Information Technology Policy and Procedure

Passed by FBC Board of Directors August 13, 2006
(Revised 8-10-2006)

TABLE OF CONTENTS

Introduction

This document establishes computer usage guidelines for the Fort Belknap College. Fort Belknap College offers a wide array of computing, networking, and telecommunications resources and services to members of the college community. These services are in place to facilitate teaching and learning, research, and administrative activities and to further Fort Belknap College's mission. This document contains information technology policies and procedures and also outlines responsibilities of those who use computing and networking facilities at the college. Users of these services agree to abide by and be subject to the terms and conditions contained in this and all other applicable College policies. Some departments on campus may have additional facilities, practices, and policies that apply to use of computing facilities in those departments. These policies are designed to enable high quality services and maximize productivity while protecting the rights of all members of the community.

Access to Information Technology Resources

Eligibility

Information Technology Resources (computer hardware, software, telephone systems, networks, services, data, and other information) are made available at FBC to support and facilitate the teaching, research and administrative functions of the College. Access to these resources is provided to employees of the College faculty, administration, staff, and enrolled students consistent with their responsibilities.

Under no circumstances may anyone use college IT resources in ways that are illegal (e.g. copyright violations), threaten the College's tax exempt or other status, or interfere with reasonable use by other members of the College community.

-

Other individuals, upon submission of a request, may be granted access to some, or all, of FBC IT resources by the President of the College. The terms of access will be stated at the time access is granted.

Account Activation/Termination

E-mail access at FBC is controlled through individual accounts and passwords. Each user of FBC's e-mail system is required to read and sign a copy of this E-Mail Acceptable Use Policy prior to receiving an e-mail access account and password. It is the responsibility of the employee to protect the confidentiality of their account and password information.

Convention For User Names

The standard FBC naming convention for access to electronic systems comprises the first initial of the first name, followed by middle initial and full last name. If duplicates occur, the middle initial is generally taken out to resolve ambiguity.

Management of Internet Bandwidth

The campus network, including our connection to the Internet, is a critical shared resource for supporting the academic programs. Uses of our Internet connection that are central to the academic/administrative mission of the college (e.g. access to FBC web, e- mail, and other sources) will receive higher priority during times when classes are in session, offices are open, and in the evenings when preparation takes place (i.e. critical times).

Low priority uses, including recreational uses, are peripheral to our mission and will receive lower priority during critical times.

Between the hours of 7:00 a.m. and 4:00 p.m. each day (critical times): Access to the FBC email and web servers from off campus is the highest priority. Incoming or outgoing web traffic between the Internet and the campus network is the next highest priority. Peer-to-Peer Internet applications (applications for distributing videos, music, software, etc.) receive the lowest priority. Between the hours of 2:00 a.m. and 7:00 a.m. (non-critical times): There will be no restrictions on bandwidth. The quality and volume of our Internet traffic is regularly monitored to assure that critical applications are available to members of the campus community.

FBC does not monitor the content of traffic on the network. It is the responsibility of each person using college resources, including the network, to do so in an ethical and legal manner. Particular attention should be given to observing copyright laws for digital materials.

Personal Computers on the Network

Internet addresses are provided by ITS. In order to obtain a static Internet (TCP/IP) computer address the owner of the system must register the computer with ITS network services. The rules and regulations contained in this policy pertaining to electronic mail and Internet access are equally applicable to the use of personal machines for file sharing or as servers. If bandwidth or other problems occur, ITS reserves the right to discontinue access to the machine. Computers connected to the network may not be used as servers for private enterprises, commercial activity, or personal profit. Computers connected to the network may not be used to provide access to the Internet for anyone not formally affiliated with the College. If personal computers on the FBC network are used as servers, the administrator has the additional responsibility to respond to any use of the server that is in violation of these policies and procedures. Server administrators must take steps to prevent recurrence of such violations and report these violations to the FBC Network Administrator (postmaster@mail.fbcc.edu).

ITS reserves the rights to disconnect any network port whose activity causes an adverse effect on the network or on any other user. Network connections may also be revoked in the case of malicious or inappropriate computing activity on the network. See Noncompliance and Sanctions for examples of these activities.

ITS reserves the right to restrict access to the network during expansion, or for diagnostic

and maintenance services. Every effort will be made to provide advance notification and schedule such disruptions during times of minimum impact and traffic.

Virus Protection

Fort Belknap College requires all existing and incoming students to install anti- virus software on their personal computers by the end of the second week of classes each semester. Failure to do so can result in the loss of connectivity to the Fort Belknap College network until anti- virus software is installed. AVG anti- virus software is provided free to all students. Other anti- virus products may be substituted as long as they are kept current.

Network Connections in Departments

All offices, laboratories, and classrooms on campus are wired for access to the network. If departments request additional network jacks, or if network connections need to be moved to different locations, the department should request this service through ITS. The department will be billed for charges resulting from moves, additions, and changes.

Network connections, wiring, equipment, or jacks may not be altered or extended beyond the location of their intended use. Any costs incurred to repair damages to a network or telephone, in a department will be billed to that department.

Dial- Up Connections

For all campus users the primary access to FBC computing services is through the campus network. Dial- in access via modem is not provided.

College Computer Equipment

Replacement of College Computer Equipment

All college computer equipment is on a regular replacement cycle of 3 years and 5 years for servers. Computer equipment is generally replaced during the summer months. During the spring term, ITS staff meet with departments to finalize needs and computers to be replaced. The goals of the replacement plan are to: Assure that appropriate computing resources are available in public and departmental computing facilities, classrooms, and college offices to support the mission of the institution; Assure that each faculty and staff member who uses computing resources in his or her position has a computer of sufficient capability to fulfill his/her responsibilities; Implement minimum standards for computing equipment on campus, and encourage planning, cost- effective installation of new equipment and disposal of old equipment. College computers are divided into three categories:

Lab Computers - Will be replaced every three years, pending funding.

Staff Computers - Will be replaced every five years, pending funding.

Research Computers - Will be changed out as needed and pending funding.

Each computer in the replacement plan is designated as being in one of these three groups with a tentative date indicated for replacement. Generally, individuals will have one college computer provided for them on the replacement plan. By the nature of their responsibilities, some individuals may need to have more than one computer to accomplish their responsibilities - for example, if they must use both Macintosh and Windows platforms in their work. In these cases, department heads/supervisors may request from the appropriate officer of the college that an exception be made.

Computers are essential tools for faculty, even when they are on sabbatical leave. For this reason the college permits faculty on leave to continue to use their computer during that period. Computers will be provided to faculty replacements from a pool of computers designated for this purpose.

Computers can or can not to be purchased from departmental operating budgets. The officers of the college approve such funds. Computers purchased with grants or special one- time funding will not be on the replacement plan unless prior approval is obtained from the officers.

Loaner Equipment

Fort Belknap College employees can borrow laptop computers for up to 7 consecutive days for uses related to college business. These computers have modems for off- campus access to resources. Students can checkout special equipment that is related to course of study with approval from Instructor and with President approval. Students are required to bring the equipment back the next day.

Reservations are required, and should be made at least two business days in advance. For more information, or to make a reservation, contact: Manager of Information Systems or Information System Specialist at 406-353-2607. You can email your request to: postmaster@mail.fbcc.edu

Departmental Equipment

All college computers are maintained in a central inventory. At the time a computer enters the inventory the replacement cycle, if any, is designated. Computers that are an integral part of a piece of scientific equipment, or are used primarily for research purposes, are not generally part of the replacement plan. Replacement of such equipment is by a special request to the Dean of Academics. Old equipment is sold for residual values through FBC official salvage process and must be returned to ITS.

Grant Funded Equipment

Individuals pursuing grants for computing equipment should discuss their plans with the Director, ITS, and Business Department as part of the budgeting process. Computing equipment that is acquired under grants will enter the inventory and be upgraded on a regular replacement cycle only if approved at the time of the application for the grant. Faculty members teaching in various special curricular programs are, under certain conditions, awarded research, or startup, funds. Some faculty members also have research

funds available to them. These funds may be used to buy additional computers and printers for office use, but the equipment will belong to the college. Such equipment should be ordered through the College purchasing process and will not normally be upgraded or replaced by the college, except through further use of research funds. If this equipment is to be on the computer replacement plan the faculty member must obtain a commitment, in writing, from the President and Finance indicating this. Otherwise, the equipment will not be on a replacement cycle.

Printers and Other Peripheral Equipment

The college provides networked printing locations for workgroup clusters in every department. Individual desktop printers are not normally provided. Other peripheral pieces of equipment such as scanners are also generally provided in clustered locations instead of individual offices. Since these pieces of equipment are usually used intermittently, clustering allows sharing of specialized technical resources.

Responsibility for Equipment

Each employee is responsible for taking reasonable safety precautions in regard to FBC- owned computer equipment. Employees will be held responsible for damage to such equipment arising out of their negligence or intentional misconduct.

Upgrades and Renewal

For computer equipment on the replacement plan ITS staff members consult with users prior to ordering and installing new equipment to determine the current and anticipated equipment needs. Machines that are replaced are returned to ITS. ITS then reassigns the machines or sells them through the campus salvage process. FBC will not upgrade on- FBC machines.

Repair of Computer Equipment

FBC Computer Equipment

All college computer equipment is maintained in-house. If a hardware problem is suspected the user should call the Helpdesk (353- 2607) during normal business hours for assistance. If hardware service is indicated, arrangements will be made with the technician.

Personally Owned Equipment

IT office also provides repair for personally owned computers. Computers are repaired at a cost rate established by FBC. There is a minimum charge for examining the equipment if repair is not needed. Equipment must be delivered to the IT office during regular business hours. IT Department will be available each day between 7 am and 4 p.m. to receive equipment, or by special arrangement by calling 406-353-2607 or by e- mail (postmaster@mail.fbcc.edu). Payment for the repairs must be made by cash, check, or money order when the equipment is picked up. Charges can be applied to your Fort Belknap College account.

Web Posting and Development

Overview:

The accuracy, timeliness, design, and speed (performance) of the web site are of strategic importance to the college since many external constituents view our web site.

The Role of the IT Committee

The President's Internet Initiative Committee (the "Committee") is the policy making body for the development of FBC presence on the Web. The Committee will determine standards for participation in, and design of, FBC web site. The Committee approves the design of the main home page (including the categories/ headings) and style guidelines for individuals/ organizations that wish to contribute to the content of the site. The Committee approves the linking of new pages to the Web site, rules on policy interpretations, and advises on matters of resource allocations.

Given the nature of the World Wide Web (WWW), FBC employees or students can not operate their own servers, but to have links created from the FBC Server to their space on web server must abide by the FBC policies, procedures, and style guidelines.

Procedures

Members of the Fort Belknap College community can obtain space on the college web site for the development of departmental or employee web pages. Students can obtain space if related to course being taught. Any organizations outside the college that are not part of the FBC may not host their site at FBC. An individual member of the College can obtain a web account by sending an e- mail to the webmaster requesting an account be set up. The request will be view and approved or disapproved from the President's Internet Initiative Committee. Within two weeks (if approved) the individual will receive his/her account password and instructions on using the web space. Requests for web accounts for academic or administrative departments, or programs must be sent by the department chair and must specify who will be the content provider. Requests for student organizations must be sent by the faculty/staff advisor for that organization and indicate who will be the content provider. Personal web page space is limited to 10mb for each individual.

When content providers have completed their pages the URL should be sent to the Webmaster (postmaster@mail.fbcc.edu). The Webmaster will inform the Committee of the request and the Committee will review URL's within two weeks and notify the content provider of their decision.

A content provider is responsible for keeping web information up- to- date and accurate.

The content providers name, e- mail address, and date of last modification must appear on all created pages to provide opportunities for viewers of the page to alert the provider about inaccuracies, suggest changes, or ask questions. Failure to maintain accurate pages will result in removal of the pages from the College site.

Style Guidelines

The first several levels of the FBC web site are designed to project a consistent look in the use of headers, colors, fonts, and approaches to navigation. Site design standards are periodically reviewed and subject to change and will be posted on the College web site.

In addition, there are guidelines for the creation of web pages that deal with issues such as page design, navigation, graphics, colors, fonts, etc.

Copyright and Links to Commercial Organizations

The use of the Fort Belknap College Web site must be consistent with other college policies relating to use of information technology resources. Of particular note are the restrictions on the use of copyrighted material and the use of college resources for profit- making activities.

Placing copyrighted material on the Web site without permission of the author is prohibited.

Links to commercial organizations that appear on Fort Belknap College departmental or organizational Web pages must be directly related to the stated mission of that department or organization. These links should not infer a preference for a particular commercial organization, but rather should be informative of the range of options available to those who might need the information provided by these links.

Links from any college web pages that generate income to a department, organization, or individual might compromise the College's tax- exempt status, and as such are prohibited.

