Technology Policies & Procedures Manual

Approved by FBCC Board of Directors September 7, 2013

The PDF version is available at

http://www.fortbertholdcc.edu/pdf/policiesprocedures/Technology_Policies_&_Procedures.pdf

Table of Contents

1 Technology Policies and Strategies

1.1 Policy Framework

This section of the policies of the Fort Berthold Community College, hereafter referred to as FBCC, covers the management of the technology matters of FBCC. The establishment of these policies is the responsibility of the FBCC Board of Directors, hereafter referred to as the Board. The development of these policies is a continuous process, and will require revisions of current policies, or the development of new policies to handle new situations and issues as they arise. The administrators, which represents the best interest of the community and FBCC as a whole, develops these policies in accordance with governmental regulations, and periodically appraises the effects of its policies and makes revisions as necessary. FBCC operates according to these policies established by the Board. The Board further entrusts the FBCC administration to implement them through more specific regulations and procedures. The responsibility to follow these policies is placed on all of the staff employed by FBCC.

1.2 Strategic Planning

The Technology Department shall conduct periodic assessment of services to determine areas of need and provide a planned approach and determination of goals to satisfy those institutional needs.

1.2.1 Purpose

A) Insure the strategy follows the current vision and mission of the institution.
B) Focus on the major challenges for the next five years.
C) Apply resources to implement the plan and strategies for optimizing them.
D) Allocate responsibilities across FBCC to achieve the plan.
E) Guide FBCC in its planning and examine available projected budget to ensure that proposed activities will fall within funding restrictions.

2 Technology Support

2.1 HelpDesk

All Requests for support will be logged, given a priority, and assigned repair time.
Response to help desk calls will be within one working days on the highest priority, two days on normal priority and four days on the lowest priority. This response period does not mean the problems will be solved within this time but that the technician will look at the problem and establish the corrective action. If additional time is required (i.e. ordering of parts), the user will be notified, and a spare piece of equipment will be given if available.

2.1.1 Times of Operation

Monday through Friday 8am – 5pm. Support can be provided during evenings and weekends with advance notice and with approval of the Director of Technology.

2.1.2 Types of Request/Contacting Technology Staff

In an effort to provide the best service possible to FBCC, the Technology Office offers various options listed below to secure support for technology issues. The Technology Office also prioritizes work orders to insure more critical issues receive quicker attention.

2.1.2.1 E-mail Submitted Work Order

At this point in time the preferred method of submitting a request for support is through e-mail. Requests should be sent to the Technology Department E-mail

List. The subject line should have the word Work Order typed. In the body of the e-mail include the nature of the problem.

2.1.2.2 Walk-in

Requests for support may be submitted in-person to the Helpdesk staff.

2.1.2.3 Phone

Staff are available for questions regarding application issues or other issues were the users can be guided through the problem. If possible Technology staff may utilize software that allows for viewing of the user's desktop or may require the user to log off of his/her workstation. If the Help Desk technician is unable to correct the problem through phone support, the call will be logged, given a priority, and assigned repair time.

Technology Office Contacts		
HelpDesk	(701) 627-4738 Ext. 224	Log-in problems, e-mail issues, application support, computer maintenance and repair, IVN Meeting and room issues, media cart requests, printing.
Network Engineer	(701) 627-4738 Ext. 284	Network (WAN/LAN/wireless issues, Classroom software systems, & Print Service Issues.
Director of Technology	(701) 627-4738 Ext. 256	Jenzabar EX, Web Site corrections, FBCC Facebook Administration, Marquee, purchasing, IVN Scheduling, myFBCC, Server Issues, Other

2.1.2.4 Web

At this time FBCC doesn't have a web based Help Desk Portal.

2.1.2.5 Intercom

Requesting support through this manner does not guarantee a quick response, as many areas of FBCC do not have phone/intercom service. Users should only utilize this method for *high priority requests* and be supplemented with an e-mail request.

2.1.2.6 Emergency/ Weekends

Emergency support is available after hours and weekends with approval of the Director of Technology.

2.1.2.7 **Work Order Priority**

Each call will be logged based on the following ranking criteria. In the event of a high priority call arrives and conflicts with a low/normal call, the high priority call shall be given first response, even if work has begun on the low priority call. In some instances it may not be possible to resolve a particular problem or return to the way it worked before the problem. If the problem restricts operational performance, a different approach or alternative solution may be recommended. (i.e. send out for third party repair, return to vender or manufacturer). The Director of Technology will set priorities when there are several problems of the same priority based on when the calls were received. The Director will have final authority on what priority calls will have and the order they are processed if questions arise.

2.1.2.7.1 High or Emergency

Campus-wide issues such as; no campus internet, e-mail, web sites. Video-conferencing room support for IVN and CLAN Rooms. The user(s) cannot work due to computer/network problems. The workstation(s) or a key program(s) is completely unusable and the workstation is required to do normal work.

Or

A class that is planning on using technology where no other equipment can be used. (ie. computer/video projector)

Or

A problem was previously logged and has not been resolved after a reasonable amount of time (generally three days)

2.1.2.7.2 Normal

The computer is functioning but an application/file/peripheral is not. The problem is significant but not severe enough to prevent fulfillment of normal duties or duties that cannot be carried out through other means. Examples could include a corrupted Office file, email errors, an error message that can be bypassed, a computer move/install, slow network/application service, a broken CD drive. All A/V repairs will be assigned a normal priority

2.1.2.7.3 Low

The computer is functioning normally except a minor irritant such as a broken Windows key on the keyboard, screen is faded, missing icon, voice mail, inter-office computer moves.

2.1.2.8 **Non-FBCC Computers**

Service to non-FBCC computers is provided only on a time available basis.

- ▪ The client acknowledges that he/she has backed up any and all data before relinquishing the computer to the HelpDesk staff.
- ▪ The client assumes all risk of loss from any and all causes or in any way related to or resulting from the repair or service by FBCC HelpDesk staff.
- ▪ The client must provide any relevant and official recovery or operating system discs for reinstallation. This also includes any third-party software such as anti-virus.
- ▪ The client shall be responsible for any parts or software needed.

2.1.3 **Unsupported Services & Equipment**

The Help Desk will provide "best effort" assistance for unsupported applications and products. If the Help Desk is unfamiliar with an unsupported application or product, assistance will be provided if possible. In cases where extensive research needs to be taken before assistance can take place, no support may be provided or require the approval of the Director of Technology. Hardware and software purchased without Director of Technology approval be will categorized as '*Unsupported*'.

2.2 New Staff & Faculty

2.2.1 **Orientation**

All new staff & Faculty will be given a short introduction into the various systems such as;

- Using their Network username and password to log into their workstation.
- Microsoft Outlook and Web Mail.
- Printing.
- Accessing the College Web Sites.
- For Faculty: Logging onto Jenzabar JICS (myFBCC) and accessing the attendance function in e-Racer.

2.2.2 **E-mail/Network Account Application**

All new staff must read and complete the E-mail/Network Account application. Included on the back of this application is the "*Acceptable Use Policy of Information Technology Resources*" . All applicants must also confirm that they have read and agree by signing and dating the document. This application is available online at http://www.fortbertholdcc.edu/pdf/E-mail_Network_Account_Application.pdf.

A) Supervisors will submit a Technology Department Work Order for their new staff requesting a new FBCC Network Account. Information to included in the work order;

a. Legal Name of Employee

b. Title
c. Office Assigned
d. E-mail Distribution List membership.

B) New Users will be added to the appropriate Active Directory User /Security Groups.

C) New Users shall be added to the All Staff & Faculty, All Faculty, or All Students E-mail Lists (Exchange Distribution Lists) as applies.

