. These devices are especially susceptible to loss, theft, hacking, and the distribution of malicious software because they are easily portable and can be used anywhere. As mobile computing becomes more widely used, it is necessary to address security to protect information resources at Bethel University.

4.2.0 Purpose

The purpose of this policy is to establish an authorized method for controlling mobile computing and storage devices that contain or access information resources at Bethel University.

4.3.0 Scope

The scope of this policy includes all personnel who have or are responsible for a mobile computing or storage device at any Bethel University facility. It also applies to mobile devices owned or operated by third parties who will be interacting with Bethel University's information resources.

4.4.0 Policy

4.4.1 General Policy

It is the policy of Bethel University that mobile computing and storage devices containing or accessing the information resources of Bethel University must be approved prior to connecting to the information systems. This pertains to all devices connecting to the network at Bethel University regardless of ownership.

Mobile Computing and storage devices include, but are not limited to: laptop computers, Smart phones, Universal Serial Bus (USB) port devices, Compact Discs (CDs), Digital Versatile Discs (DVDs), flash drives, modems, handheld wireless devices, wireless networking cards, and any other existing or future mobile computing or storage devices, either personally owned or Bethel University owned, that may connect to or access the information systems at Bethel University. A risk analysis for each new media type shall be conducted and documented prior to its use or connection to the network at Bethel University unless the media type has already been approved by the Information Technology Department.

Mobile computing and storage devices are easily lost or stolen, presenting a high risk for unauthorized access and introduction of malicious software to the network at Bethel University. These risks must be mitigated to acceptable levels.

Bethel University provides all employees that use mobile devices with personal and group based network storage. Individuals with mobile devices that must access these resources from remote locations are given secured VPN accounts. Since all employees are given access to these network resources, private, confidential, and sensitive information should be stored on secured network resources and not directly on mobile devices.

Unless written approval has been obtained from the designated Information Security representative for Bethel University, databases or portions thereof, which reside on the network at Bethel University or on Bethel University's hosted networks, shall not be downloaded to mobile computing or storage devices.

Compliance with this policy is mandatory.

4.4.2 General Procedures

To report lost or stolen mobile computing and storage devices, call the Bethel University Help Desk. If the user of the lost or stolen equipment adequately followed the guidelines of this policy, there will be little to no threat of compromised confidential or sensitive data. The user should be prepared to answer any questions concerning the data on their mobile computing or storage device.

The Bethel University Information Technology department shall approve all new mobile computing and storage devices that may connect to the information systems at Bethel University. Mobile computing or storage devices that have not been approved by the Information Technology staff should never be connected to Bethel University's information systems without prior approval.

Any requests for an exception to this policy must be submitted to the Information Technology staff for review and consideration.

4.4.3 Roles and Responsibilities

Users of mobile computing and storage devices must diligently protect such devices from loss of equipment and disclosure of private information belonging to or maintained by Bethel University. Mobile devices may be audited at any time by members of the Information Technology staff to ensure that the user is taking the necessary precautions to comply with this policy.

The **Help Desk** must be notified immediately upon detection of a security incident, especially when a mobile device may have been lost or stolen.

The **Information Technology Department** is responsible for the *Mobile Computing and Storage Devices Policy* at Bethel University and shall conduct a risk analysis to document safeguards for each media type to be used on the network or on equipment owned by Bethel University.

The **Information Technology Department** is responsible for developing procedures to implement and enforce this policy including performing the necessary audits to ensure compliance.

4.5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

4.6.0 Terms and Definitions

Term	**Definition**
CD	A *compact disc* (sometimes spelled *disk)* is a small, portable, round medium made of molded polymer (close in size to the floppy disc) for electronically recording,

storing, and playing back audio, video, text, and other information in digital form.

DVD

The *digital versatile disc* stores much more than a CD and is used for playing back or recording movies. The audio quality on a DVD is comparable to that of current audio compact discs. A DVD can also be used as a backup media because of its large storage capacity.