Hardware Standards

The following guidelines for standards are based on the current technology available combined with the current needs of the end- user today. These apply to both the Macintosh and Wintel platforms. The primary considerations for each configuration (desktop, printing, portable computing) are: Ease of connectivity to the college network

1. Consistent performance of all integrated components in our network environment;

2. Industry leader with an established track record in manufacturing, sales and service;

3. Successful in- house experience with the chosen product and configuration

4. Serviceability by the IT Department

5. The machine has a minimum campus lifetime of four years

The detailed listings below are the standard configurations for new replacement computers for the year 2006-2008, and will be updated as need be:

Macintosh Configurations

Desktop: Power Macintosh G4 - MiniTower
733 MHz PowerPC G4 Processor
1 GB RAM
40 GB Hard Drive
CD- RW/DVD- ROM ComboDrive
Ethernet Adapter
17" Color Display
Apple USB Keyboard
Apple USB Mouse
Mac OS X

Notebook: PowerBook G4 Titanium
667 MHz PowerPC G4 Processor
1GB RAM
80 GB Hard Drive
CD- RW/DVD- ROM ComboDrive
Built- in Ethernet
56 K Modem
15.2 " Color Display
AC Adapter
Carrying Case
Mac OS X

Windows Intel Configurations

Desktop: Dell Optiplex GX240 - MiniTower
1.2 GHz Pentium 4 Processor
1GB RAM
80 GB Hard Drive
1.44 MB Floppy Drive
CD- RW/DVD- ROM ComboDrive
3COM Ethernet Adapter
17" Color Display
Windows Keyboard
Microsoft Mouse
Windows XP Professional

Notebook: Dell Latitude C840
1.60 GHz Pentium 4 Processor
1GB RAM
80 GB Hard Drive
CD- RW Drive
1.44 MB Floppy Drive
3COM Ethernet Adapter
56 K Modem
15" Color Display

AC Adapter
Carrying Case
Windows XP Professional

Software Standards

Rationale:

In FBC modern networked environment, the ability to easily share information is important. Ideally, the ease of sharing should not depend upon which hardware environment is being used on the desktop (Wintel or Macintosh). Central to making sharing facile is the software environment, particularly software used for word processing, spreadsheets, databases, network browsing, and electronic mail.

The following are advantages of campus- wide software standards:

Improved Data Sharing

Consistency of file formats provides for optimal file sharing capabilities between individuals, departments, and groups across campus. Identical resources on each desktop (private offices and public labs) provide ease of transferability and a consistent tool- set for all users, from any room, office or public lab, needed resources will be available. Sharing of data between applications (word processors, spreadsheets, data bases) is seamless.

Simplified Budgeting and Purchasing Software standards would permit centralized budgeting and purchasing. This would relieve an individual or department from the time consuming tasks of choosing a product, tracking down the best pricing and product availability, and generating the proper paperwork to place an order for the product. Significant savings can be achieved through site licenses or quantity discounts.

Improved Support

ITS support personnel can focus on depth of application knowledge rather than breadth of numerous applications. Product expertise means questions can be answered more quickly and efficiently. Support efforts can be focused on supporting the end- user and documenting known problems. Support could come from any member of the Fort Belknap College community, since most will be using the same application. Support subscriptions to Knowledge Data Bases provided by third party vendors could be made available online to all users via the campus network. Support licenses from the vendor could be made available to users.

Improved Training

Training teams can focus on developing curricula for levels of user proficiency (introductory, intermediate, advanced). Training specialists from outside campus can be used more effectively and economically. Smoother Software Installation and Upgrades Software installations for new machines could become invisible to the end- users by making it part of the hardware installation. Installations can become routine, rather than a specialized process for each individual, resulting in time savings. Installations and

upgrades could be made available to all users via the campus network, and automated for consistency. Upgrades can be tested and documented prior to campus- wide deployment to reduce potential incompatible and problems. Simplified Software Licensing Separate record keeping for software licenses would not be required by the individual; rather it could become part of the central inventory of hardware.

Software Standards:

Microsoft Word
Microsoft Excel
Microsoft PowerPoint
Microsoft FrontPage
Internet Explorer
Adobe Acrobat Creator/Reader

For questions about these Policies, Procedures, Plans and Standards, contact: Manager of Information Systems or President of Fort Belknap College (406) 353- 2607.

Telephone and Voicemail Acceptable Use Policy

Purpose

Telephone communication is an essential part of the day-to-day operations of Fort Belknap College. Telephone and voicemail services are provided to employees of Fort Belknap College in order to facilitate performance of Fort Belknap College work. The goal of this policy is to balance the business need for telephone and voicemail use by Fort Belknap College with the costs involved.

Scope

This policy applies to all employees of Fort Belknap College, and all usage of Fort Belknap College telephone and voicemail services.

Telephone and Voicemail Services

Fort Belknap College Telephone system is one pair digital telephone system with voice mail system. It is designed to hold up to 300 extensions. The telephone system is not part of the data network and is separate from the main data core.

Basic Policy

As with all Fort Belknap College resources, the use of telephones and voicemail should be as cost effectively as possible and in keeping with the best interests of Fort Belknap College. All employees must operate within the following basic policy guidelines. Further information on appropriate and inappropriate use follows this section.

- All telephones, telephony equipment, voicemail boxes, and messages contained within voicemail boxes are the property of Fort Belknap College.

- The IT Department is responsible for installation and repair of all company name telephony equipment and administration of telephone and voicemail accounts.
- Department supervisors are responsible for overseeing telephone and voicemail use and ensuring policy compliance, as well as ensuring IT is notified of any adds, moves, or changes required to telephone or voicemail services.
- All FBC's employees are eligible to receive a telephone based on their needs.
- Employees that require a dedicated telephone must submit in writing to the President on why he/she needs one. It will be brought up in the Executive Committee meeting for approval.
- Employees that require direct lines are the key administrators. Example would be the President, Dean of Academics, Dean of Students, and Comp Controller. This will be based on job function and approval by the Executive Committee. All other employees will receive extensions based on their job function.
- FBC will limit the number of extensions and voicemail boxes because of the current configuration of the PBX system.
- The number of telephone calls made should be limited in number and duration to that necessary for effective conduct of business. Efforts should be made to limit the length of telephone calls to less than [insert duration] in length.
- All voicemail boxes will be protected with a PIN (personal identification number). PINs must be changed at least once a year to aid in mailbox security. PINs must not be shared with others.
- A voicemail box can hold 5 minutes of message storage time. If a voicemail box is full, no further messages can be recorded. Read voicemail messages will be up to the employee to delete after 2 days.
- Voicemail is to be used as a backup in the event you are not available to answer a call, and should not be used to "screen" calls. Each user is expected to respond to voicemail messages in a timely manner.
- If you will be away from the office for more than one business day, you are expected to change your voicemail greeting to reflect this fact and direct callers to alternate contacts if applicable.
- Use of directory assistance (i.e. 411) should be avoided since a fee is incurred with each use. If you are unsure of a number, please consult print or online telephone directories first.

Unacceptable Use

Fort Belknap College telephone and voicemail services may not be used for the following:

- Transmitting obscene, profane, or offensive messages.

- Transmitting messages or jokes that violate our harassment policy or create an intimidating or hostile work environment.
- Using the telephone system or breaking into a voicemail box via unauthorized used of a PIN or other password.
- Broadcasting unsolicited personal views on social, political, or other non-business related matters.
- Soliciting to buy or sell goods or services unrelated to Fort Belknap College.
- Calling 1-900 phone numbers.
- Making personal long-distance phone calls without supervisor permission.

Misuse of telephone and voicemail services can result in disciplinary action, up to and including termination.

Limited Personal Acceptable Use

In general, personal use of telephone and voicemail services is allowable, but must be limited in number and duration and must not interfere with performance of official business duties. Limited personal acceptable use is allowed under the following circumstances:

- An employee's work schedule changes without advance notice and the employee must notify a family member or make alternate transportation or childcare arrangements.
- Brief local calls to a spouse, minor child, or elderly parent, or to those responsible for them (e.g. school, daycare center, nursing home).
- The employee needs to make a call that can only be made during regular working hours, such as to a doctor or local government agency.
- The employee needs to make arrangements for emergency repairs to his or her residence or automobile.
- A call that reasonably could not be made at another time and is of moderate duration.

Any personal long-distance calls that must be made (excepting toll-free 1-800 calls) should be charged to the employee's home telephone number, personal credit card, personal calling card, or be charged to the called party. If a personal long-distance call must be made that will be billed to Fort Belknap College, the employee should receive permission from a supervisor to make the call first. Regardless, employees are expected to reimburse Fort Belknap College for the cost of any long-distance calls within 2 days of receipt of the relevant bill.

Monitoring

Fort Belknap College reserves the right to monitor telephone and voicemail use, including telephone conversations and the contents of voicemail boxes. Monitoring of telephone and voicemail use will only be done for legitimate reasons, such as to assess

customer service quality assurance, retrieve lost messages, recover from system failure, or comply with investigations of wrongful acts.

The following telephone and voicemail usage reports are generated by Fort Belknap College:

- Date, time, length of call, number called;
- Costs per call;
- And type of usage.

Service and Repair

The IT Department requires 10 days notice to set up a standard telephone service and voicemail box. If there is a problem with an existing telephone or voicemail box, contact the IT Department immediately at extension 229. Fixes are typically made within 3 days.

Telephone Procedures

All employees that receive a telephone also receive the manual on how to operate their phone. It is the employees responsibility to learn how to operate their phone. If employee has lost their manual, they can contact the IT Department to receive another copy.

Voicemail Procedures

All employees are to follow FBC's voicemail procedures. How to setup your voicemail will be in the manual you received with your telephone. If you have trouble in setting up your voicemail, you can contact the IT Department for help.

Printer Policy

Purpose

Printers represent one of the highest equipment expenditures at Fort Belknap College. The goal of this policy is to facilitate the appropriate and responsible business use of Fort Belknap College's printer assets, as well as control Fort Belknap College's printer cost of ownership by preventing the waste of paper, toner, ink, and so on.

Scope

This Printer Policy applies to all employees and students of Fort Belknap College, as well as any contract employees in the service of Fort Belknap College who may be using Fort Belknap College networks and equipment.

Supported Printers

Fort Belknap College supports all network printers on the college's network system. An effort has been made to standardize on specific printer models in order to optimize contractual agreements and minimize support costs.

General Policy

1. Printers are to be used for documents that are relevant to the day-to-day conduct of business at Fort Belknap College. Fort Belknap College printers should not be used to print personal documents.

2. Installation of personal printers is generally not condoned at Fort Belknap College due to the cost of maintaining and supporting many dispersed machines. In certain circumstances, however, where confidentiality, remote location, the need to print a large number of low volume print jobs, or other unusual situation is an issue, personal printers may be allowed.

3. Do not print multiple copies of the same document – the printer is not a copier and typically costs more per page to use. If you need multiple copies, print one good copy on the printer and use the photocopier to make additional copies.

4. If you print something, please pick it up in a timely fashion. If you no longer want it, please dispose of it appropriately (i.e. recycle).

5. If you come across an unclaimed print job, please stack it neatly and turn into the main office. All unclaimed output jobs will be discarded after two days.

6. Make efforts to limit paper usage by taking advantage of duplex printing (i.e. double-sided printing) features offered by some printers and other optimization features (e.g. printing six PowerPoint slides per page versus only one per page).

7. Make efforts to limit toner use by selecting light toner and lower dpi default print settings.

8. Avoid printing large files, as this puts a drain on network resources and interferes with the ability of others to use the printer. Please report any planned print jobs in excess of 100 pages to the IT Department so that the most appropriate printer can be selected and other users can be notified.

9. If printing a job in excess of 25 pages, please be at the printer to collect it when it comes out to ensure adequate paper supply for the job and that the output tray is not overfull (i.e. you may need to remove some of the output before the print job is finished).

10. Avoid printing e-mail messages. This is wasteful. Instead, use the folders and archiving functionality in your e-mail application to organize and view your messages.

11. Avoiding printing a document just to see what it looks like. This is wasteful.

12. Avoid re-using paper in laser printers, as this can lead to paper jams and other problems with the machine.

13. Many printers do not support certain paper types, including vellum, transparencies, adhesive labels, tracing paper, card stock, or thicker paper. If you need to use any of the paper types, consult with IT to find out which machines can handle these specialty print jobs.

14. Color printing is typically not required by general business users. Given this selective need, as well as the high cost per page to print color copies, the number of color-capable printers available has been minimized. You are strongly encouraged to avoid printing in color when monochrome (black) will do.

15. Printer paper is available at all departments. Toner cartridges are available at all departments.

16. If you encounter a physical problem with the printer (paper jam, out of toner, etc.) and are not "trained" in how to fix the problem, please do not try. Instead, report the problem to IT or ask a trained co-worker for help.

17. Report any malfunction of any printing device to the IT Department as soon as possible.

Wireless Security Access Policy and Agreement

Purpose

The purpose of this policy is to define standards, procedures, and restrictions for connecting to Fort Belknap College's internal network(s) or related technology resources via any means involving wireless technology. This can include, but is not limited to, access from the following:

- External hosts via remote access technology (for example, using a wireless router at home to connect to the Fort Belknap College Virtual Private Network).
- Wireless gateways on Fort Belknap College premises.
- Third-party wireless Internet service providers (also known as "hotspots").