D) Supervisors shall request additional membership in Committee and other Security or e-mail Mailing List Groups.

E) The new employee will be notified upon completion of account set-up.

F) Account should be set-up by the end of the new employees' first day of work.

2.2.3 Computer and Software Needs

FBCC Departments / Programs hiring staff into newly created positions are responsible for purchasing new workstations and software. Departments requiring additional software should explore available grant funding before purchasing through general fund budgets. The Technology Department can (if available) set-up a temporary workstation upon request from the department administrator.

2.2.3.1 Jenzabar EX Software and Accounts

Only positions requiring Jenzabar EX software shall have this software installed to their workstation. Staff that require this software for their position shall receive:

- Jenzabar Database/SQL Account.
- Given membership in the Active Directory Security Group: Jenzabar Module Manager or Users.
- ODBC Connections.
- Jenzabar EX Software Installation
- InfoMaker Software Installation.
- Jenzabar EX Tasklist Group membership and Permissions based on position and duties.

2.2.3.2 Dynamics Great Plains and Accounts

Microsoft Dynamics GP (formerly Microsoft Business Solutions–Great Plains) is a business management solution that streamlines and automates financial, manufacturing, and supply chain management.

- Employees requiring Great Plains software must contact the Business Manager for installation, configuration and training.

- Technology Staff will add the new user to the Great Plains Active Directory User Group.
- The Technology Department does not provide support for the Dynamics GP system.

2.2.3.3 PowerFAIDS, EDExpress, and EDConnect

Installation of these financial aid software products requires approval of the Director of Financial Aid or the President. The services/information that these products access is highly confidential and require secure and restricted access.

- The Technology office will add new users to the appropriate network security groups for these software products to operate securely on the FBCC network.
- Only staff designated as the Department of Education "Point of Contact" for these software products have clearance to set-up internal users and other configuration settings.

2.2.4 Existing Positions

Newly hired personnel into existing positions shall receive the same workstation as the employee leaving that position unless the supervisor indicates otherwise.

2.2.4.1 Transfers

Employees that transfer from one department of another shall receive a workstation from the Department that the employee is moving into. If the employee is moving within the Department, it is at the discretion of the supervisor whether the workstation follows the employee.

2.2.4.2 New Positions

Employees hired into newly created positions shall receive a temporary workstation or laptop (if available) to utilize until the Supervisor can purchase the employee a new workstation.

2.2.5 Telephone & the Telephone Directory

All new hire and transfer requests for office phone installation, Voice Mail changes, and Telephone problems should be directed to the FBCC Receptionist, who will in-turn will submit a work order to Reservation Telephone. All new hires or transfers shall be added to the Telephone Directory after the supervisor makes a request to the Technology Director by e-mail.

2.3 Laptop Computer Check-out

All Laptops purchased by the Fort Berthold Community College will be checked –out through the FBCC Technology Department to insure proper tracking and maintenance of college laptop computers. Each Department is responsible for purchasing Laptops, software, and accessories. Only current staff, full-time faculty, and program supported students are allowed to check out FBCC laptops. Laptop units MUST remain under the control of the user at all times. Users must never leave a laptop unattended; borrowers are financially responsible for the return of the unit.

2.3.1 Staff / Faculty

- The computer will be shown to the Faculty or Staff to be in good working order upon check-out.
- The computer will be booted up and checked upon return. When returning a laptop, the Faculty or Staff must allow adequate time for that check to take place.
- Adjunct faculty may check-out laptop computers with authorization from the Academic Dean or Vice President of Academics. Adjunct Faculty shall return the laptop at the end of the semester, unless a specific returned date is specified by the Academics Dean or Vice President of Academics.
- The Faculty or Staff checking out a laptop is expected to read and abide by the Faculty/Staff Laptop Checkout Policy, the Computer and Network Usage Policy, and all other Fort Berthold Community College policies and guidelines regarding access and rights to information and use of FBCC resources.
- All Staff laptops will be returned to the Technology Department during the month of June for inventory and any needed maintenance.
- The Faculty or Staff should report any problems encountered with the computer to the Technology Department Help Desk at (701) 627-4738 ext.224, Monday - Friday 8:00am to 5:00pm.

2.3.2 Students

- At this time only students enrolled in academic programs that provide laptop support may check-out FBCC laptops with approval of the program head.
- Under special circumstances exceptions can be made for students needing a computer laptop for the weekend with an authorization from the students’ advisor. Check period shall be no longer than 5 days.

- Students will be required to complete and sign a Student Laptop Check-out Agreement and adhere to all FBCC Policies and Procedures pertaining to Computer Use.
- Students will return the laptop computer on or before the agreed upon return date.
- The student will return the computer laptop in person and be prepared to wait for the Technology staff time to insure the computer laptop is returned in the same operating condition as when the equipment was originally checked-out.
- If the computer laptop is not returned in the same condition as when it was checked-out, the student be billed the cost of repair to their FBCC Student Account.
- If the laptop is not returned by the return date, then the student will be charged $30.00 each business day until the replacement cost of the computer laptop is reached. At that time a replacement cost $1500 will be bill to the students' FBCC account.

2.4 Damage, Repairs, Loss

- Keep the laptop away from water, humidity, extreme temperatures and beverages.
- Do not drop the laptop. Maintain control of the laptop in whatever position that you work.
- Return the laptop to the Technology Department in the same condition it was received, except for ordinary wear. If an accident occurs, do not attempt to fix the laptop. Instead, bring back the damaged laptop for Technology staff to evaluate or repair.
- Do not tamper with or alter the computer or permit any repair to the computer or the replacement of any part in the computer without prior express, written consent of the Technology staff.
- The Borrower will pay for all unauthorized repairs and replacement parts, as well as the cost of restoring any unauthorized alterations.
- In case of accidental damage or non-crime related loss, the Borrower shall promptly notify the library, and if in possession of the laptop, return it to the library for repairs. A Borrower must cooperate fully with Technology Department staff in documenting what led to the damage or loss of the laptop.
- In case of significant damage due to crime or theft of the computer, the Borrower shall promptly complete incident reports with the police and deliver a copy of all related documents to the Technology Department. A Borrower must fully cooperate with the investigation of any vandalism, theft, claim, or lawsuit involving use of the computer while it is checked out in his or her name.

2.5 Staff Leaving Employment

2.5.1 Return of Equipment

All Staff and Faculty leaving employment at the College must return all equipment such as Laptops (power cords/laptop bags), cameras, or other media equipment. Equipment must all be returned before an Exit Interview will be authorized by the Director of Technology. Equipment should be in the condition as when it was checked out.

2.5.2 Network Accounts

A) Mailing List (Distribution/Security) memberships are removed upon termination of Employment.

B) E-Mail accounts are disabled for a period of 30 days and then deleted. If Supervisors need to view e-mail of the past employee, they will have the 30 day period to do so.

C) Computer documents from their documents folder, desktop, and Internet links that are pertinent to the staff or faculty members' position will be backed up to a network folder to await transfer to new personnel or review by the supervisor.

D) Documents that need to be shared through the Department should be relocated to the Departments SharePoint intranet site.

2.5.3 Other Accounts & Password

Out-going staff and faculty are required to relinquish any work related external account information to their supervisor that would make for a smooth transition to the new employee. This should include links, and passwords. If possible the supervisor should take ownership or update Point of Contact information before the employee completes their Exit Interview. It is highly recommended that Supervisors take ownership of external accounts by changing the Point Of Contact in the interim.

2.6 Technical Assistance

2.6.1 Training

The Technology Department staff are available for staff, faculty or student training dependent on available time and schedule of the Technology staff. Any requests for Training should be submitted to the Director of Technology.