Flash Drive

A plug-and-play portable storage device that uses flash memory and is lightweight enough to attach to a key chain. The computer automatically recognizes the removable drive when the device is plugged into its USB port. A flash drive is also known as a keychain drive, USB drive, or disk-on-key. A keychain drive, which looks very much like an ordinary highlighter marker pen, can be used in place of a floppy disk, Zip drive disk, or CD.

Media Type

For the purpose of this policy, the term "media type" is interchangeable with "mobile device." Not to be confused with media makes, models, or brands.

Mobile Devices

Mobile media devices include, but are not limited to: PDAs, plug-ins, USB port devices, CDs, DVDs, flash drives, modems, handheld wireless devices, and any other existing or future media device.

Modems

A device that modulates and demodulates information so that two computers can communicate over a phone line, cable line, or wireless connection. The connection talks to the modem, which connects to another modem that in turn talks to the computer on its side of the connection. The two modems talk back and forth until the two computers have no further need of either modem's translation services.

4.7.0 Revision History

5.0 Personal Communication Devices and Voicemail Policy

5.1.0 Overview

With advances in computer technology, Personal Communication Devices (PCDs) have become a necessity to meet the business needs of Bethel University. These devices are especially susceptible to loss, theft, hacking, and compromise due to them being portable. As Personal Communication Devices and Voicemail are used, it is necessary to address security to protect these information resources at Bethel University.

5.2.0 Purpose

This document describes Information Security requirements for Personal Communication Devices and Voicemail for Bethel University.

5.3.0 Scope

This policy applies to any use of Personal Communication Devices and Voicemail issue by Bethel University or for Bethel University business purposes.

5.4.0 Policy

5.4.1 Issuing Policy

Personal Communication Devices (PCDs) will be issued only to Bethel University personnel with duties that require them to be in immediate and frequent contact when they are away from their normal work locations. For the purpose of this policy, PCDs are defined to include handheld wireless devices, cellular telephones, laptop wireless cards and pagers. Effective distribution of the various technological devices must be limited to persons for whom the productivity gained is appropriate in relation to the costs incurred.

Handheld wireless devices may be issued, for operational efficiency, to Bethel University personnel who need to conduct immediate and critical Bethel University business. These individuals generally are at the executive and management level. In addition to verbal contact, it is necessary that they have the capability to review and have documented responses to critical issues.

5.4.2 Bluetooth

Hands-free enabling devices, such as the Bluetooth, may be issued to authorized Bethel University personnel who have received approval. Care must be taken to avoid being recorded when peering Bluetooth adapters; Bluetooth 2.0 Class 1 devices have a range of 330 feet.

5.4.3 Voicemail

Voicemail boxes may be issued to Bethel University personnel who require a method for others to leave messages when they are not available. Voicemail boxes must be protected by a PIN which must never be the same as the last four digits of the telephone number of the voicemail box.

5.4.4 Loss and Theft

Files containing confidential or sensitive data may not be stored in PCDs unless protected by approved encryption in accordance with the *Acceptable Encryption Policy*. Confidential or sensitive data shall never be stored on a personal PCD. Charges for repair due to misuse of equipment or misuse of services may be the responsibility of the employee, as determined on a case-by-case basis. The cost of any item beyond the standard authorized equipment is also the responsibility of the employee. Lost or stolen equipment must immediately be reported.

5.4.5 Personal Use

PCDs and voicemail are issued for Bethel University business. Personal use should be limited to minimal and incidental use.

5.5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action that leads to being ineligible for continued use of PCDs. Extreme cases could lead to additional discipline, up to and including termination of employment.

5.6.0 Terms and Definitions

Term	**Definition**
Bluetooth	Bluetooth is an industrial specification for wireless personal area networks (PANs), also known as IEEE 802.15.1. Bluetooth provides a way to connect and exchange information between devices such as personal digital assistants (PDAs), and mobile phones via a secure, globally unlicensed short-range radio frequency.