The policy applies to any equipment used to access Fort Belknap College resources, even if said equipment is not Fort Belknap College, owned, or supplied. For example, use of a public library's wireless network to access the Fort Belknap College network would fall under the scope of this policy.

The overriding goal of this policy is to protect Fort Belknap College's technology-based resources (such as Fort Belknap College data, computer systems, networks, databases, etc.) from unauthorized use and/or malicious attack that could result in loss of information, damage to critical applications, loss of revenue, and damage to our public image. Therefore, all users employing wireless methods of accessing Fort Belknap College technology resources must adhere to company-defined processes for doing so.

Scope

This policy applies to all Fort Belknap College employees, including full-time staff, part-time staff, contractors, freelancers, and other agents who utilize company-owned, personally-owned, or publicly-accessible computers to access the organization's data and networks via wireless means. Wireless access to enterprise network resources is a privilege, not a right. Consequently, employment at Fort Belknap College does not automatically guarantee the granting of wireless access privileges.

Wireless networks should not be considered a replacement for a wired network. They should be seen solely as extensions to the existing wired network, and are to be used for general purpose access in areas of transient use, such as common areas or meeting rooms. Wireless segments should not be used for work sessions involving any form of access to sensitive organizational data.

Addition of new wireless access points within Fort Belknap College facilities will be managed at the sole discretion of IT. Non-sanctioned installations of wireless equipment, or use of unauthorized equipment within the organizational campus, is strictly forbidden. This policy is complementary to any previously-implemented policies dealing specifically with network access and remote access to the enterprise network.

Supported Technology

All wireless access points within the Fort Belknap College firewall will be centrally managed by Fort Belknap College's IT Department and will utilize encryption, strong authentication, and other security methods at IT's discretion. Although IT is not able to manage public wireless resources, end-users are expected to adhere to the same security protocols while utilizing this equipment. Failure to do so will result in immediate suspension of all network access privileges so as to protect the company's infrastructure.

Eligible Users

All employees requiring the use of wireless access for business purposes must go through an application process that clearly outlines why the access is required and what level of service the employee needs should his/her application be accepted. IT will define a list of traffic types that are acceptable for use over a wireless connection. More sensitive business activities will be similarly defined, and will be limited to non-wireless environments. Application forms must be approved and signed by the employee's unit manager, supervisor, or department head before submission to the IT Department. Employees may use privately owned connections (under 'Supported Technology') for business purposes. If this is the case, the IT Department must approve the wireless connection as being secure and protected. However, the company's IT Department cannot and will not technically support third-party wireless hardware or software, a hotspot wireless ISP connection, or any other wireless resource located outside the Fort Belknap College firewall . In the event that expenses are incurred and leadership has approved reimbursement, all expense forms for reimbursement of costs (if any) incurred due to the need for wireless access for business purposes (i.e. Internet connectivity charges) must be submitted to the appropriate unit or department head. Financial reimbursement for wireless access is not the responsibility of the IT Department. If you

foresee an upcoming need for this class of access, ask your leader to help you fill out a business case.

Policy and Appropriate Use

It is the responsibility of any employee of Fort Belknap College who is connecting to the organizational network via wireless means to ensure that all components of his/her wireless connection remain as secure as his or her network access within the office. It is imperative that any wireless connection used to conduct Fort Belknap College business be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account. Based on this, the following rules must be observed:

1. General access to the organizational network through the Internet by residential remote users through Fort Belknap College's network is permitted. However, the employee and student members using the Internet for recreational purposes through company networks are not to violate any of Fort Belknap College's Internet acceptable use policies.

2. Employees using wireless access methods will, without exception, use secure remote access procedures. This will be enforced through public/private key encrypted strong passwords in accordance with Fort Belknap College's password policy. Employees agree to never disclose their passwords to anyone, particularly to family members if business work is conducted from home.

3. All remote computer equipment and devices used for business interests, whether personal- or company-owned, must display reasonable physical security measures. Users are expected to secure their Fort Belknap College-connected machines when they are physically at their machines, as well as when they step away. Computers will have installed whatever antivirus software deemed necessary by Fort Belknap College's IT Department. Antivirus signature files must be updated in accordance with existing company policy.

4. Due to the potential for bandwidth conflicts within the Fort Belknap College campus, use of unsanctioned equipment operating within the 2.4 GHz range is strictly forbidden. If you have a need to use such equipment – for example, a wireless phone – please consult IT before proceeding further.

5. Prior to initial use for connecting to the Fort Belknap College network, all public hotspots must be registered with IT.

6. Remote users using public hotspots for wireless Internet access must employ for their devices a company-approved personal firewall, VPN, and any other security measure deemed necessary by the IT Department. VPNs supplied by the wireless service provider should also be used, but only in conjunction with Fort Belknap College's additional security measures. IT will support its sanctioned hardware and software, but is not accountable for conflicts or problems whose root cause is attributable to a third-party product.

- Hotspot and remote users must disconnect wireless cards when not in use in order to mitigate attacks by hackers, wardrivers, and eavesdroppers.
- Users must apply new passwords every business/personal trip where company data is being utilized over a hotspot wireless service, or when a company device is used for personal Web browsing.

7. Any remote connection (i.e. hotspot, ISDN, frame relay, etc.) that is configured to access Fort Belknap College resources must adhere to the authentication requirements of Fort Belknap College's IT Department. In addition, all hardware security configurations (personal or company-owned) must be approved by Fort Belknap College's IT Department.

8. Employees, contractors, and temporary staff will make no modifications of any kind to company-owned and installed wireless hardware or software without the express approval of Fort Belknap College's IT Department.

9. Employees, contractors, and temporary staff with wireless access privileges must ensure that their computers are not connected to any other network while connected to Fort Belknap College's network via remote access.

10. The wireless access user agrees to immediately report to his/her manager and Fort Belknap College's IT Department any incident or suspected incidents of unauthorized access and/or disclosure of company resources, databases, networks, and any other related components of the organization's technology infrastructure.

11. The wireless access user also agrees to and accepts that his or her access and/or connection to Fort Belknap College's networks may be monitored to record dates, times, duration of access, data types and volumes, etc., in order to identify unusual usage patterns or other suspicious activity. As with in-house computers, this is done in order to identify accounts/computers that may have been compromised by external parties.

12. IT reserves the right to turn off without notice any access port to the network that puts the company's systems, data, users, and clients at risk.

Policy Non-Compliance

Failure to comply with the Wireless Security Access Policy and Agreement may result in the suspension of remote access privileges, disciplinary action, and possibly termination of employment.

Web Posting Policy

Purpose

Fort Belknap College maintains a Web site to provide information about the College to the campus community and the public at large. Individuals, departments, divisions, and colleges may develop and maintain local Web pages within the [www.fbcc.edu] domain. These guidelines are to insure that Web pages within the [www.fbcc.edu] domain further the purpose of Fort Belknap College's Web site.

Content Guidelines

The object of these guidelines is to ensure that the content of Web pages accurately represent Fort Belknap College.

1. Content must be consistent with the purpose of Fort Belknap College's Web site.
2. Content must conform to Acceptable Use Policies and Fort Belknap College's Web Policy so that it is
    - Non-discriminatory,
    - Non-commercial, and
    - Protective of individual privacy.
3. Language must be suitable to a public forum.
4. Content provided must be appropriately current and accurate.
5. Links are to be monitored, with non-functioning links removed or repaired regularly.

Format Guidelines

The object of these guidelines is to ensure that Web pages present a favorable, professional image of Fort Belknap College.

1. Spelling and grammar should be correct.
    - Merriam-Webster Online
    - *Elements of Style* (William Strunk)
    - *Grammar and Style Notes* (Jack Lynch)
    - *An Elementary Grammar* (The English Institute)
2. HTML should be used correctly.
    - Quick Introductions: HTML Sampler and HTML Primer.
    - Advice on basic elements of good style: W3C's Style Overview.
    - HTML Documentation: HTML Tag Reference, W3C's HTML 3.2 Reference Specification
3. Use of the FBC logo should comply with the *FBC Graphics Identification Program.*
    - Colleges and departments may use the College logo anywhere in their web design.

- Please do not scan the logo. Several sizes of the official logo are available for download.
- You may also wish to use the official Fort Belknap College colors in your page design.

4. Images should load correctly within a reasonable amount of time.
   - Large images may load very slowly and can discourage those attempting to browse your pages. Make the viewing of large images optional by showing them as links and forewarning your audience of their size. *Example:* Aerial view of Fort Belknap College (179K)
   - Include alternate text for users browsing in a text only mode by using the ALT= parameter of the IMG tag. *Example:* Always include "Fort Belknap College" as alternate text with the Fort Belknap College logo: <IMG SRC="images/logos/FBC-125.gif" border="0" WIDTH="125" HEIGHT="110" ALT="FORT BELKNAP COLLEGE">
5. Relative links should be used in place of the full URL whenever possible.
   - To link to a file in the same directory on the server, just use the filename in the link. *Example:* <A HREF="filename.html">Filename</A>
   - To link to a file in a subdirectory on the server, use the directory and filename in the link. *Example:* <AHREF="/directory/filename.html">Filename</A>
   - See HTML Sampler or other HTML references for a full explanation of link syntax.
6. Navigational aids should be provided to assist the user in returning to Fort Belknap College's home page.
   - Preferred: Use the home page footer image within a link back to Fort Belknap College's home page.
7. Documentation should be displayed on each page to indicate:
   - Person or office responsible for the page,
   - E-mail address or phone number of individual to contact about page, and
   - Date page was last updated. To avoid confusion with different international date conventions, spell out the month (e.g. February 11, 1999 or 11 FEB 99 rather than 02/11/99).
8. Institutional and local pages should include information to facilitate accurate indexing by search engines.
   - Our Compass server uses document titles, meta tags, headings, and the first n bytes of text, where n is configurable. See the help file on our search page and follow the link to "Preparing Documents" on the left side of the page.
   - How to Use Meta Tags from Search Engine Watch.
   - Meta Tagging for Search Engines from the Web Developer's Virtual Library.
9. Pages should be checked before posting.

- Examine pages with recent versions of Netscape Navigator and Internet Explorer.
- HTML Code Checking: W3C's HTML Validation Service

All Web content submitted must be approved prior to posting. The following individuals retain the right to edit, request changes, approve, or deny submitted content: FBC Web Site Committee.

All submissions must be entered at least two days in advance of the requested posting date. If significant changes are required to the content, this timeframe may be extended.

Submission of Copyrighted Work

No employee of Fort Belknap College may reproduce any copyrighted work in violation of the law. Copyrighted works include, but are not limited to: text (e.g. articles), images (e.g. photographs), graphics (e.g. logos), sound recordings (e.g. MP3s), video recordings (e.g. movies), or software programs.

In some countries, such as the U.S., copyrighted materials are not required by law to be registered, unlike patents and trademarks, and may not be required to carry the copyright symbol (©). Therefore, a copyrighted work may not be immediately recognizable. Assume material is copyrighted until proven otherwise.

If a work is copyrighted, you must seek out and receive express written permission of the copyright holder to reproduce the copyrighted work in order to avoid violation. This also includes all copyrighted works held by Fort Belknap College. In order to get permission to copy or reproduce Fort Belknap College's copyrighted materials.

Enforcement

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

End-User Backup Policy

Introduction

Data is one of Fort Belknap College's most important assets. In order to protect this asset from loss or destruction, it is imperative that it be safely and securely captured, copied, and stored. The goal of this document is to outline a policy that governs how and when data residing on company desktop computers, PCs, and PDAs – as well as home office/mobile devices and appliances – will be backed up and stored for the purpose of providing restoration capability. In addition, it will address methods for requesting that backed up data be restored to individual systems.

Scope

This policy refers to the backing up of data that resides on individual PCs, notebooks, PDAs, laptop computers, and other such devices (to be referred to as "workstations").

Responsibility for backing up data on local desktop systems or laptops rests solely with the individual user. It is imperative that end-users save their data to the appropriate media and/or network space outlined in this policy in order that their data is backed up regularly in accordance with company regulations and business continuity plans.

This policy does not cover end-user information that is saved on a network or shared drive, as these are backed up when the servers are backed up. For information on how often the IT Department backs up servers, please refer to Fort Belknap College's Server Backup Policy.

Backup Schedule

Backups are conducted on every Friday evening. Backups must be verified at least once a month.

Data Storage

It is Fort Belknap College's policy that ALL Fort Belknap College data will be backed up according to schedule. This includes any company documentation (i.e. reports, RFPs, contracts, etc.), e-mails, applications/projects under development, Web site collateral, graphic designs, and so on, that reside on end-user workstations.

* **Office Users:** Fort Belknap College data, especially works-in-progress, should be saved. This ensures that data will be backed up when the servers are backed up. If data is saved on a workstation's local drive, then that must be backed up every week onto storage media such as CD Read/Write disks or some type removable storage device, such as a mini hard drive, data cartridge, or solid state memory card.