2.6.2 Purchasing and Planning

The Director of Technology shall evaluate technology purchases to ensure up-grade ability, compatibility, and integration with current and future programs (hardware, software, and networking).

3 Network Account Usage

3.1 Authorized Use

FBCC provides Network access only to authorized users for the purposes directly related to your employment or study at FBCC. For more information se the FBCC "Acceptable Use Policy" at http://www.fortbertholdcc.edu/Departments/Acceptable_Us_Policy.htm. Use for any other purposes may lead to suspension or withdrawal of access, or in the more serious case to action under FBCC disciplinary procedures. Please keep your passwords secret. If your password has been compromised, change the password or notify the Technology Office immediately.

3.2 Local Area Network Administrator Roles

3.2.1 Domain Administrators

A person who is a member of the Domain Administrator group can create, delete, and manage all objects that reside within the network domain in which they are administrators. They can also assign and reset passwords and delegate administrative authority for network resources to other trusted users. Only members of the Technology Department may be members of this group.

3.2.2 Local Administrators

On Windows-based computers, a user account that is a member of the computers' local Administrators group or a member of a group that is a member of the local Administrators group, such as the Domain Administrator group in a Windows domain. This is the first account that is created when you install an operating system on a new workstation, stand-alone server, or member server. By default, this account has the highest level of administrative access to the local computer. In special instances Staff and faculty may be granted membership in this group. Requests for addition to the Local Administrator Group must be made to the Director of Technology. Membership to this Group can be revoked if the privilege is abused or the user violates the FBCC "*Acceptable Use Policy of Information Technology Resources*" Policy.

3.3 Username Convention

The standard FBCC username convention for staff and faculty to access FBCC network resources comprises the first initial of the first name, followed by the first five letters of their last name. If a username is already in use, the first two letters of the first name will be used and the first four letters of the last name. If the username should be cause for ridicule or communicate some other meaning, an alternate username is acceptable.

3.4 Passwords

Passwords will not be re-set over the phone. Supervisors can request subordinate staff members password reset to allow temporary access. Passwords cannot be blank or the word “password” and should follow the rules for creating a strong password: An ideal password is long and has letters, punctuation, symbols, and numbers.

A) Whenever possible, use at least 14 characters or more.

B) The greater the variety of characters in your password, the better.

C) Use the entire keyboard, not just the letters and characters you use or see most often.

To check the strength of your password go to:

https://www.microsoft.com/protect/fraud/passwords/checker.aspx?WT.mc_id=Site_Link

3.5 E-mail

All full-time students, staff, and faculty are provided with an FBCC e-mail account. Staff and faculty utilize Microsoft Outlook e-mail client software, which is installed on their workstation and can also access their e-mail through the internet. Students utilize Microsoft Office Outlook Web Access or WebMail for their e-mail access through the internet. FBCC e-mail is the official means of contact for FBCC staff students. All official FBCC e-mail correspondence will be delivered to these addresses.

3.5.1 Purpose of the Policy

In order to satisfy the need for timely and efficient communication, and to provide a better service to its students, FBCC has instituted a policy that establishes e-mail as an official means of communicating with students. This is motivated by the convenience, speed, cost-effectiveness, and environmental advantages of using e-mail rather than printed communication.

3.5.2 Scope

This e-mail policy provides guidelines regarding the following aspects of e-mail as an official means of communication:

- Use of e-mail;
- Assignment of e-mail addresses;
- Redirection of e-mail;
- Expectations regarding student use of e-mail;
- Educational uses of e-mail;
- Appropriate use of e-mail;

- Account Limitations and Data Backup;
- Account Expiration/Termination;

3.5.3 Use of e-mail

The use of the FBCC e-mail system is a privilege, not a right. Users are expected to honor this policy and comply with the rules of usage and etiquette. Students are expected to check their email on a frequent and consistent basis in order to stay current with FBCC-related communications.

3.5.4 Assignment of e-mail addresses.

All students will be provided with an official FBCC e-mail account as part of the Registration process. It is to this official address that FBCC will send e-mail communications.

3.5.5 Redirection of e-mail

In special circumstances any Staff, Faculty, or Student may have e-mail electronically redirected to another e-mail address. If the user wishes to have e-mail redirected from his or her official FBCC account to another e-mail account (e.g., @aol.com, @hotmail.com), they may do so, but at his or her own risk. The FBCC account remains their official e-mail address and a copy is forwarded to their Second account.

1. FBCC will not be responsible for the handling of e-mail by outside e-mail servers.
2. The users must make the request in person and show proof of identity and additional e-mail account access.
3. Email lost as a result of redirection *does not* absolve the user from responsibilities associated with communication sent to his/her official FBCC email address.

3.5.6 College Expectations Regarding Student Use of e-mail.

Students are expected to check their official e-mail address on a frequent and consistent basis in order to stay current with FBCC communications. Checking e-mail on a daily basis is recommended, in recognition that certain communications may be time-critical.

3.5.7 Educational uses of e-mail

Faculty determine how e-mail will be used in their classes, but it is highly recommended that faculty include their e-mail requirements and expectations in their course syllabi. Faculty may also expect that students' official FBCC e-mail accounts are being accessed with regularity.

3.5.8 Appropriate use of e-mail

Use of the FBCC e-mail system allows the users to conduct collaborative work efforts and share information with students, professors, and other individuals regardless of time and/or geographic boundaries. Because of this open freedom, and the possibility of conversing with individuals with whom you may have never met, users should conduct themselves in an appropriate manner during their communications. Every e-mail message sent from your FBCC account carries FBCC's name, and all communications should reflect that.

- In general, e-mail is not appropriate for transmitting sensitive or confidential information unless its use for such purposes is matched by an appropriate level of security.
- Design Guidelines:
  1. Keep bulk mail short and without attachments.
  2. Always use a clear, specific and non-empty subject line.
  3. Do not attach personal, confidential, or sensitive information.

- Confidentiality regarding student records is protected under the Family Educational Rights and Privacy Act of 1974 (FERPA). All use of e-mail, including use for sensitive or confidential information, will be consistent with FERPA.
- E-mail shall not be the sole method for notification of any legal action.
- FBCC maintains the right to access user email accounts in the pursuit of an appropriately authorized investigation, but will not normally be monitored by staff unless there is a suspicion of improper use.

3.5.9 Inappropriate Use

- It is unacceptable to send or receive any material that is obscene or defamatory or which is intended to annoy, harass or intimidate another person.
- Use of electronic mail systems for any purpose restricted or prohibited by copyright laws or regulations.
- Attempting unauthorized access to electronic mail or attempting to breach any security measures on any electronic mail system, or attempting to intercept any electronic mail transmissions without proper authorization.
- The college e-mail service is not provided for private or personal use. Incidental personal uses of the e-mail system are permitted as long as they do not violate the law, restrictions that derive from the college's tax-exempt status, or FBCC Policies. The FBCC e-mail services may not be used for commercial or profit-making purposes unrelated to College business.

3.5.10 E-mail Account Limitations (Quotas) and Backup

Due to finite resources, FBCC reserves the right to restrict the amount of user storage space on the email server as necessary. The FBCC E-mail system is a communication system and is not a storage or archival system. Messages in the system are of a temporary nature and FBCC does not perform any archival of these messages. It is the user responsibility to archive any messages that he/she wishes to permanently maintain by printing, exporting or archiving to a portable storage.