5.7.0 Revision History

6.0 Anti-Virus Policy

6.1.0 Purpose

Establish requirements which must be met by all computers connected to Bethel University networks to ensure effective virus detection and prevention.

6.2.0 Scope

This policy applies to all Bethel University computers that are PC-based or utilize PC-file directory sharing. This includes, but is not limited to, desktop computers, laptop computers, servers, and any PC based equipment such as traffic generators.

6.3.0 Policy

All Bethel University PC-based computers must have Bethel University's standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date. Virus-infected computers must be removed from the network until they are verified as virus-free. Network Managers are responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into Bethel University's networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited, in accordance with the *Acceptable Use Policy*.

Noted exceptions: Smart phones, iPads, and machines with operating systems other than those based on Microsoft/Apple/Linux products are not accepted at the current time.

6.4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.5.0 Terms and Definitions

Term	Definition

6.6.0 Revision History

7.0 Email Use and Retention Policy

7.1.0 Overview

Bethel University's intentions for publishing an Email Use and Retention Policy is not to impose unnecessary restrictions that are contrary to Bethel University's established culture of openness, trust and integrity. Bethel University is committed to protecting all stakeholders from illegal or damaging actions through email communication.

7.2.0 Purpose

The Email Use and Retention Policy is intended to prevent tarnishing the public image of Bethel University. It is intended to prevent unauthorized or inadvertent disclosure of sensitive university information through email communication. Lastly, this policy is intended to help employees determine what information sent or received by email should be retained and for how long.

7.3.0 Scope

This policy covers appropriate use of any email sent from a Bethel University email address and applies to all employees, vendors, and agents operating on behalf of Bethel University.

7.4.0 Policy

7.4.1 Prohibited Email Content

Bethel University email systems shall not be used for the creation or distribution of any disruptive or offensive messages, including but not limited to offensive comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this type of content from any Bethel University employee should report the matter to their supervisor immediately.

7.4.2 Prohibited Email Activity

Prohibited email activity includes but is not limited to email communication in the form of chain letters, jokes, SPAM, virus distribution, malware distribution, and non-business related mass mailings. Business related mass mailings must be approved and sent out by a designated employee of the HR staff.

7.4.3 Email Forwarding

Employees must exercise utmost caution when sending any email from inside Bethel University to an outside network. Unless approved by the designated Information Security specialist, Bethel University email will not be automatically forwarded to any external destination. Sensitive information will not be forwarded via any means, unless that email is critical to business and is encrypted according to the *Acceptable Encryption Policy*.

7.4.4 Personal Use

Bethel University employees are allowed to use a reasonable amount of university resources for personal emails as long as the email communication complies with this policy. Employees must keep their personal email separated into a different organizational folder so that university and personal data are kept separate.

7.4.5 Email Retention

All ingoing and outgoing email will be copied and stored in an Enterprise Archive where it will be retained for 7 years. Email communication in the archive can be referenced at anytime by approved personnel. Email retention is done on a global level and thus employees are not responsible for their personal email retention. Employees may keep or delete email as they see fit as long as they do not exceed their assigned mailbox size.

7.5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

7.6.0 Terms and Definitions

Term	**Definition**
Email	The electronic transmission of information through mail protocols such as SMTP or IMAP. Typical email clients include Eudora and GMail.
Forwarded Email	Email resent from one internal account to one or more internal or external accounts.
Chain Email or Letter	Email sent to successive people. Typically the body of the email or letter includes directions that encourage the recipient to send out copies of the email to multiple people. Emails of this nature often promise good luck or money if the direction is followed.
Sensitive Information	Information is considered sensitive if it can be damaging to Bethel University or its customers' reputation or market standing.
Virus/Malware	Mobile malicious code that may cause harm to information systems.
Encryption	Secure Bethel University Sensitive information in accordance with the *Acceptable Encryption Policy*.
Unauthorized Disclosure	The intentional or unintentional revealing of restricted information to people who do not have a need to know that information.