* **Remote/Mobile Users:** Remote and mobile users will also back up data and then follow the *same procedure* as "Office Users" shown above. If this is not feasible due to distance from their office, then the remote/mobile user will employ CD Read/Write disks. Should Read/Write disks not be available, then select files should be copied to some type removable storage device, such as a mini hard drive, data cartridge, or solid state memory card.

Managing Restores

The ultimate goal of any backup process is to ensure that a restorable copy of data exists. If the data cannot be restored, then the process is useless. As a result, it's essential that the IT Department regularly test its ability to restore data from the storage media or network drive. As such, all storage media must be tested at least once every month to ensure that the data they contain can be completely restored to end-user workstations. Data will be restored from a backup if:

- There is an intrusion or attack.
- Files have been corrupted, deleted, or modified.
- Information must be accessed that is located on an archived backup.

- That workstation belongs to a domain.

In the event that an end-user requires or desires a data restore, the following policy will be adhered to:

1. The individual responsible for overseeing backup and restore procedures is Manager of Information Systems. If a user has a restore request, they can contact IT Department by calling, sending an e-mail, or filling out and submitting a request form.

2. Mobile and/or remote users will likely be carrying their backups with them. In the event that a restore is needed, the user will contact Fort Belknap Colleges IT Department at 406-353-2607 or e-mail address. The IT Department will walk the user through the restore procedure for their mobile device.

3. In the event of unplanned downtime, attack, or disaster, Fort Belknap College's full restoration procedures will take place.

4. In the event of a local data loss due to human error, the end-user affected must contact the IT Department and request a data restore. The end-user must provide the following information:

   - Name.
   - Contact information.
   - Name of file(s) and/or folder(s) affected.
   - Last known location of files(s) and/or folder(s) affected.
   - Extent and nature of data loss.
   - Events leading to data loss, including last modified date and time (if known).
   - Urgency of restore.

5. Depending on the extent of data loss, backup tapes and storage media may both need to be used. The timing in the cycle will dictate whether or not these tapes and/or other media are onsite or offsite. Tapes and other media must be retrieved by the server administrator or pre-determined replacement. If tapes and/or other media are offsite and the restore is not urgent, then the end-user affected may be required to wait for a time- and cost-effective opportunity for the tape(s) and/or other media to be retrieved.

6. If the data loss was due to user error or a lack of adherence to procedure, then the end-user responsible may be required to participate in a tutorial on effective data backup practices.

Employee Departure Checkout Checklist

This checklist explains the employee departure checkout process. Follow these steps for any employee departure, whether voluntary or involuntary. This checklist assumes that appropriate written notification of pending departure has either been supplied by the

employee in the event of resignation, or will be supplied to the employee in the event of termination.

1. Notify the appropriate personnel in IT in advance that an employee will be departing so that they can take appropriate security measures. If the employee is being terminated, notify IT that all of the employee's accounts (network, e-mail, voice) will need to be deactivated at a particular date and time. Ideally, deactivation should take place while the employee is being notified of his or her termination.

2. List in advance any equipment and files that should be in the employee's possession and must be returned.

3. Conduct an exit interview. At this interview, the following must be addressed:
   - Review final compensation procedures and timeframe, including payout of any vacation pay accrued.
   - Review termination date of any and all benefits, and any provisions for temporary extension of benefits.
   - Review any confidentiality and non-disclosure requirements. Remind employee that all files and documents are property of Fort Belknap College and cannot be destroyed, removed, modified, or copied without approval from the direct supervisor.
   - Ensure return of all company property to the employee's supervisor, or make arrangements for its immediate return. Company property includes all keys, access cards, identification cards, credit cards, parking passes, tools, books, reference materials, software, and equipment (such as laptop computers, personal digital assistants, pagers, and cell phones).
   - Gather and/or confirm the employee's forwarding information, including home address and e-mail address (if appropriate).
   - Have the employee disclose all usernames and passwords to all accounts and/or applications to the employee's supervisor for records management and redistribution purposes.
   - Review the status of any and all projects or work in progress.
   - Have the employee disclose the location of key work-related documents and records.

4. Have all work-related computer files transferred to [location] for secure review by the departing employee's successor or supervisor. These files will be deleted, stored, or forwarded to the appropriate Fort Belknap College staff member.

5. Arrange for return of personal print and computer files to the employee

6. All personal items, such as plants and family photos, must be removed from the employee's work area by the employee as close as possible to the time of

employee departure. Under stressful circumstances, arrangements can be made for employees to clear out their personal items during off hours.

7. Arrange for the departing employee's e-mail and phone calls to be temporarily forwarded to the employee's supervisor.

IT Asset Disposal Policy

Purpose

The purpose of this policy is to establish and define standards, procedures, and restrictions for the disposal of non-leased IT equipment in a legal, cost-effective manner. Fort Belknap College's surplus or obsolete IT assets and resources (i.e. desktop computers, servers, databases, etc.) must be discarded according to legal requirements and environmental regulations through the appropriate external agents and Fort Belknap College's upgrade guidelines. Therefore, all disposal procedures for retired IT assets must adhere to company-approved methods.

Scope

This policy applies to the proper disposal of all non-leased Fort Belknap College IT hardware, including PCs, printers, handheld devices, servers, databases, hubs, switches, bridges, routers, and so on. Company-owned surplus hardware, obsolete machines, and any equipment beyond reasonable repair or reuse are covered by this policy. Where applicable, it is desirable to achieve some residual value of the IT asset in question through reselling, auctioning, donation, or reassignment to a less-critical function.

Definitions

"Non-leased" refers to any and all IT assets that are the sole property of Fort Belknap College; that is, equipment that is not rented, leased, or borrowed from a third-party supplier or partner company.

"Disposal" refers to the reselling, reassignment, recycling, donating, or throwing out of IT equipment through responsible, ethical, and environmentally sound means.

"Obsolete" refers to any and all equipment over 10 years old and/or that which no longer meets requisite functionality.

"Surplus" refers to hardware that has been replaced by upgraded equipment or is superfluous to existing requirements.

"Beyond reasonable repair" refers to any and all equipment whose condition requires fixing or refurbishing that is likely cost equal to or more than total replacement.

Guidelines

Disposal and disposal procedures of all IT assets and equipment will be centrally managed and coordinated by Fort Belknap College's IT Department. Fort Belknap

College's IT Department is also responsible for backing up and then wiping clean of company data all IT assets slated for disposal, as well as the removal of company tags and/or identifying labels. The IT Department is in charge of selecting and approving external agents for recycling hardware and/or sanitizing hardware of harmful toxins before shipment to landfills.

Practices

Acceptable methods for the disposal of IT assets are as follows:

a) Sold to existing staff.

b) Donated to Students.

c) Sold as scrap to a licensed dealer.

d) Used as a trade-in against cost of replacement item.

e) Reassigned to a less-critical business operation function.

f) Donated to schools, charities, and other non-profit organizations.

g) Recycled and/or refurbished to leverage further use (within limits of reasonable repair).

h) Discarded as rubbish in a landfill after sanitized of toxic materials by approved service provider.

Policy

It is the responsibility of any employee of Fort Belknap College's IT Department with the appropriate authority to ensure that IT assets, equipment, and hardware are disposed of according to one or more of the methods prescribed above. It is imperative that any disposals performed by Fort Belknap College are done appropriately, responsibly, and ethically, as well as with company resource planning in mind. The following rules must therefore be observed:

Obsolete IT Assets: As prescribed above, "obsolete" refers to any and all computer or computer-related equipment over 10 years old and/or equipment that no longer meets requisite functionality. Identifying and classifying IT assets as obsolete is the sole province of Fort Belknap College's IT Department. Decisions on this matter will be made according to Fort Belknap College's purchasing/procurement strategies. Equipment lifecycles are to be determined by IT asset management best practices (i.e. total cost of ownership, required upgrades, etc.).

Reassignment of Retired Assets: Reassignment of computer hardware to a less-critical role is made at the sole discretion of Fort Belknap College's IT Department. It is, however, the goal of Fort Belknap College to – whenever possible – reassign IT assets in order to achieve full return on investment (ROI) from the equipment

and to minimize hardware expenditures when feasible reassignment to another business function will do instead.

Trade-Ins: Where applicable, cases in which a piece of equipment is due for replacement by a newer model, reasonable actions must be taken to ensure that a fair and market trade-in value is obtained for the old IT asset against the cost of the replacement. Fort Belknap College's Purchasing and Procurement manager or IT Asset manager will assume this responsibility.

Income Derived from Disposal: Whenever possible, it is desirable to achieve some residual value from retired or surplus IT assets. Any and all receipts from the sale of IT assets must be kept and submitted to the Finance Department. Income derived from sales to staff, the public, or students must be fully receipted and monies sent to Fort Belknap College's Finance Department. Sales to staff should be advertised through the company intranet or via e-mail.

Cannibalization and Assets Beyond Reasonable Repair: The IT manager is responsible for verifying and classifying any IT assets beyond reasonable repair. Equipment identified as much should be cannibalized for any spare and/or working parts that can still be put to sufficient use within the organization. The IT Department will inventory and stockpile these parts. Remaining parts and/or whole machines unfit for use or any other disposal means will be sold to an approved scrap dealer or salvaging company.

Decommissioning of Assets: All hardware slated for disposal by any means must be fully wiped clean of all company data. Fort Belknap College's IT Department will assume responsibility for decommissioning this equipment by deleting all files, company-licensed programs, and applications using a pre-approved disk-sanitizer. This sanitizer must **completely overwrite** each and every disk sector of the machine with zero-filled blocks. In addition, any property tags or identifying labels must also be removed from the retired equipment.

Harmful Substances: Hazardous materials such as lead, mercury, bromine, cadmium, etc. must be thoroughly removed from computer hardware before shipment to a landfill as rubbish. The IT Department may perform this action itself using government-approved disposal methods, or hire an accredited disposal company specializing in this service. No matter what the route taken, the removal and discarding of toxins from Fort Belknap College equipment must be in full compliance with local and federal laws.

Donations: IT assets with a net residual value that are not assigned for reuse, discarding, or sale to employees or external buyers, may be donated to a company-approved school, charity, or other non-profit organization (i.e. a distributor of free machines to developing nations). All donations must be authorized by Fort Belknap College. All donation receipts must be submitted to the Finance department for taxation purposes.

Information Technology Standards Policy

The Information Technology Standards Policy lists all technologies supported by the organization and serves as a guideline for all technology purchasing and use decisions, including hardware, software, peripherals, and network components. The primary goals of developing and implementing such a policy are:

- To ease purchasing decisions by pre-evaluating and pre-approving technology solutions.
- To reduce training and support costs and create economies of scale by narrowing the number of technologies and products used.
- To ensure integration and interoperability between technologies.
- To set parameters for future technology innovation and development.

The following standard technologies were selected based on prevalence in the organization or – in the case where two or more competing technologies previously existed – on an assessment of relative quality and performance as dictated by business needs.

Please refer to this document, which is located in the Appendices, when making a purchasing decision or when selecting technologies as part of a development project. Sections of this document may be extracted and used as part of project charters or other agreements where technology parameters should and must be set, such as in the case of contracted work.

PDA Usage Policy and Agreement

Purpose

The purpose of this policy is to define standards, procedures, and restrictions for connecting to Fort Belknap College's internal network(s) or related technology resources via any means involving mobile devices that are categorized as Personal Digital Assistants (PDAs). This policy applies to, but is not limited to, all devices that fit the following device classifications:

- Handhelds running the PalmOS, Microsoft Windows CE, PocketPC or Windows Mobile, Symbian, or Mobile Linux operating systems.

- Mobile devices that are standalone (i.e. connectible using wired sync cables and/or cradles.)

- Devices that have integrated wireless capability. This capability may include, but is not limited to, Wi-Fi, Bluetooth, and IR.

- Smartphones that include PDA functionality.

- Any related components of Fort Belknap College's technology infrastructure used to provide connectivity to the above.

- Any third-party hardware, software, processes, or services used to provide connectivity to the above.

The policy applies to any PDA hardware and related software that could be used to access Fort Belknap College resources, even if said equipment is not Fort Belknap College's sanctioned, owned, or supplied.

The overriding goal of this policy is to protect Fort Belknap College's technology-based resources (such as Fort Belknap College data, computer systems, networks, databases, etc.) from unauthorized use and/or malicious attack that could result in loss of information, damage to critical applications, loss of revenue, and damage to our public image. Therefore, all users employing PDA-based technology to access Fort Belknap College technology resources must adhere to company-defined processes for doing so.

Scope

This policy applies to all Fort Belknap College employees, including full- and part-time staff, contractors, freelancers, and other agents who utilize company-owned, personally owned, or publicly-accessible PDA-based technology to access the organization's data and networks via wired and wireless means. Such access to enterprise network resources is a privilege, not a right. Consequently, employment at Fort Belknap College does not automatically guarantee the granting of these privileges.

Addition of new hardware, software, and/or related components to provide additional PDA-related connectivity within Fort Belknap College facilities will be managed at the sole discretion of IT. Non-sanctioned installations of PDA-related hardware, software, and/or related components, or use of same within the organizational campus, or to gain access to organizational computing resources, are strictly forbidden.