3.5.10.1 E-mail Quotas

To provide a fair e-mail service to all users, there is a quota applied to the amount of e-mail each user can store on the server. Users will receive a warning when they are approaching their quota usage, and will see a message indicating how much e-mail they have stored when using the Web-based e-mail system. When the user exceeds their storage quota they will no longer be able to receive any new e-mail. To prevent this from happening users are encouraged to delete e-mail messages they no longer need, and to download old messages to their local computer and delete them from the server. For additional information on this topic see the Technology Department staff.

These limits are:

- For Staff & Faculty: 500 megabytes.
- For Students: 50 megabytes.

3.5.11 Account Expiration/Termination

Network accounts and email are deleted on a periodic basis to conserve storage space on FBCC e-mail servers. Student e-mail accounts are deleted when a student does not register for the subsequent semester. Students enrolled in Spring semester will not have their e-mail accounts reviewed for termination until the last day for registration in the following Fall semester. All e-mail accounts of staff & faculty that leave employment at FBCC are disabled upon completion of their Exit Interview and removed from any security group memberships for a thirty-day period before deletion. It is the responsibility of the staff or faculty supervisor to notify the Technology Department of an employees' departure from employment.

3.5.12 Web Based E-Mail

FBCC utilizes Microsoft Office Outlook Web Access system to provide e-mail access via the internet. Clients can utilize a web browser to access their Microsoft Exchange mailbox from any computer with an Internet connection. This software is sometimes referred to as WebMail or OWA. WebMail is accessible by all students, staff, and faculty and contains most of the same features as Microsoft Outlook. The FBCC WebMail may be accessed at: http://mail.fortbertholdcc.edu/owa/

3.5.13 E-mail Lists

Most e-mail are addressed to an individual or a small list of addresses. At times, it's more effective to use a pre-arranged mailing list, particularly if you often need to send a message to the same group of people. For some purposes, personal mail-lists are appropriate. These are set-up on the workstation, using features built into Microsoft Outlook. These personal lists are quick and easy to set up, but they can only be used by the individual who set them up. An alternative, preferable for large, shared lists, is the server based list. These server based lists have the advantage over the personal lists in that they are shared with all the e-mail users whether on the Outlook Client or the WebMail version.

3.5.14 Disclaimer

FBCC assumes no liability for direct and/or indirect damages arising from the user's utilization of the FBCC e-mail system and services. Users are solely responsible for the content they disseminate. FBCC is not responsible for any third-party claim, demand, or damage arising out of use of the FBCC e-mail systems or services. By accessing and using the FBCC student e-mail system, you agree to abide by the above policies of FBCC.

4 Networks and Communications

4.1 New Installations

The installation of network cabling for new or redeveloped buildings and rooms is the responsibility of the Project Coordinator for development. Funding for all new network infrastructure, for example, connectors, routers and cables should be billed into the project. The Director of Technology shall be consulted on all new network installations. Upon completion all new cooper and fiber connections the work shall be performance verified using an automated test set.

4.1.1 Wiring Standards

The Technology Department sets minimum cabling standards for all network installation at FBCC. All new installations, upgrades or redevelopments must conform to these standards.

4.1.1.1 **CAT-6 Cooper Cabling**

The Category 6 portion of the cabling system shall comply with the proposed link and channel performance requirements of the latest revision of TIA/EIA 568-B.2-1 “Performance Specifications for 4-pair 100 Ohm Category 6 Cabling”, NEC, NRTL listing, and manufacturer's recommendations and instructions. Cable length will not to exceed 295 feet.

General Cable, Superior Essex, or Belden meeting the following characteristics at 250 MHz.

- ACR: 14.4 dB min. @ 100m
- PSACR: 12.4 dB min. @ 100m
- PSNEXT 43.3 dB min.
- ACRF 23.8 dB min.
- NEXT: 45 dB min.
- PSACRF 23.8 dB min.
- INSERTION LOSS 30.9 max.
- LCL 26 dB min.
- Return Loss 19 dB min.
- ELTCTL 5 dB min.

4.1.2 **Work Area Communication Outlets**

Each work area must have at least one communications outlet. Each communications outlet should be sized to accommodate three Category 6 cables and connectors. Communications outlets should be within 3 feet of an electrical outlet and installed at the same height, unless otherwise specified. Communications outlets should be placed so that the work area or workstation cable does not exceed 5 meters (16 ft) in length. This length is figured into the total horizontal cabling length and must not be exceeded.

4.1.3 **Cabling System Labeling**

At a minimum, the labeling system shall clearly identify the following components of the system: racks, patch panels and outlets. Racks and patch panels shall be labeled to identify the location within the cabling system infrastructure. All labeling information shall be recorded on the as-built drawings and all test documents shall reflect the appropriate labeling scheme. All label printing will be machine generated using indelible ink ribbons or cartridges. Self-laminating labels will be used on cable jackets, appropriately sized to the OD of the cable, and placed within view at the termination point on each end.

4.1.4 Cabling Pathways

Pathways will be constructed from J-hooks or other suitable communications cable trays or raceway. Open cable tray is the preferred method of installation. Cable pathways shall be so designed to avoid EMF and RFI interference. Common causes of this interference are fluorescent lighting fixtures, air handling motors and many kinds of electrical controls including starters, lighting contactors, and power distribution panels. Never run parallel with electrical conduits or strap to them. Every cable, whether an individual or many grouped together, shall be supported. Wherever possible, cable shall be grouped together in pathways. Plastic cable ties should not be used; they deform the outer cable jacket causing cable performance problems in the future (use of Velcro straps is recommended for cable management. Route open air cables (where not in raceway or cable tray) parallel or perpendicular to building construction supporting with specified products, maximum 4'-0" on center. Bending radius shall be minimum 1 inch. All cable runs shall be continuous, with no splicing.

4.1.5 Testing Requirements

All terminated voice and data cables shall be tested and certified for TIA/EIA-568-B.2-1 Category 6 standards. The test shall be performed on the permanent link configuration (from station jack to patch panel jack). These standards require the following when tested at 250 MHz:

- Near End Cross Talk (NEXT) shall be no less than 35.3dB.
- Power Sum Near End Cross Talk (PSNEXT) shall be no less than 32.7dB.
- Equal Level Far End Cross Talk (ELFEXT) shall be no less than 16.2dB.
- Power Sum Equal Level Far End Cross Talk (PSELFEXT) shall be no less than 13.2 dB.
- Return Loss shall be no less than 10.0dB.
- 6. Propagation Delay shall be less than 498 nanoseconds when measured at 10 MHz.
- 7. Propagation Delay Skew shall be less than 44 nanoseconds when measured at 10 MHz.
- 8. Insertion Loss (Attenuation) shall not exceed 31.1dB.

Additional testing shall include line mapping and cable length before final acceptance by Owner. All permanent link cable runs shall be documented with a hard copy print-out of the test results. Compile one copy of test results in a loose-leaf binder, similar to manual references in Section 16010, 1.04E. Submit at project completion with referenced Record Manual. Field tester to be Level III and conform to TIA/EIA 568-B.2-1 Annex A & B requirements.

4.1.5.1 Fiber-optic cabling

All Fiber-optic cabling shall be 6 strand multi-mode fiber from MDF to all IDF locations. Only .50/125um multi-mode fiber with LC or SC ends shall be utilized. All fiber to meet OM3 10Gig specs.

4.1.6 As-Built Drawings

The installation contractor will be provided with drawings at the start of the project. Anticipated variations from the build-to drawings may be for such things as cable routing and actual outlet placement. The drawings must clearly define all cabling pathways (cable tray, conduits, slots or sleeves) and spaces (Telecommunications rooms). They must also clearly show the location of each communications outlet, the number of cables per communications outlet, and which TR the cables for each communications outlet terminate in. The Contractor shall provide a drawing to the FBCC on the conclusion of the project. The marked up drawing will accurately depict the as-built status of the system including termination locations, cable routing, and all administration labeling for the cabling system. In addition, a narrative will be provided that describes any areas of difficulty encountered during the installation that could potentially cause problems to the telecommunications system.