7.7.0 Revision History

8.0 Remote Access Policy

8.1.0 Purpose

The purpose of this policy is to define standards for connecting to Bethel University's network from any host. These standards are designed to minimize the potential exposure to Bethel University from damages which may result from unauthorized use of Bethel University resources. Damages include the loss of sensitive or university confidential data, intellectual property, damage to public image, damage to critical Bethel University internal systems, etc.

8.2.0 Scope

This policy applies to all Bethel University employees, contractors, vendors and agents with a Bethel University-owned or personally-owned computer or workstation used to connect to the Bethel University network. This policy applies to remote access connections used to do work on behalf of Bethel University, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, VPN and public Internet access over DSL, Cable modem, dial-up, ISDN and frame relay.

8.3.0 Policy

8.3.1 General

1. It is the responsibility of Bethel University employees, contractors, vendors and agents with remote access privileges to Bethel University's university network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Bethel University.
2. General access to the Internet for recreational use by immediate household members from a remote location through the Bethel University Network on personal computers is not permitted. The Bethel University employee bears responsibility for the consequences should the access be misused.
3. Please review the following policies for details of protecting information when accessing the university network via remote access methods, and acceptable use of Bethel University's network:
   a. *Acceptable Encryption Policy*
   b. *Acceptable Use Policy*
4. For additional information regarding Bethel University's remote access connection options and troubleshooting, call the IT Help Desk.

8.3.2 Requirements

1. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication and or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the *Password Protection Policy*.
2. At no time should any Bethel University employee provide their login or email password to anyone, not even family members.
3. Bethel University employees and contractors with remote access privileges must ensure that their Bethel University-owned or personal computer or workstation, which is remotely connected to Bethel University's network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.

4. Bethel University employees and contractors with remote access privileges to Bethel University's university network must not use non-Bethel University email accounts (i.e., Yahoo, Gmail), or other external resources to conduct Bethel University business, thereby ensuring that official business is never confused with personal business.
5. It is the responsibility of employees with VPN access privileges to ensure a VPN connection to Bethel University is not used by non-employees to gain access to university information system resources. An employee who is granted VPN access privileges must remain constantly aware that VPN connections between their location and Bethel University are literal extensions of the university network, and that they provide a potential path to the university's most sensitive information. The employee and/or authorized third party individual must take every reasonable measure to protect Bethel University's assets.
6. Account activity is monitored, and if a VPN account is not used for a period of six months the account will expire and no longer function. If VPN access is subsequently required, the individual must request a new account
7. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
8. Non-standard hardware configurations must be approved by IT Networking, and Information Security must approve security configurations for access to Bethel University networks.
9. All hosts that are connected to Bethel University internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers. Third party connections must comply with requirements as stated in the *Third Party Agreement*.
10. Personal equipment that is used to connect to Bethel University's networks must meet the requirements of Bethel University-owned equipment for remote access and must be approved.
11. Organizations or individuals who wish to implement non-standard Remote Access solutions to the Bethel University production network must obtain prior approval from IT Networking and Information Security.

8.4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

8.5.0 Terms and Definitions

Term	**Definition**
Cable Modem	Cable companies such as Time Warner Cable provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps.
CHAP	Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function. Data Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies

a particular PVC endpoint within a user's access channel in a frame relay network, and has local significance only to that channel.

Dial-in Modem A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.

Dual Homing Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the University network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP). Being on a Bethel University-provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into Bethel University and an ISP, depending on packet destination is another form of remote access.

DSL Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).

Frame Relay A method of communication that incrementally can go from the speed of an ISDN to the speed of a T1 line. Frame Relay has a flat-rate billing charge instead of a per time usage. Frame Relay connects via the telephone university's network.

ISDN There are two flavors of Integrated Services Digital Network or ISDN: BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signaling info.

Remote Access Any access to Bethel University's university network through a non-Bethel University controlled network, device, or medium.

Split-tunneling Simultaneous direct access to a non-Bethel University network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into Bethel University's university network via a VPN tunnel.

VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.

8.6.0 Revision History