This policy is complementary to any previously implemented policies dealing specifically with network access, wireless access, and remote access to the enterprise network.

Supported Technology

All PDAs and related connectivity points within the Fort Belknap College firewall will be centrally managed by Fort Belknap College's IT Department and will utilize encryption and strong authentication measures. Although IT is not able to manage the public network to which wireless-enabled PDA devices and smartphones initially connect, end-users are expected to adhere to the same security protocols while utilizing this equipment. Failure to do so will result in immediate suspension of all network access privileges so as to protect the company's infrastructure.

The following table outlines Fort Belknap College's minimum system requirements for a computer, workstation, or related device to properly support and sustain PDA connectivity and functionality. Equipment that does not currently meet these minimum

requirements will need to be upgraded before PDA implementation may be sanctioned by IT.

Eligible Users

All employees requiring the use of PDAs for business purposes must go through an application process that clearly outlines why the access is required and what level of service the employee needs should his/her application be accepted. Application forms must be approved and signed by the employee's unit manager, supervisor, or department head before submission to the IT Department.

Employees may use privately owned PDAs (under 'Supported Technology') for business purposes. If this is the case, the IT Department must approve the specific handheld and connection type as being secure and protected. However, the company's IT Department cannot and will not technically support third-party wireless hardware or software, or any other unapproved remote e-mail connectivity solution.

All expense forms for reimbursement of cost (if any) incurred due to the need for PDA-based access for business purposes must be submitted to the appropriate unit or department head. Financial reimbursement for PDA devices and related equipment is not the responsibility of the IT Department. If you foresee an upcoming need for PDA use in a business context, ask your leader to help you fill out a business case.

Policy and Appropriate Use

It is the responsibility of any employee of Fort Belknap College who is connecting to the organizational network via a PDA to ensure that all components of his/her connection remain as secure as his/her network access within the office. It is imperative that any wired (via sync cord, for example) or wireless connection, including, but not limited to PDA devices and service, used to conduct Fort Belknap College business be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account. Based on this, the following rules must be observed:

Employees using PDAs and related software to connect to Fort Belknap College's technology infrastructure will, without exception, use secure remote access procedures. This will be enforced through public/private key encrypted strong passwords in accordance with Fort Belknap College's password policy. Employees agree to never disclose their passwords to anyone, particularly to family members if business work is conducted from home.

All PDAs that are used for business interests, whether personal- or company-owned, must display reasonable physical security measures. Users are expected to secure all handhelds and related devices used for this activity whether or not they are actually in use and/or being carried. This includes, but is not limited to, power-on passwords. Any non-Fort Belknap College computers used to synchronize with PDAs will have installed whatever antivirus software deemed necessary by Fort Belknap College's IT Department. Antivirus signature files must be updated in accordance with existing company policy.

Passwords and other confidential data as defined by Fort Belknap College's IT Department are not to be stored on PDAs or their associated storage devices (such as SD and CF cards, as well as Memory Sticks and related flash-based supplemental storage media.)

Due to the potential for bandwidth conflicts within the Fort Belknap College campus, use of unsanctioned equipment operating within the 2.4 GHz range is strictly forbidden. If you have a need to use such equipment – for example, a wireless PDA or smartphone – please consult IT before proceeding further.

Prior to initial use for connecting to the Fort Belknap College network, all PDA-related hardware, software and related services must be registered with IT. If your preferred PDA solution does not appear on this list, contact the IT Department to have it registered and added to the list.

Remote users using non-Fort Belknap College network infrastructure to gain access to Fort Belknap College resources via their PDAs must employ for their devices and related infrastructure a company-approved personal firewall, VPN, and any other security measure deemed necessary by the IT Department. VPNs supplied by the wireless service provider should also be used, but only in conjunction with Fort Belknap College's additional security measures. IT will support its sanctioned hardware and software, but is not accountable for conflicts or problems whose root cause is attributable to a third-party product.

- For wireless-enabled PDAs, users must deactivate their devices when not in use in order to mitigate attacks by hackers, wardrivers, and eavesdroppers.
- Users must apply new passwords every business/personal trip where company data is being utilized on or synchronized to a PDA.

Any PDA that is configured to access Fort Belknap College resources via wireless or wired connectivity must adhere to the authentication requirements of Fort Belknap College's IT Department. In addition, all hardware security configurations (personal or company-owned) must be approved by Fort Belknap College's IT Department.

Employees, contractors, and temporary staff will make no modifications of any kind to company-owned and installed hardware or software without the express approval of Fort Belknap College's IT Department. This includes, but is not limited to, installation of PDA software on company-owned desktop or laptop computers, connection of sync cables and cradles to company-owned equipment, and use of company-owned wireless network bandwidth via these devices.

Fort Belknap College will maintain a list of approved PDA-specific software applications and utilities.

Employees, contractors, and temporary staff with Fort Belknap College-sanctioned wireless-enabled PDAs must ensure that their computers and handheld devices are

not connected to any other network while connected to Fort Belknap College's network via remote access.

All connections that make use of wireless PDA access must include a "time-out" system. In accordance with Fort Belknap College's security policies, sessions will time out after 30 minutes of inactivity, and will terminate after 8 hours of continuous connection. Both time-outs will require the user to reconnect and re-authenticate in order to re-enter company networks through a wireless PDA connection.

The PDA-based user agrees to immediately report to his/her manager and Fort Belknap College's IT Department any incident or suspected incidents of unauthorized access and/or disclosure of company resources, databases, networks, etc.

The PDA-based wireless access user also agrees to and accepts that his or her access and/or connection to Fort Belknap College's networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. As with in-house computers, this is done in order to identify accounts/computers that may have been compromised by external parties.

Fort Belknap College will not reimburse employees for business-related wireless PDA-based access connections made on a pre-approved privately owned ISP service. All submissions for reimbursement must be accompanied by sufficient and appropriate documentation (i.e. original service bill). Employees requesting reimbursement will also be asked to certify in writing prior to reimbursement that they did not use the connection in any way that violates company policy.

IT reserves the right to turn off without notice any access port to the network that puts the company's systems, data, users, and clients at risk.

Policy Non-Compliance

Failure to comply with the PDA Usage Policy and Agreement may, at the full discretion of the organization, result in the suspension of any or all-remote access privileges, disciplinary action, and possibly termination of employment.

IT Equipment Borrowing Policy and Loan Form

Equipment Borrowing Policy

BORROWERS ARE RESPONSIBLE FOR LOSS OR DAMAGE TO EQUIPMENT
EQUIPMENT THAT IS NOT PICKED UP WITHIN THE ONE HOUR OF THE BOOKED TIME MAY BE LOANED TO OTHERS.
A MINIMUM OF 1 WEEKS ADVANCE NOTICE IS REQUESTED TO ENSURE EQUIPMENT AVAILABILITY.

IT Equipment may be borrowed:

* By: Staff and Faculty.

* For the use of: research, instruction, presentations, and practicum use.

* For the period of: 24 hours and if longer will need approval from Department Supervisor.

NOTE: BORROWING TIMES MAY BE SHORTENED AT ANY TIME IN CASE OF SIGNIFICANT DEMAND

To borrow IT equipment, proper procedures must be done:

* Fill out a sign-out sheet with printed name, signature, name of equipment, FBC Tag Number, Serial number, model number, destination, and date.

Privileges to borrow IT equipment may be revoked or suspended due to the following:

* Repeatedly returning equipment late.

* Returning equipment that is damaged or otherwise not complete or in good condition.

* Repeatedly not picking up booked equipment.

To book required IT equipment, visit the IT Department.

If any assistance is needed for setting up or using the borrowed IT equipment, please contact the IT Department. The form needed to do this is located in the Appendices.

Network Security Policy for Portable Computers

Introduction

Portable computers offer staff the ability to be more productive while on the move. They offer greater flexibility in where and when staff can work and access information, including information on our Fort Belknap College network. However, network-enabled portable computers also pose the risk of data theft and unauthorized access to our Fort Belknap College network.

Any device that can access the Fort Belknap College network must be considered part of that network and therefore subject to policies intended to protect the network from harm. Any portable computer that is proposed for network connection must be approved and certified by the IT Department.

Protecting the Laptop

In order to qualify for access to our Fort Belknap College network, the laptop must meet the following conditions:

Network settings, including settings for our VPN, must be reviewed and approved by IT support personnel.

A personal firewall must be installed on the computer and must always be active.

Anti-virus software must be installed. Software must have active scanning and be kept up-to-date. Recommended anti-virus software is MacAfee Antivirus.

Laptop User's Responsibilities

The user of the laptop is responsible for network security of the laptop whether they are onsite, at home, or on the road.

The user of the laptop is responsible for keeping their anti-virus scanning software up-to-date at all times. It is strongly recommended that they update their anti-virus software before going on the road.

The user of the laptop shall access network resources via a VPN connection. Use of public Internet services is discouraged, as they do not offer adequate protection for the user.

Security Audits

The IT Department reserves the right to audit any laptop used for company business to ensure that it continues to conform to this certification policy. The IT Department will also deny network access to any laptop, which has not been properly configured and certified.

Anti-Virus Policy

Purpose

A virus is a piece of potentially malicious programming code that will cause some unexpected or undesirable event. Viruses can be transmitted via e-mail or instant messaging attachments, downloadable Internet files, diskettes, and CDs. Viruses are usually disguised as something else, and so their presence is not always obvious to the computer user. A virus infection can be very costly to Fort Belknap College in terms of lost data, lost staff productivity, and/or lost reputation.

As a result, one of the goals of Fort Belknap College is to provide a computing network that is virus-free. The purpose of this policy is to provide instructions on measures that must be taken by Fort Belknap College employees to help achieve effective virus detection and prevention.

Scope

This policy applies to all computers that are connected to the Fort Belknap College network via a standard network connection, wireless connection, modem connection, or virtual private network connection. This includes both company-owned computers and personally owned computers attached to the Fort Belknap College network. The definition of computers includes desktop workstations, laptop computers, handheld computing devices, and servers.

General Policy

Currently, Fort Belknap College has MacAfee anti-virus software in use. Licensed copies of MacAfee anti-virus software can be obtained from the IT Department. The most current available version of the anti-virus software package will be taken as the default standard.

All computers attached to the Fort Belknap College network must have standard, supported anti-virus software installed. This software must be active, be scheduled to perform virus checks at regular intervals, and have its virus definition files kept up to date.

Any activities with the intention to create and/or distribute malicious programs onto the Fort Belknap College network (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.) are strictly prohibited.

If an employee receives what he/she believes to be a virus, or suspects that a computer is infected with a virus, it must be reported to the IT Department immediately. Report the following information (if known): virus name, extent of infection, source of virus, and potential recipients of infected material.

No employee should attempt to destroy or remove a virus, or any evidence of that virus, without direction from the IT Department.

Any virus-infected computer will be removed from the network until it is verified as virus-free.

Rules for Virus Prevention

Always run the standard anti-virus software provided by Fort Belknap College.

Never open any files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source.

Never open any files or macros attached to an e-mail from a known source (even a coworker) if you were not expecting a specific attachment from that source.

Be suspicious of e-mail messages containing links to unknown Web sites. It is possible that the link is a malicious executable (.exe) file disguised as a link. Do not click on a link sent to you if you were not expecting a specific link.

Never copy, download, or install files from unknown, suspicious, or untrustworthy sources or removable media.

Avoid direct disk sharing with read/write access. Always scan a floppy diskette for viruses before using it.

If instructed to delete e-mail messages believed to contain a virus, be sure to also delete the message from your Deleted Items or Trash folder.

Back up critical data and systems configurations on a regular basis and store backups in a safe place.

Regularly update virus protection on personally owned home computers that are used for business purposes. This includes installing recommended security patches for the operating system and other applications that are in use.

IT Department Responsibilities

The following activities are the responsibility of the Fort Belknap College IT Department:

The IT Department is responsible for maintaining and updating this Anti-Virus Policy.

The IT Department will keep the anti-virus products it provides up-to-date in terms of both virus definitions and software version in use.

The IT Department will apply any updates to the services it provides that are required to defend against threats from viruses.

The IT Department will install anti-virus software on all Fort Belknap College owned and installed desktop workstations, laptops, and servers.

The IT Department will assist employees in installing anti-virus software according to standards on personally owned computers that will be used for business purposes. The IT Department will not provide anti-virus software in these cases.

The IT Department will take appropriate action to contain, remove, and assist in recovery from virus infections. In order to do so, the IT Department may be required to disconnect a suspect computer from the network or disconnect an entire segment of the network.

The IT Department will perform regular anti-virus sweeps.

The IT Department will attempt to notify users of Fort Belknap College systems of any credible virus threats via e-mail or telephone messages. Virus reports will not be acted upon until validated. Employees should not forward these or any virus warning messages in order to keep network traffic to a minimum.

Department and Individual Responsibilities

The following activities are the responsibility of Fort Belknap College departments and employees:

Departments must ensure that all departmentally managed computers have virus protection that is in keeping with the standards set out in this policy.