4.2 Network Management

Network management refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems. The Technology 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. The Technology 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.

4.3 Network Security

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator.

4.3.1 Firewalls

The purpose of this document is to establish an understanding of the function that a firewall plays in the overall security of FBCC’s network. All connections to the FBCC network must pass through a network firewall. Network firewall configuration rules and permissible services rules must not be changed unless permission is obtained from the Director of Technology.

Given the nature of FBCC's academic environment, the campus firewall cannot be configured to typical industry accepted standards. FBCC does not constrict all unnecessary traffic; it is open to all traffic and denies access as needed. Due to individual security needs, depending on the type of information to be protected, the following information should be used to maximize the security of the network environment.

The Network Time Protocol (NTP) or another appropriate mechanism is used to synchronize the logs with other logging systems such as intrusion detection. In addition to examining logs, the Executive Director of Communications and Networking periodically reviews the configuration of the firewall to confirm that any changes made are legitimate.

4.3.2 Routing and Sub netting

4.3.2.1 Reserved IP Address Ranges

Some infrastructure situations have to use static addressing, such as when finding the Domain Name System (DNS) host that will translate domain names to IP addresses. Static addresses are also convenient, but not absolutely necessary, to locate servers inside an enterprise. An address obtained from a DNS server comes with a time to live, or caching time, after which it should be looked up to confirm that it has not changed. Even static IP addresses do change as a result of network administration

- Servers - 10.1.0.1-10.1.0.50
- Printers – 10.1.1.0-10.1.1.50
- Wireless Access Points – See IT Director

4.4 Network Remote Access

Remote access is a privilege granted to certain individuals who have a demonstrated need to perform mission-specific activities using enterprise resources while situated off campus. It may not be possible for everyone to receive the privilege of remote access. These standards are designed to minimize the potential exposure to FBCC from damages which may result from unauthorized use of FBCC resources. Damages include the loss of sensitive or confidential data, intellectual property, damage to public image, damage to critical internal systems, etc. A person's request for remote access to information systems that contain sensitive data must be documented in writing and authorized by his or her supervisor.

- Remote access must be strictly controlled through the same on-campus authentication and authorization measures. Logon information may not be shared with others. Unauthorized people (including family and friends) are not allowed to use FBCC resources.
- Workstations owned by staff & faculty members, contractors or other affiliates of FBCC must have anti-virus/anti-spyware software installed with the latest virus definitions.

- Data transmitted between remotely situated workstations and the network must be encrypted (128-bit minimum length). Acceptable mechanisms of encryption include either institutionally approved VPN or browser-based SSL connections.
- Points for remote access entry into FBCC networks must be configured to drop inactive connections after 30 minutes whenever possible. Using contrivances to circumvent this requirement is prohibited.
- Third-party products or services (e.g., PCAnywhere, VNC, GoToMyPC, etc.) that establish remote access or that bypass institutionally approved VPN or browser-based SSL connections may not be used unless explicitly approved by the Director of Technology. Third-party product access will be controlled by blocking known ports at local firewalls.
- PC modems or PC fax connections to telephone equipment are not permitted without the explicit knowledge and approval of the Director of Technology.

4.5 Wireless Access

The purpose of this policy is to define standards, procedures, and restrictions for connecting FBCC internal network(s) or related technology resources via any means involving wireless technology.

- 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 FBCC facilities will be managed at the sole discretion of the Technology Department. 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.

- The Technology Department reserves the right to turn off without notice any access port to the network that puts FBCC systems, data, users, and clients at risk.
- The wireless access user also agrees to and accepts that his or her access and/or connection to FBCC 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.
- Failure to comply with the above Wireless Access Policies may result in the suspension of remote access privileges, disciplinary action, and possibly termination of employment.

4.6 Telephone

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

4.6.1 New Phone Lines or Staff Moving to Different Rooms

Anytime a department needs an additional phone or moving a phone to another room the supervisor should contact the FBCC receptionist at extension 272. The Receptionist will contact Reservation Telephone to summit a work order and arrange for their Support Technicians to perform the change. Reservation Telephone service times vary from one day to a week. Supervisors hiring new staff should contact the Receptionist as soon as possible to insure the new employee has a phone and voice mail. The Receptionist or Reservation Telephone Support Technicians will provide a short orientation to the phone, voice mail, and other features other phone

4.6.2 Fax Lines or Dedicated Phones Lines

All Requests for additional fax lines or dedicated phone lines are submitted to the Administrative Committee for approval. Reservation Telephone service times vary from one day to a week.

4.6.3 Problems

Any problems with phones or phone service are submitted to the receptionist at extension 272.

5 Appropriate Use and Information Security / Confidentiality

5.1 Purpose

To provide FBCC faculty, staff, and students with accessible and professional computing facilities and establish appropriate terms, conditions, and restrictions on the use of said facilities. This appropriate use policy covers all computing assets of FBCC. “Computing assets” includes but is not limited to all networks, desktop computers, servers, printers, e-mail services, web services, and any computer access. By using any FBCC computing asset, the user agrees to all the following policies outlined in the policy.

5.2 Policy

5.2.1 Information Use

- Follow standard security practices such as maintaining password secrecy and logging out of accounts when not in use;
- Use it only as required in the performance of their jobs;
- Use it only as required in the performance of their jobs;
- Disclose confidential information to other staff on a need-to-know basis; and
- Exercise due and diligent care to protect data and information from unauthorized access, use, disclosure, alteration, or destruction.

5.2.2 Educational Rights and Privacy Act (FERPA)

Users are responsible for complying with all applicable laws and regulations regarding the dissemination and protection of data and information that is confidential, particularly with regards to the Family Educational Rights and Privacy Act (FERPA) – also known as the Buckley Amendment, the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLB), and any other applicable state and federal legislation dealing with information privacy.

5.2.2.1 FBCC Database Access

Under no circumstances shall student, alumni, or employee data designated as confidential be extracted and/or stored on computer systems external to FBCC enterprise databases maintained by the Director of Technology without express written permission from the FBCC Registrar and Director of Technology. Confidential data elements covered by this policy include:

- Social Security Numbers
- Birthdates
- Driver’s License Numbers
- Credit Card Numbers
- Bank Account Numbers or Routing Information

5.2.2.2 Printing Reports from FBCC Database Systems

Printed reports containing one or more of the data elements listed above may only by created and printed by the office responsible for the data (Registrar for student data, Human Resources for employee data, and so on. The reports shall be used in a “need to know” manner and shall be kept in a confidential environment. Paper reports containing Social Security Number(s) or other confidential information may not be thrown in the trash, but should be shredded (not by hand) or returned to the originating office for proper disposal.

5.2.2.3 Departmental Databases and Reports

Faculty or staff maintaining databases and/or copies or printed reports containing Social Security Number(s) or other confidential information are personally responsible for abiding by FERPA, HIPAA, and other state and federal regulations.

5.2.2.4 Backup Policy

5.2.2.4.1 Purpose

The purpose of this policy is to establish rules for the backup of college computer systems and storage of backup media.

5.2.2.4.2 Scope

This policy applies to all computer systems that are supported and directly controlled by the FBCC Technology Department.

5.2.2.4.3 Desktop and Laptop Backup Policy

Local documents stored on desktop and laptop computers should be backed up so the documents and files can be restored in the event of a physical problem with the machine or if individual files or folders are inadvertently removed. FBCC faculty and staff have access to a networked drive located on the fortbertholdcc.edu campus domain.