Departments that allow employees to use personally-owned computers for business purposes must implement virus protection processes and procedures that are in keeping with the standards set out in this policy.

All employees are responsible for taking reasonable measures to protect against virus infection.

Employees must not attempt to either alter or disable anti-virus software installed on any computer attached to the Fort Belknap College network without the express consent of the IT Department.

Enforcement

Any employee or student who is found to have violated this policy are subject to the Employee/Student Conduct Code and may be subject to disciplinary action, up to and including termination of employment/school.

Student & Employee Handbook

Introduction

This document establishes computer usage guidelines for the Fort Belknap College. Fort Belknap College offers a wide array of computing, networking, and telecommunications resources and services to members of the college community. These services are in place to facilitate teaching and learning, research, and administrative activities and to further Fort Belknap College's mission. This document contains information technology policies and procedures and also outlines responsibilities of those who use computing and networking facilities at the college. Users of these services agree to abide by and be subject to the terms and conditions contained in this and all other applicable College policies. Some departments on campus may have additional facilities, practices, and policies that apply to use of computing facilities in those departments. These policies are designed to enable high- quality services and maximize productivity while protecting the rights of all members of the community. All students and employees of Fort Belknap College are required to read and comply with the policies laid out in this Manual (which may be amended from time to time). This manual does not attempt to anticipate every situation that may arise and does not relieve anyone of their obligation to use common sense and good judgment.

Questions or suggested improvements on these policies and procedures or other computing matters should be addressed to the Manager of Information Technology at Fort Belknap College. This handbook is posted on the IT Department web site and is reviewed every two years by the Committee on Information Technology.

Access to Information Technology Resources

Eligibility

Information Technology Resources (computer hardware, software, telephone systems, networks, services, data, and other information) are made available at FBC to support and facilitate the teaching, research and administrative functions of the College. Access to these resources is provided to faculty, administration, staff, and enrolled students consistent with their responsibilities.

Under no circumstances may anyone use college IT resources in ways that are illegal (e.g. copyright violations), threaten the College's tax- exempt or other status, or interfere with reasonable use by other members of the College community.

Other individuals, upon submission of a request, may be granted access to some, or all, of FBC IT resources by the President of the College. The terms of access will be stated at the time access is granted.

Account Activation/Termination

E-mail access at FBC is controlled through individual accounts and passwords. Each user of FBC's e-mail system is required to read and sign a copy of this E-Mail Acceptable Use Policy prior to receiving an e-mail access account and password. It is the responsibility of the employee and student to protect the confidentiality of their account and password information.

Personal Computers on the Network

Internet addresses are provided by IT Department. In order to obtain a static Internet (TCP/IP) computer address the owner of the system must register the computer with IT Department network services.

The rules and regulations contained in this policy pertaining to electronic mail and Internet access are equally applicable to the use of personal machines for file sharing or as servers. If bandwidth or other problems occur, IT Department reserves the right to discontinue access to the machine. Computers connected to the network may not be used as servers for private enterprises, commercial activity, or personal profit. Computers connected to the network may not be used to provide access to the Internet for anyone not formally affiliated with the College. If personal computers on the FBC network are used as servers, the administrator has the additional responsibility to respond to any use of the server that is in violation of these policies and procedures. Server administrators must take steps to prevent recurrence of such violations and report these violations to the FBC Network Administrator (postmaster@mail.fbcc.edu).

IT Department reserves the rights to disconnect any network port whose activity causes an adverse effect on the network or on any other user. Network connections may also be revoked in the case of malicious or inappropriate computing activity on the network. See Noncompliance and Sanctions for examples of these activities.

IT Department reserves the right to restrict access to the network during expansion, or for diagnostic and maintenance services. Every effort will be made to provide advance notification and schedule such disruptions during times of minimum impact and traffic.

Virus Protection

Fort Belknap College requires all existing and incoming students to install anti- virus software on their personal computers by the end of the second week of classes each semester. Failure to do so can result in the loss of connectivity to the Fort Belknap College network until anti- virus software is installed. AVG anti- virus

software is provided free to all students. Other anti- virus products may be substituted as long as they are kept current.

Dial-Up Connections

For all campus users the primary access to FBC computing services is through the campus network. Dial- in access via modem is not provided.

Personally Owned Equipment

IT office also provides repair for personally owned computers. Computers are repaired at a cost rate established by FBC. There is a minimum charge for examining the equipment if repair is not needed. Equipment must be delivered to the IT office in the basement of White Clay Hall during regular business hours. IT Department will be available each day between 7 am and 4 p.m. to receive equipment, or by special arrangement by calling x211 or by e- mail (postmaster@mail.fbcc.edu). Payment for the repairs must be made by cash, check, or money order when the equipment is picked up. Charges for repair cannot be applied to your Fort Belknap College account.

Electronic Mail (E-Mail)

Department or Group Accounts

By special permission, college departments and student groups will be granted a single account to facilitate connections between the department or group and interested parties. The department or group must identify one person to be responsible for the account and to act as the contact person. In addition, student organizations must be registered with Student Support Services before an account will be granted.

All employees and students of FBC are entitled to an e-mail account. E-mail accounts will be granted to third party non-employees on a case-by-case basis. Applications for these temporary accounts must be submitted in writing to Fort Belknap College President. All terms, conditions, and restrictions governing e-mail use must be in a written and signed agreement. E-mail access will be terminated when the employee or third party terminates their association with FBC, unless other arrangements are made. FBC students who have graduated from FBC will still be on FBC's Alumni E-mail system for as long as the student wants it. FBC is under no obligation to store or forward the contents of an individual's e-mail inbox/outbox after the term of their employment has ceased.

Appropriate Use of E-mail

FBC strongly recommends that e- mail not be used for confidential communication. E- mail is now considered a formal written record that carries the same legal weight as a formal memorandum. Users of e- mail should remember that e- mail messages become the possession of the receiver and can be easily duplicated and redistributed by recipients. Messages that have been deleted can unintentionally be retained on system backup files. In addition, even secure passwords are not completely confidential. When a private message needs to be conveyed between two individuals, a conversation is the best way to accomplish it, and messages that should not be preserved should be deleted immediately.

College policy prohibIT Department certain types of e- mail. These include mail that may be perceived as harassment, political campaigning, or commercial solicitation. Chain mail is also prohibited. Violators will be subject to loss of computer access privileges, as well as additional disciplinary action as determined by the FBC judiciary procedures. Certain types of e- mail,

including but not limited to harassing e- mail, may also subject the sender to civil or criminal penalties. In spite of College policy, e- mail can be abused by malicious users who know the owner's computing ID and password. Users are responsible for protecting their own passwords.

ListServ Lists

ListServ is a commercial software product installed on our E- mail system. It is designed to provide an easy way to create and maintain large E- mail mailing lists. These lists can be used for the one- way distribution of information, for E- mail based discussion, questions and answers, etc. Lists are created and "owned" by an E- mail user who manages the lists behavior.

Any faculty, staff, or student member of the Fort Belknap College community is entitled to become a ListServ list owner. Campus- based organizations and departments are also entitled to own lists, but an individual within the group must be designated as the list owner. Students must be in good standing with the Dean of Students office and student organizations must be registered with Student Support Services.

All lists must be approved by the IT Department ListServ administrator prior to creation, but the following general guidelines apply:

1.) The purpose of the list must pertain to Fort Belknap College business.

2.) Lists are not open to off- campus subscribers unless special permission is obtained. However, Fort Belknap College students or employees who use off- campus E- mail addresses are allowed to own and belong to lists.

3.) It is the list owner's responsibility to learn the commands necessary to manage the list's subscribers.

4.) Under no circumstances can a list be used to participate in or promote activities that are illegal, violate the Fort Belknap College code of conduct, or the Fort Belknap College Policy and Procedure Manual.

To apply for list ownership and select a list type, please read Becoming a ListServ List Owner from which you can create your list.

ListServ Mass Mailing Lists

As a service to the Fort Belknap College community, several E- mail based mass mailing lists have been created. These are designed to facilitate the timely and cost- effective distribution of information to the campus community. E- mail now reaches almost all faculty, administration and staff and students. Participation in the mass mailing lists is voluntary.

In order that these lists remain a reliable means of communication, it is important that members of the FBC community abide by a few guidelines. These guidelines are not designed to limit free speech but are intended to keep your mail volume at a reasonable level.

Most importantly, anonymous mailings are prohibited. The sender's real name must be identified (in full) within the body of the message - not just at the top in the "from" line. The mass mailing lists are intended for:

1. Announcement of campus events and deadlines

2. Changes in campus policies, procedures, organizations, or

departments

3. Notification of the availability of services and/or facilities

Any individual wanting to post a message to the mass e- mail lists that falls outside of the guidelines, but is felt to be of vital importance to the community, must send a request for an exception to: The request will be directed to the appropriate college official (Dean of Students, Dean of Academics, President). If the exception is approved the message will be posted by that college official. Approval or denial will be communicated to the person making the request. Examples of such exceptions might include reports of inappropriate behavior, including campus vandalism, and racist, sexist, or other acts against members of the community.

Please consider your audience carefully (e.g., do not send a mailing to all employees if you only need to reach faculty and students). These lists are NOT intended for messages of a personal nature. Examples of inappropriate uses include, but are not limited to:

1. Soliciting support (financial or otherwise) for charity or special causes not connected with a College effort

2. Personal opinion, public debate, or campaigning

3. Give- aways (personal property such as furniture, tickets, equipment, books, etc.)

4. Unverified public service announcements (such as virus alerts, unsafe products, etc.)

5. Chain mail

6. Services offered or services sought (except for College related services)

7. Lost and found (except when it is Fort Belknap College property, or involves animals)

8. Items for sale - or items desired (including houses, tickets, books, services, etc.)

9. Rides

Penalties for Violations

Any violation will be sent to the appropriate referral person. First, Dean of Students, if it can not be solved there, onto Dean of Academics with Dean of Students, if it can not be solved there, onto IT Technology Committee, if it can not be solved there, onto FBC Executive Committee and President has the authority for penalties.

Licensing of Software

The use of all software in the College is protected by copyright laws and must be used in accordance with software licenses. It is against College policy to copy or reproduce any licensed software. Unlicenced software may not be installed on any computers owned by FBC. The unauthorized use or copying of software is a serious violation of policy and subject to disciplinary action. Such unauthorized use or copying may also subject the offending individual to lawsuits by third parties.

Software on Personally Owned Equipment

FBC educational licensing agreements for software specifically limit installation to machines owned by the college. Therefore, software purchased by FBC under these agreements may not be installed on personally owned equipment. Our current license

agreement with Microsoft does allow the installation of one copy of Microsoft MSDNAA on the home machine. For information on these programs, FBC current licensing agreements, and exceptions, contact the Director, IT Department, Consulting Services.

Security

Security On Data Networks

Security for access to the data network and to files or applications on a server is implemented via user ID and password systems. Each user is responsible for all e- mail transactions made under the authorization of his or her ID and password, and for all network e- mail activity originating from that connection. Users are personally responsible for the security of the ID and password assigned to them. Viewing, copying, altering or destroying any file, or connecting to a computer on the network without explicit permission of the owner is prohibited. Users may not use the FBC data network or telephone system to attempt to circumvent protection schemes or exercise security loopholes in any computer, network, or telephone system component.

User IDs and Passwords

Passwords should be known only to the person responsible for the account and user ID. Ways to ensure this include avoiding storing passwords or any other information that could be used to gain access to other computing resources on your workstation, never sharing passwords, and never taping passwords to a wall, under a keyboard, or in other easily discoverable areas. Access to user IDs may not be loaned or sold and any suspected breach of password security should be immediately reported to the IT Department e- mail administrator. Passwords should be changed (at least) every six months.

Protecting Desktop Equipment and Files

Backups and protection of files stored on desktop equipment are the responsibility of the user of that equipment. Users must back up their work files on a regular basis. Department members are responsible for ensuring that critical files are backed up in their areas. (see appendics)

Individual users are responsible for safeguarding the equipment entrusted to them by the college. This includes reasonable protection of equipment from damage and theft. Individual users are also responsible for safeguarding any equipment they own personally and bring to campus.

Confidentiality and Privacy

FBC takes reasonable steps to protect users from unauthorized entry into their accounts or files, whether by other users or by system administrators, except in instances where a system- related problem requires such entry. A limited number of authorized FBC personnel must occasionally monitor information on the network and/or computer systems to maintain the integrity of the systems. This access is required for reasons that include, but are not limited to, trouble- shooting hardware and software problems; preventing unauthorized access and system misuse; providing for the overall efficiency and integrity of the systems; protecting the rights and property of the College; ensuring compliance with software and copyright, distribution, and other College policies concerning the use of the computer network; and complying with legal and regulatory requests for information.

System monitoring is a mechanism for keeping track of computer system activities, rather than a method for accessing private information. IT Department personnel also take reasonable steps to prevent the dissemination of information concerning individual user activities. It is the policy of IT Department to disclose neither

the contents of electronic mail and data files stored in or transmitted via the College Computer System nor the activities of individuals on the campus network to other individuals within or outside the College community in the absence of a court order, or other legal mandate, or permission of the owner.

Private communication via computer is treated with the same degree of protection as private communication in other media. However, due to limitations of current technologies, which are inadequate to protect against unauthorized access, the confidentiality of e- mail and other system files can not be assured. All users should be aware of this and use reasonable caution when transmitting confidential materials.

Central Computer Operations

Access to computer operations areas is restricted to those responsible for operation and maintenance. Computing facilities on campus are secured when not open for business. IT Department takes action to provide reasonable protection against environmental threats such as flooding, lightning, extreme temperatures, and loss or fluctuation of electrical power for central server and network facilities. IT Department maintains procedures for protecting critical data that reside on central servers. While FBC provides security for files stored on central computing facilities, FBC cannot be responsible for protection against floods, fires, and catastrophic events of this type. Backup files from central servers are kept for only a few days. IT Department does not guarantee the availability of backups for the restoration of files deleted through user error.

Responsible Use of Networks and Computing Facilities

Fort Belknap College is a public institution fully committed to the ideals of academic freedom, freedom of expression, and cultural

diversity. At the same time, inappropriate behavior and malicious misuse of computing resources that in any way degrades the College equipment and services or violates the rights of others in the community is strictly prohibited.

Individual Responsibility

While IT Department is responsible for monitoring the use of computer systems, it is also the responsibility of all individuals in the FBC community to urge their peers and colleagues to use the network and systems appropriately. This is the only way that the integrity and availability of the network and systems can be ensured for everyone. Each member of the community is responsible for using only those accounts or computers for which he or she has authorization and is responsible for protecting all passwords. Individual responsibility includes respecting the rights of other users. Individuals are urged to report unauthorized use of computers, networks, or other IT Department facilities on campus by calling the IT Department e- mail administrator or notifying the Information Technology Department.

Logging In

All students, employees, and individuals will see the below message each time they log into a computer.

This is a private computer system and is the property of Fort Belknap College. It is for authorized use only. Users have not explicit or implicit expectation of privacy. Any or all users of this system maybe be intercepted, monitored, recorded, copied, audited, inspected and disclosed to management and law enforcement personnel if applicable. By using this system, the user consents to the aforementioned practices at the discretion of management. Unauthorized or improper use of this system may result in administrative disciplinary action and or civil and

criminal penalties. By continuing to use this system you indicate you are aware and consent to these terms and conditions of use. DO NOT LOGON if you do not agree to the conditions stated above.

Institutional Privileges

Fort Belknap College reserves the right to allocate resources in different ways in order to achieve maximum usage. To accomplish this, the system administrators may suspend or terminate privileges of individuals without notice if malicious misuse or use inconsistent with this policy, any other College policy, or applicable law is discovered. Privileges may also be suspended, without notice, to meet time dependent, critical operational needs. System administrators may also limit the number of messages or files that each user has in order to keep the system functioning.

Legal Compliance

All existing federal and state laws and College regulations and policies apply to the use of computing resources and all users of such resources are required to be in compliance with all laws, regulations and policies at all times. This includes not only those laws and regulations that are specific to computers and networks, but also those that apply generally to personal conduct.

Copyright on Digital Information Systems

Introduction

Individuals using computers and networks ("Digital Information Systems") at Fort Belknap College (the "College") are responsible for complying with copyright laws and the College's policies and procedures regarding use of the Digital Information Systems. The College reserves the right to deny, limit, revoke or extend

computing privileges and access to the Digital Information Systems in IT Department discretion. In addition, alleged violations of this procedure, the College's policies regarding use of the Digital Information Systems, or other policies of the College in the course of using the Digital Information Systems may result in an immediate loss of computing privileges and may also result in the referral of the matter to the College's judicial system or other appropriate authority.

The procedures outlined below will apply when the College receives notification of an alleged copyright infringement. For purposes of these procedures, an E−mail message shall be considered a written notice or request.

Notification of Infringement

1. Copyright holders who believe their copyrighted material has been infringed by an account holder must notify the College's President of the allegedly infringing action or material in writing. The notification must:
   a) identify the copyrighted material being infringed in sufficient detail to permit the College to locate the allegedly infringing material on the College's Digital Information Systems,
   b) state the basis for the claim of possible infringement,
   c) state the basis for the copyright holder's copyright in the work (e.g., author, owner, assignee).

2. The Designated Agent will notify the account holder who appears to have posted the allegedly infringing material, and will investigate the complaint promptly.

3. If, after conducting an investigation, the IT or Designated Agent determines that the allegedly infringing material

appears to infringe the copyright of the copyright holder, the Designated Agent will follow the procedures for Removal of Infringing Material set forth below.

Removal of Infringing Material

In the event that the allegedly infringing material is being used for an active class at the College, the Designated Agent will attempt to work out an arrangement with the copyright holder for use of the allegedly infringing material by the account holder until the end of the current semester. Failing a satisfactory arrangement, the Designated Agent will conduct an investigation of the incident and take action as set forth below regarding any allegedly infringing material.

If, after the Designated Agent's investigation, the Designated Agent determines that the allegedly infringing material appears not to infringe the copyright of the copyright holder, the Designated Agent will notify the copyright holder and the account holder of the determination. If the copyright holder disagrees with the determination of the Designated Agent, the copyright holder may request in writing that the College ask IT Department attorney's to render an opinion as to whether the allegedly infringing material constitutes copyright infringement pursuant to paragraph below.

If, after the Designated Agent's investigation, the Designated Agent determines that the allegedly infringing material appears to infringe the copyright of the copyright holder, the Designated Agent will notify the President for Information Technology, Fort Belknap College, the copyright holder and the account holder whose account was used to post the allegedly infringing material.

Upon receipt of such notification from the Designated Agent, the President Fort Belknap College, will direct the appropriate IT Department staff member to remove, or block access to, the allegedly infringing material.

Upon receipt of notification from the Designated Agent that the allegedly infringing material appears to infringe the copyright of the copyright holder and is being blocked or removed from FBC Digital Information Systems, the account holder may request that the Designated Representative restore the removed or blocked material based on the account holder belief that the allegedly infringing material is not infringing. Such request must be in writing and include a detailed statement of the basis for the account holder's belief that the allegedly infringing material is not infringing, as well as a request that the removed or blocked material be restored.

If the Designated Agent receives such request from the account holder, the Designated Agent will provide a copy of the request to the copyright holder.

If, within 10 days after a copy of the account holder's request is sent to the copyright holder by the Designated Agent, the Designated Agent has not received a written request from the copyright holder to continue the blocking or removal of the allegedly infringing material, the Designated Agent will notify the President for Information Technology, Fort Belknap College to restore the material. The President for Information Technology, Fort Belknap College, will restore the allegedly infringing material within four days after receipt of such notification.

If the Designated Agent receives within 10 days a written request from the copyright holder to continue the blocking or removal of the allegedly infringing material is received from the original sender, the Designated Agent will provide copies of all correspondence in the matter to the President for Information Technology, Fort Belknap College, who will forward copies of such correspondence to the College's attorneys, who will be asked to render an opinion as to whether the allegedly infringing material

constitutes copyright infringement. If the allegedly infringing material is determined not to constitute copyright infringement, the material will be restored by the President for Information Technology, within four days of such determination.

Designation of Agent to Receive Notification of Claimed Infringement

This is to notify copyright holders that Fort Belknap College's Designated Agent to receive notices and requests concerning claimed infringement, pursuant to the Digital Millennium Copyright Act, is President. Any copyright holder wishing to send a notice to Fort Belknap College regarding possible copyright infringement should file that notice in writing with President at the following address:

President
Fort Belknap College
BlackFeet Street
PO Box 159
Harlem, MT 59526
Telephone: 406-353-2607
Fax: 406-353-2898

Indemnification of Fort Belknap College

Users agree, in consideration of access to the College's computing, networking and media services, to indemnify, defend, and hold harmless the College for any lawsuits, claims, losses, expenses or damages, including, but not limited to, the user's access to or use of the College's computing, networking, and media services and facilities.

Noncompliance and Sanctions

Information Technology Services may suspend or terminate all computing privileges of any individuals without notice who engage

in improper computing activities. Serious cases, as determined by the President of Fort Belknap College, will be referred to the Board of Directors for disciplinary action. Such disciplinary action may include the suspension, expulsion, or termination of the offending individual, as appropriate and as determined at the sole discretion of Fort Belknap College. Where violation of state and federal law is involved, cases will be referred to the proper legal authorities for action. The following serves to provide examples of violations of computing or computing facility policies at Fort Belknap College. The list of violations includes, but is not limited to:

Malicious misuse. Examples

Using IDs or passwords assigned to others, disrupting the network, destroying information, removing software from public computers, spreading viruses, sending e−mail that threatens or harasses other people (**Class A** - misdemeanor under Montana State law), invading the privacy of others, and subscribing others to mailing lists or providing the e−mail addresses of others to bulk mailers without their approval.

Unacceptable use of software and hardware

Examples: knowingly or carelessly running or installing unlicensed software on any computer system or network; giving another user a program intended to damage the system; running or installing any program that places an excessive load on a computer system or network, or compromises the security of the systems or network; violating terms of applicable software licensing agreements, including copying or reproducing any licensed software; or violating copyright laws and their fair use provisions through inappropriate reproduction or dissemination of copyrighted text, images, or other materials; using imaging equipment to duplicate, alter and subsequently reproduce official documents.

Inappropriate access

Examples: unauthorized use of a computer account; providing misleading information in order to obtain access to computing facilities; using the campus network to gain unauthorized access to any computer system; connecting unauthorized equipment to the campus network; unauthorized attempts to circumvent data protection schemes to uncover security loopholes (including creating and/or running programs that are designed to identify security loopholes and/or decrypt intentionally secure data); knowingly or carelessly performing an act that will interfere with the normal operation of computers, terminals, peripherals, or networks; deliberately wasting or overloading computing resources, such as printing too many copies of a document; or other activities.

Inappropriate use of electronic mail and Internet access

E−mail communications are subject to statements of conduct as published in the Student, Faculty, Administrator, Staff, and Maintenance and Operations Handbooks, as well as all applicable federal and state laws. In addition, other activities that threaten the integrity of the system or harm individual users are not allowed. These include, but are not limited to initiating or propagating electronic chain letters; inappropriate mass mailing including multiple mailings to news groups, mailing lists, or individuals, forging the identity of a user or machine in an electronic communication or sending anonymous e−mail; using another person's e−mail account or identity to send e−mail messages; attempting to monitor or tamper with another user's electronic communications; reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner; or using e−mail or personal web page advertising to solicit or proselytize others for commercial ventures, religious or political causes, or for personal gain.

Reporting Critical Service Outages During An Academic Term

During normal business hours (Monday – Friday, 8:30 a.m. - 4:30 p.m.), members of the College community should notify the IT Department of suspected problems with computers, networks, and related information technology resources. IT will investigate the problem and determine corrective action. If the IT staff determines that the problem is related to the campus network or a server they will notify IT Department Manager who will take appropriate action. Resolution of critical service outages (defined below) will be a top IT Department priority and will be resolved in a timely manner. Non–critical problems will be investigated and resolved as soon as is feasible.

Outside of business hours and on college holidays suspected critical service outages should be reported as follows:

4:30 p.m. – 10 p.m. (Monday – Friday) and
10 a.m. – 10 p.m., Saturday and Sunday

Any suspected critical service outages should be reported to the Department Head on duty in the Fort Belknap College Lab. The student will follow prescribed diagnostic routines to determine if the problem is indeed of a critical nature. If so, s/he will call the appropriate IT Department staff member to resolve the problem. No member of the community should call IT Department staff outside of normal business hours.

Outside of these times, suspected critical service outages should be reported at the next designated time the following day.

A critical service outage is defined as one or more of the following:

1. Failure of the campus network equipment or Internet connection making it impossible for a majority of users to

access on campus or off campus resources.

2. Campus wide printing failure (not individual printers).

3. Failure of a majority of computers in a public computer lab.

4. Failure of the campus web server affecting the entire campus.

5. Failure of the campus telephone system making it impossible for a majority of users to make outgoing calls or receive incoming calls.

6. Failure of the college e−mail system affecting the entire campus.

7. Failure of the college administrative system affecting the entire campus.

Chain of Command

All violations will be report to the Dean of Students and IT Department Manager. Dean of Students will report to the President who has the final decision.

FORT BELKNAP COLLEGE'S INFORMATION TECHNOLOGY USER AGREEMENT

I have read and understand the INFORMATION TECHNOLOGY HANDBOOK. I understand if I violate the rules explained herein, I may face legal or disciplinary action according to the Fort Belknap College Code of Conduct policy.

Name:_____

Signature:_____

Date:_____

APPENDICES

Cyber crime Report Form

Incident Number: _____

Date of Incident: _____

Time of Incident: _____

First IT Contact (Name): _____

Incident Information:

	Details/Notes
How was the attack or intrusion executed or perpetrated?	
What systems or network components were involved in the attack or intrusion?	
What steps or precautions were taken to stop or remedy the attack?	
Is there a suspect in mind or not (i.e. former employee)?	
What evidence can be compiled to help authorities (i.e. log files, IDS data, etc.)?	