5.2.2.4.4 Server Backup Policy

Backup procedures and policies are developed for two purposes, disaster recovery and file recovery. In the event of a catastrophe, due to a physical disaster, personnel error, or other misfortune, reliable backups must provide timely and accurate restoration of all functions of the organization. Individual file recovery may be required to restore programs, information or other data that has become corrupted or inadvertently removed.

5.2.2.4.5 Guidelines

- FBCC utilizes a tape library backup system in conjunction with Symantec Backup Exec software to backup server system states and server data.
- The system backups will consist of regular and cumulative incremental backups.
- The Technology Department performs nightly (Monday through Thursday) incremental backups of all servers.

- A full systems backup will be performed weekly.
- Tape backups are kept for a two week period then overwritten daily for the new week.
- Weekly backups of critical SQL data backups are saved to an external storage device and kept off campus.
- Periodic tests of the backups should be performed to determine if files can be restored.
- Offsite online backups will also be utilized for all mission critical data.

5.2.2.4.6 Responsibilities

- The Director of Technology is primarily responsible for insuring proper backups are being made, proper records are kept, and regular testing of restores are made. The Network Engineer is responsible for periodically verifying backups and records, and also assists the Director of Technology in configuring backups and record keeping. Only the Director of Technology and Network Engineer has the ability to modify the backup schedule for all backups. In the absence of the Director of Technology, it is the responsibility of the Network Engineer to verify a successful backup. In situations where a server/software system is managed by a third party vender, the Technology cannot effectively guarantee data backup unless the Technology Department is notified of changes to the file structure or new software installations.

6 Campus Information Systems

6.1 Jenzabar

Jenzabar® EX is a comprehensive, fully-scalable campus information system or administrative platform designed specifically for use in Higher Education. In 2007, the President, Administrative Committee, and the Board of Directors approved the transition and implementation of the Jenzabar Campus Information System. FBCC joined a consortium of North Dakota Tribal College Jenzabar users to receive a group discount. Jenzabar EX is based on the industry-leading Microsoft® SQL Server database software, is a proven system and the fastest-growing SQL solution in the marketplace today.

6.1.1 Jenzabar EX

Jenzabar EX allows your administrative and academic staff to access, update, store, and report on crucial data through a common database and a complete suite of end-to-end, fully integrated modules. Authorized users share real-time information across departments, streamlining workflow and optimizing business processes. FBCC has The following Jenzabar EX modules:

Student Information Modules

- Admissions
- Financial Aid
- Registration
- Student Life
- Advising
- Alumni Development

Business Operations

- General Ledger
- Accounts Receivable
- Accounts Payable
- Purchasing
- Budget
- Human Recourses
- Payroll & Personnel
- Fixed Assets

6.1.2 Jenzabar Internet Campus Solution (JICS)

Jenzabar's Internet Campus Solution (JICS) helps you connect with all your constituents, from applicants to alumni, and keep them engaged and involved in the life of your school. It's a powerful resource that enables you to offer everyone on campus a single point of access to Web-based self-service, e-learning, communications, and community-building applications. With one login and password, your constituents have 24x7 access to role-specific content, from administrative records and reports to personal email and calendars, from chat rooms to online exams. JICS delivers a flexible, customizable, and extremely scalable infrastructure—the mission-critical elements of a successful portal.

6.1.2.1 Constituent Relationship Modules (CRM)

Jenzabar offers seven CRMs for Candidates, Admissions Officers, Students, Faculty, Staff, Advancement Officers and Alumni. Each of these modules allows institutions to provide content specific to each constituent group along with access to relevant applications and data supported through the institution's administrative system. Together with Jenzabar's ERP systems, the CRMs and Web portal bring a comprehensive, completely integrated community management platform that leverages administrative data for more effective relationship management. FBCC currently utilizes the following CRM's:

- Admissions
- Student
- Faculty
- Staff

6.1.2.2 Learning Management System (LMS)

Referred to as ***myFBCC***, the college utilizes Jenzabar e-Racer as it's web-based learning management system, or LMS. e-Racer is a component of Jenzabar's Internet Campus Solution, which is the product used to generate a web site where members of a school's community — teachers, students, and others — can log in, communicate, and collaborate. e-Racer is a component of JICS that lets you manage the course sections you teach. You can use eRacer to track attendance, create assignments, and much more. A great deal of e-Racer's functionality is accessed through the LMS tab in your myFBCC portal. Available at:

http://myfbcc.fortbertholdcc.edu/ics/

The Technology Department provides a number of online resources to aid Faculty, Staff, and Students in utilization of this system.

- Jenzabar Faculty Guide
- Student Guide
- Online Tutorials
- Distance Education Policies & Procedures

6.1.2.3 Jenzabar System Managers

- System Administrator – Director of Technology
- Human Resources – Human Resource Director
- Advising – Registrar
- Payroll – Chief Financial Officer
- Accounts Payable – Business Manager
- General Ledger – Chief Financial Officer
- Fixed Assets – Chief Financial Officer
- Purchasing – Business Manager
- Accounts Receivable – Business Manager
- PowerFAIDS – Financial Aid Director
- Registration – Registrar
- Admissions – Dean of Students
- Student Life – Dean of Students

- Common – Data Manager
- JICS – Director of Technology
- myFBCC – Director of Technology

6.1.2.4 **Support**

More Information about Customer Support is available at:

http://www.myjenzabar.net/ics/

6.2 Library Solutions

A server based Oracle database driven library automation system that is connected to a web based Library Web Portal that included a Public Access Catalog. The system includes a workstation client for Circulation, Cataloging, **a**nd reporting.

6.2.1 **Support**

The Technology Department provides minimal to medium level support for this product; such as web programming, backup services, and workstation maintenance and updates. The Library Corporation provides the majority of support required through their Helpdesk and remote access portal at: http://www.tlcdelivers.com/helpdesk/default.asp

7 FBCC Web Site

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.

7.1 Disclaimer

All information provided in official FBCC Web sites is provided for information purposes only and does not constitute a legal contract between FBCC and any person or entity unless otherwise specified. Information on official FBCC web sites is subject to change without prior notice. Although every reasonable effort is made to present current and accurate information, FBCC makes no guarantees of any kind. The FBCC web site may contain information that is created and maintained by a variety of sources both internal and external to FBCC. These sites are un-moderated forums containing the personal opinions and other expressions of the persons who post the entries. FBCC does not control, monitor or guarantee the information contained in these sites or information contained in links to other external web sites, and does not endorse any views expressed or products or services offered therein. In no event shall FBCC be responsible or liable, directly or indirectly, for any damage or loss caused or alleged to be caused by or in connection with the use of or reliance on any such content, goods, or services available on or through any such site or resource. Any links to external Web sites and/or non-FBCC information provided on college pages or returned from college Web search engines are provided as a courtesy. They should not be construed as an endorsement by FBCC of the content or views of the linked materials.

7.2 Style Guidelines

The first several levels of the FBCC 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 by the Director of Technology. . All WWW publishing should conform to the HTML standard. The use of proprietary extensions is strongly discouraged. Pages should be accessible and look professional, irrespective o f the browser being used. All pages should be W3C CSS & XHTML 1.1 compliant.

7.3 Content Guideline

The object of these guidelines is to insure that the content of FBCC Web pages accurately represents FBCC. All content must conform to the Acceptable Use Policies of FBCC, language must be suitable to a public forum, content must be appropriately current and accurate, and external links monitored. Content should be non-discriminatory and protect individual privacy.

7.4 Format Guideline

- Spelling and grammar should be correct.
- HTML should meet W3C's Standards.
- Images should load correctly within a reasonable amount of time and include the ALT image tag parameter.
- All pages should utilize the FBCC web page template and be connected to the appropriate CSS style sheets for uniformity.

7.5 Copyright

Copyright infringement is the illegal use of works under copyright, infringing the copyright holder's "exclusive rights", such as the right to reproduce, distribute, display or perform the copyrighted work, spread the information contained within copyrighted works, or to compose derived works. It frequently refers to copying "intellectual property" lacking written agreement from the copyright holder, which is normally a publisher or other business representing or assigned by the work's originator. Placing copyrighted material on the Web site without permission of the author is prohibited. For information about copyright policies relating to staff, see section 2.8 of the FBCC Personnel Policy Manual.

8 Print Services

FBCC provides networked printing locations for workgroup clusters in most departments. 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. The goal of this policy is to facilitate the appropriate and responsible business use of FBCC printer assets, as well as control printer cost of ownership by preventing the waste of paper, toner, ink and so on.

8.1 Scope

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

8.2 Supported Printers

The FBCC Technology Department supports all network printers on FBCC networks. An effort has been made to standardize on specific models in order to minimize support costs.

8.3 Policy

- Installation of personal printers is generally not condoned at FBCC 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.
- 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.
- 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).
- 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).
- Make efforts to limit toner use by selecting light toner and lower dpi default print settings.
- 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).

- 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.
- 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.
- 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.
- Departments are responsible for their own printer supplies such as paper and toner.
- 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.
- If a printer cannot be serviced by the IT staff, IT will recommend to the Department responsible for the printer to contact a service vender.
- Purchase of any new printer equipment requires review and authorization by the Director of Technology.

9 Equipment Acquisition and Disposal

9.1 Replacement Cycle

Most FBCC computer equipment is replaced every three to five years to assure that appropriate computing resources are available in public and departmental computing facilities, classrooms, and FBCC offices to support the mission of the institution; and to 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; and implement minimum standards for computing equipment on campus; and also to encourage planning, cost-effective installation of new equipment and disposal of old equipment. 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.

9.2 Purchasing

To ensure that technology purchases are compatible with existing campus systems, and can be supported by the Technology Department, it is highly recommended that staff consult the Technology Director for all such purchases. Technology Director will make final authorization prior to submission. Failure to comply may result in equipment that cannot be supported by the FBCC Technology Department.

9.3 Recommended Computer Specifications (FBCC Computers)

9.3.1 Desktop Systems

1. Operating System - Windows 7 Professional (Pre-Installed).
2. Operating System - Windows 7 Ultimate.(optional in lieu of above)
3. Minimum Intel Core i5-520M Processor (2.53GHz, 3 MB Cache).
4. 4 Gb Memory (Upgradable to 8Gb).
5. 250 Gb Hard-drive or greater.
6. Graphics Card - any with DVI support
7. DVD-RW
8. Monitor - 19" or larger LCD with DVI support.
9. USB Keyboard/Mouse Kit
10. 3-year Warranty

9.3.2 Laptop Systems

1. Operating System - Windows 7 Professional (Pre-Installed).
2. Operating System - Windows 7 Ultimate.(optional in lieu of above)
3. Minimum Intel Core i5-520M Processor (2.53GHz, 3 MB Cache).
4. 4 Gb Memory (Upgradable to 8Gb).
5. 250 Gb Hard-drive or greater.
6. DVD-RW
7. Wireless 802.11abg
8. 3-year Warranty

9.4 Desktop Software and Licenses

The list of software recommended and supported by the Technology Department is subject to revision as new versions and products become available and as needs of FBCC change. The List below is current at the time of publication but should be used as a guide only; for a more up to date listing please refer to the online version: http://www.fortbertholdcc.edu/Departments/software.htm

- Windows Vista Business
- Windows 7 Professional (Preferred)

- Windows 7 Ultimate
- Adobe Flash (free)
- Adobe Reader (free)
- Adobe Shockwave (free)
- Apple ITunes (free)
- Apple QuickTime Player (free)
- Google Chrome
- Google Earth
- Microsoft FrontPage
- Microsoft Office Professional (License/computer)
- RealPlayer
- Sun Java
- Symantec Endpoint Protection

9.5 Software Licenses

Use of software on computers is protected under United States copyright laws from the time of its creation. The FBCC Technology Department maintains all College software and computer/AV equipment licensing and the "library" of licenses and media on which the software is stored. Unless otherwise provided in the software license, duplication of copyrighted software is a violation of the local, state and federal laws and this policy.

a. Computer software is protected by the copyright laws of the United States. The owner of a copyright holds the exclusive rights to the reproduction and distribution of his or her work. Therefore, it is illegal to duplicate software or its documentation without the express written permission of the copyright holder.

b. It is illegal for a user of the College's computers to make a copy of any software purchased by the College for his or her personal use.

c. All software installed on FBCC computers/equipment will be licensed to the Fort Berthold Community College.

d. The College explicitly prohibits the illegal copying of copyrighted computer software. Violators will be held personally liable.

e. The College assumes no responsibility for software that has not been approved and inventoried.

9.6 Computer Deployment, Inventory and Delivery

All newly purchased computer workstations, laptops and servers shall be transferred to the Technology Department after the item has been logged in the Business Office.

9.6.1 Computer Deployment

The Technology will install all supported software, enter into inventory, and deliver/set-up the computer to the required work area. The Technology Department is not responsible for setting-up cell phones. See Business Office. The Department purchasing the computer workstation is responsible for purchasing all peripheral items such as:

- Computer desks or tables.
- Keyboard/mouse.
- Surge protectors.
- Wireless or video cards.
- Network switches.
- UPS Battery Backup systems.
- Additional RAM or hard-drives.
- Other.

9.6.2 Inventory

All computers, printers, and other devices to connect to the FBCC LAN will be entered into the FBCC Technology Department Inventory System. The following information should accompany any new item to be deployed by the Technology Department:

- Date of Purchase.
- Cost of item.
- Fund Code information.
- Warranty Information.
- Staff, Faculty office, or room to be set-up in.
- Additional software requirements

9.7 Assets Disposal

9.7.1 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. FBCC 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 FBCC upgrade guidelines.

Therefore, all disposal procedures for retired IT assets must adhere to company-approved methods.

9.7.2 Scope

This policy applies to the proper disposal of all non-leased Fort Berthold Community 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.

9.7.3 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.

9.7.4 Guidelines

Disposal and disposal procedures of all IT assets and equipment will be centrally managed and coordinated by FBCC Technology Department. FBCC Technology 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.

9.7.5 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.

9.7.6 **Policy**

It is the responsibility of any employee of the FBCC Technology 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 FBCC 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 FBCC IT Department. Decisions on this matter will be made according to FBCC purchasing/procurement strategies. Equipment lifecycles are to be determined by IT asset management best practices (i.e. total cost of ownership, required upgrades, etc.).

10 Enterprise Server Rooms and Network Closets

10.1 Purpose

The purpose of this policy is to ensure a minimum level of security is maintained by all College staff that has access to the FBCC Server Rooms.

10.2 Scope

This policy applies to all College information technology resources and Personnel who access those resources. It pertains especially to those resources that support critical enterprise systems.

10.3 Policy

It is the policy of FBCC to maintain an IT security program that protects the integrity, confidentiality, and availability of information resources, as well as addresses compliance with all applicable laws and regulations.