Affected System Information:

Affected System	**Location**	**Damage?**
1.		
2.		
3.		

Other Notes on Nature of Incident:

_____
_____
_____
_____

IT Staff Member(s) Assigned:

7. _____
8. _____
9. _____

Authority Contact Information:

Type of Cyber crime	Appropriate Law Enforcement Agency
Computer intrusion/hacking	FBI local office, the National Infrastructure Protection Center (NIPC), or a US Secret Service field office.
Password trafficking	FBI local office, the National Infrastructure Protection Center (NIPC), or a US Secret Service field office.
Copyright piracy	FBI local office or a US Customs Service local office.
Theft of trade secrets	FBI local office
Internet fraud	FBI local office, US Secret Service field office, Federal Trade Commission, Securities and Exchange Commission, or The Internet Fraud Complaint Center.
Internet harassment	FBI local office
Internet bomb threat	FBI local office or an ATF field office.

(Note: Consult the resources found in the Cyber Criminals Most Wanted sites for reporting Internet crime in Canada and across the globe.)

IT Manager (Signature): _____

Information Technology Policy and Procedure Handbook for Employees

Employee Agreement

I, _____, have read and understand the above Information Technology Policy and Procedure Handbook Policy, and agree to adhere to the rules outlined therein.

_____ _____
Employee Signature Date

_____ _____
Manager Signature Date

_____ _____
IT Administrator Signature Date

IT Equipment Loan Form

Name: _____ Department: _____

Phone Number: _____ E-mail Address:_____

Department Head: _____

Equipment Information: _____

_____

_____

_____

Reason equipment is being borrowed: _____

_____

_____

_____

Location where borrowed equipment will be used: _____

_____

Terms of Loan:

The equipment indicated above is the property of Fort Belknap College and is to be used only for the purposes indicated in the borrowing policy.

Period of loan: From _____ To _____

Restrictions of use: _____

_____

_____

□ I have read and understand the equipment borrowing policy detailed above.

□ I understand that I am responsible for damage or loss of the above equipment while it is in my care, custody, and control.

Signature of borrower: _____ Date:_____

Authorized by: _____ Date:_____

IT Department Representative

Complete upon return of loaned equipment:

I, _____ (print name), acknowledge receipt and inspection of the equipment listed above.

Remarks:

_____

_____

Signed: _____ Date:_____

Desktop Computer Installation Checklist

Purpose

This form is to be used when a client/user requests the addition or reconfiguration of a computer on Fort Belknap College network.

Prior to Installation

Prior to installation, ensure that a Move/Add/Change Request Form has been completed. The client/user must also be contacted in order to schedule a date and time for service.

Desktop Computer Installation Checklist

The form below must be filled out by the IT Department technician tasked with installing or reconfiguring the computer.

A) Backup of Current Machine Data (if applicable)

Approach being used for data backup and transfer:
_____
Make sure that the following items are backed up from the current machine:

- _____ Internet favorites and bookmarks
- _____ E-mail address book
- _____ Desktop shortcuts

* **_____ Internet Browser profile:**
  - _____ Internet Explorer profile
  - _____ Other
* **_____ Document folders: Everything in My Documents and My Files folders.**
  - _____ Check for multiple occurrences of My Documents or My Files folders
  - _____ Check for multiple user profiles
* **_____ Check for additional data by searching for .doc, .xls, and .wpd**
* **_____ Palm/Pocket PC desktop profile (if applicable)**
* **_____ FTP program settings (if applicable)**
* **List any other folders/files included in backup and transfer:**
* _____

* _____

* _____

* ***The user is responsible for backing up any music or photo files before the installation appointment.**

B) Inventory of Current System

This section is to be completed prior to the installation of the PC and is meant as an inventory for the systems currently being used and as a guide to assist in the backup from the current machine (if applicable).

Is the installation a rebuild or new PC installation (select one)? Rebuild New Installation

Is the user present for the inventory procedure (select one)? Yes No

Network properties:

- IP address: _____
- Gateway: _____
- DNS host: _____
- OS domain information: _____
- Computer name: _____
- Workgroup: _____
- Computer login name: _____

What browser is currently used? _____

What e-mail client is currently used? _____

What word processor program is currently used? _____

What calendar program is currently used? _____

Is data currently synchronized with a PDA? _____

What other peripheral devices are in use (scanner, digital camera)? _____

_____

_____

List any software installed on the current machine that will not be installed by default on the new machine. Put a star beside the software that the client requests to have on the new machine beyond the standard configuration:

_____ _____

_____ _____

_____ _____

_____ _____

Before taking down the old machine:

- _____ Remove the TCP/IP properties
- _____ Delete My Documents personal files and user's e-mail profile
- _____ Empty the Recycle Bin

C) Setup of the New Machine

Date: _____
Name of Technician: _____
Computer Name: _____
Login(s): _____
_____
Is the computer to be used for multiple clients (select one)? Yes No
Is the user present for the installation (select one)? Yes No

_____ Configured the network properties (IP address, gateway, host, OS domain, computer name, workgroup)
_____ Installed and check activation of anti-virus software
_____ Transferred "My Documents" personal files and user profile from external storage device and place in correct folders
E-mail setup:

- Client used on old PC _____
- Client to be used on new PC _____
- _____ Address book restored
- _____ E-mail settings and/or local files restored.

Browser setup:

- _____ Restored Internet favorites or bookmarks.
- _____ Installed Internet Explorer
- _____ Other

Word processing software:

- _____ Installed Microsoft Word
- _____ Installed WordPerfect
- _____ Other

Software setup:

- _____ Installed all approved applications (listed below):
  - _____ _____
  - _____ _____
  - _____ _____
  - _____ _____

_____ Run Windows update and install updates (if applicable)
_____ Set up calendar
_____ Completed drive mappings (list drives below):

- _____ _____
- _____ _____

- _____ _____

_____ Restored all other data and files
_____ Deleted user data from the file server (if applicable)
Hardware installed:

- _____ Installed printer drivers.

* **Type:** _____ __ * **_____ Local** * **_____ Networked** * **Path:** _____ ___	* **Type:** _____ ___ * **_____ Local** * **_____ Networked** * **Path:** _____ ___

- _____ Installed scanner.
- PDA set up:
  - _____ Installed PDA software
  - _____ Installed synchronization software
  - _____ Verified synchronization
- _____ Other (digital camera, lab equipment)

_____ Deleted unnecessary icons from the Desktop and Start menu.
_____ Had user set logon password.
_____ Ensured that the anti-theft cable (if applicable) is removed from the old machine and secured to the new machine.

D) Ensure the Client/User Can Perform the Following

This section needs to be filled out prior to the technician leaving the installation/reconfiguration area to ensure that the system is functioning properly. The user:

_____ Can log in to all resources.

_____ Has located where documents were restored.

_____ Has found their Internet favorites or bookmarks.

_____ Has found drive mappings.

_____ Can print documents to all printers.

_____ Can find and open previously saved documents.

_____ Can save new documents.

_____ Has tested the scanner and any other attached hardware, and all is functioning properly.

_____ Can open and use their calendar functions.

_____ Can open their e-mail account and has received a test message.

_____ Can access old saved mail.

_____ Has located sent mail.

_____ Can access all applications used on a regular basis.

_____ Has all requested and approved software packages installed and are functioning properly?

_____ Has verified speaker functionality.

E) Receive Verification

Fill out the following form and have the user sign, verifying the installation.
Technician Name: _____ Date: _____
I, _____, verify that the above tasks were completed and that I have been instructed in using my new computer.
User Signature _____ Date: _____

IT Records Form

A copy of this completed form should be kept on file to ensure that service information is catalogued for each user workstation.

<table>
<tr><td colspan="2">Technician Assigned: _____</td><td>Call ID#: _____</td></tr>
<tr><td>Brand: _____</td><td>Model#: _____</td><td>CPU: _____</td></tr>
<tr><td colspan="2">Memory Type: _____
Hard Disk Drive: _____
Serial Number: _____
Comp. ID/Name: _____</td><td>IP: _____
Floppy Disk Drive: _____
Port Number: _____</td></tr>
<tr><td colspan="3">Additional Comments:</td></tr>
</table>

Operating Systems/Desktop				
Component	**Current Standard**	**Emerging Standard**	**Next Review**	**Comments**
Operating System				
Desktop Workstation				
Laptop Computers				
Internet Browser				
SERVERS				
Component	**Current Standard**	**Emerging Standard**	**Next Review**	**Comments**
Application Servers				
Database Servers				
Department Servers				
Web Servers				
LOCAL AREA NETWORK				
Component	**Current Standard**	**Emerging Standard**	**Next Review**	**Comments**
Protocols				
Performance				
Network Hardware Components				
Network Operating System				
WIDE AREA NETWORK				
Component	**Current Standard**	**Emerging Standard**	**Next Review**	**Comments**
Protocol				

Performance				
Topology				
NETWORK MANAGEMENT				
Component	**Current Standard**	**Emerging Standard**	**Next Review**	**Comments**
Management Software				
Monitoring Software				
Remote Control Software				
Asset Management				
Backup/Availability				
Software Distribution				
STORAGE				
Component	**Current Standard**	**Emerging Standard**	**Next Review**	**Comments**
Media				
Backup Software				
WIRING				
Component	**Current Standard**	**Emerging Standard**	**Next Review**	**Comments**
Topology				
Media				
SECURITY				

Component	Current Standard	Emerging Standard	Next Review	Comments
Firewalls				
Server Certificates				
Client Certificates				
Virus Detection				
Intrusion Detection				
REMOTE ACCESS AND VIRTUAL PRIVATE NETWORKS				
Component	**Current Standard**	**Emerging Standard**	**Next Review**	**Comments**
Connections				
Remote Access Servers				
INTERNET ACCESS				
Component	**Current Standard**	**Emerging Standard**	**Next Review**	**Comments**
Connections				
Availability of Sites				
Video/Audio Streaming				
MESSAGING AND TELECOMMUNCATIONS				
Component	**Current Standard**	**Emerging Standard**	**Next Review**	**Comments**
Electronic Mail				

Fax				
Telephony System				
Voice Mail				
Instant Messaging				
Directory Services				
Message Broker				
OFFICE AUTOMATION				
Component	**Current Standard**	**Emerging Standard**	**Next Review**	**Comments**
Word Processing				
Spreadsheet				
Presentation				
DOCUMENT COPYING/IMAGING				
Component	**Current Standard**	**Emerging Standard**	**Next Review**	**Comments**
Imaging Scanners				
Photocopiers				
MOBILE/WIRELESS COMPUTING				
Component	**Current Standard**	**Emerging Standard**	**Next Review**	**Comments**
Protocol				
Handheld Operating				

System				
Personal Digital Assistants				
Cellular Phones				
DATA MANAGEMENT				
Component	**Current Standard**	**Emerging Standard**	**Next Review**	**Comments**
Databases				
Query Tools				
VIDEO CONFERENCING				
Component	**Current Standard**	**Emerging Standard**	**Next Review**	**Comments**
High End				
Midrange				
Desktop				
HTML AUTHORING AND WEB PUBLISHING				
Component	**Current Standard**	**Emerging Standard**	**Next Review**	**Comments**
Web Site Content/Design				
Accessibility				
HTML Creation/ Conversion/Editing				

Drawing/Illustration				
APPLICATION DEVELOPMENT METHODOLOGY AND SOFTWARE				
Component	**Current Standard**	**Emerging Standard**	**Next Review**	**Comments**
Design/Analysis/Data Modeling				
Graphical User Interface				
Compilers				
Developer Support Tools				
PROJECT MANAGEMENT				
Component	**Current Standard**	**Emerging Standard**	**Next Review**	**Comments**
Project Management Software				
GEOGRAPHIC INFORMATION SYSTEMS (GIS)				
Component	**Current Standard**	**Emerging Standard**	**Next Review**	**Comments**
General				
Database				

Desktop/Laptop Minimums for PDA Installation

PalmOS

	PC and PC-Compliant Computers	***Macintosh Computers***	***Other Client OS/Environment (As Applicable)***
Operating System			
CPU			
RAM			
Disk Space			
E-mail Client Version			

Microsoft Windows CE, PocketPC, Windows Mobile

	PC and PC-Compliant Computers	***Macintosh Computers***	***Other Client OS/Environment (As Applicable)***
Operating System			
CPU			
RAM			
Disk Space			
E-mail Client Version			

Other Mobile OS (Please Specify)

	PC and PC-Compliant Computers	***Macintosh Computers***	***Other Client OS/Environment (As Applicable)***
Operating System			
CPU			
RAM			
Disk Space			
E-mail Client Version			

Approved PDA Devices

PDA Devices	***PC and PC-Compliant Computers***	***Macintosh Computers***	***Other Client OS/Environment (As Applicable)***

Note: Fill in device information in the left-hand column. Check off supported platforms in the boxes to the right.