10.3.1 Physical Access

The primary mechanism for controlling access to server rooms is a mechanical lock. Only Technology Department staff shall be permitted in the server rooms unescorted. All other visitors shall be escorted by Technology Dept. staff. The Technology Director shall be notified of all server room visitors. FBCC recognizes the responsibility for promoting an open computing environment.

10.3.2 Climate Control

General recommendations suggest that you should not go below 10°C (50°F) or above 28°C (82°F). Although this seems a wide range these are the extremes and it is far more common to keep the ambient temperature around 20-21°C (68-71°F).

- Technology Department staff shall monitor server room temperatures and notify the Maintenance Department if the room temperature rises above 72 degrees.
- If Maintenance Department has exhausted local remedies, and needs to bring in third party support: The Technology Department will take need measures such as powering off non-essential servers and other equipment. Additional fans may be used to circulate air. Critical services include FBCC network domain controllers, primary DNS server, web server, and active director/e-mail services.
- If temperatures rise above 80 degrees, the Technology Department will notify the President, and give all staff and students 30 minutes notice via e-mail of the pending shut-down. Notice of Network Services downtime will be posted at the entry points to the college and college social media.

10.3.3 Video security

Entry points to critical server and network closets shall be monitored and recorded by the campus video security system.

10.3.4 Server Rack Guidelines

The following guidelines have been established to guide installation of new equipment to the campus server racks.

10.3.4.1 Power

Systems with redundant power supplies must have their power cords plugged into separate power strips. Power must be isolated from data cables.

10.3.4.2 Rack Space

Severs must be installed from the bottom up in the rack enclosures. Equipment must be clearly labeled.

10.3.4.3 Data Connections

Patch Cables must not exceed required length by more than one foot. All Fiber connections must not exceed a minimum bend radius as specified by the manufacturer. All Data connections must be clearly labeled.

11 Computer Workstation Security Policy

11.1 Purpose

This Policy identifies FBCC's procedures for ensuring that computers connected to the FBCC are managed in a secure manner.

11.2 Scope

FBCC has a distributed computing environment with local responsibilities for the maintenance of computer security. This security policy applies to networked computers owned or managed by FBCC that contain information or allow access to information that is confidential under law or policy.

11.3 Policy

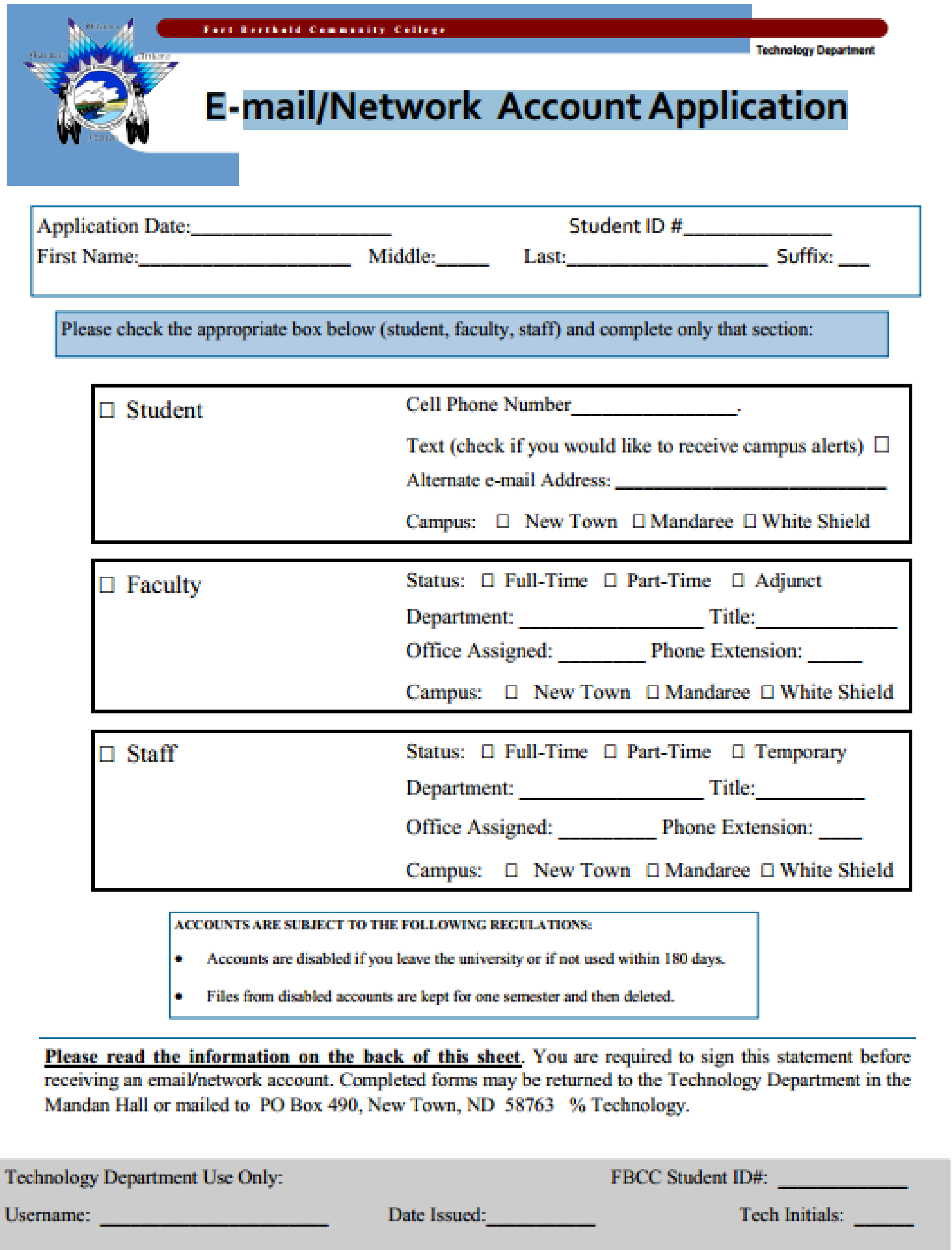
To maximize the security of computers connected to the FBCC network:

- All computers are required to have a user password at startup.
- All authorized users of FBCC network resources are required to "Lock Down" (or log out of) the computer each time the computer is left unattended. If you are unsure how to Lock Down (or log out) of your computer, contact the Technology Help Desk.
- Individual user sessions must also initiate a password protected screensaver after a period of no more than thirty (30) minutes of inactivity. A shorter period of inactivity may be implemented at the direction of a department head.
- All authorized users of FBCC network resources are required to follow the strong password characteristics and management practices. Whenever possible, passwords should be 8 or more characters long, and include letters, numbers, and punctuation characters. They should not be names, words in dictionaries, or permutations of personal data (birth dates or anniversaries, social security numbers, etc.). Passwords should be changed periodically.
- Computers must contain –up-to-date antivirus software to ensure that files saved to them are not infected.
- Workstations should have installed the latest system updates and patches.

12 Enforcement

Employee violations of any part of this policy will result in disciplinary action up to and including dismissal. Student violations of any part of this policy will result in disciplinary action up to and including suspension or expulsion. Authorized access to networks, systems, data, and information is a privilege grant to individuals to perform their FBCC duties. Misuse of this access could result in the loss of this privilege and therefore the inability to perform one's job. By using FBCC computing systems and signing the Appropriate Use statement users signify understanding and acceptance of the policies outlined therein

13 Appendix 1 - E-mail/Network Account Application



Fort Berthold Community College

Technology Department

E-mail/Network Account Application

Application Date:___________________ Student ID #______________

First Name:____________________ Middle:_____ Last:___________________ Suffix: ___

Please check the appropriate box below (student, faculty, staff) and complete only that section:

□ Student

Cell Phone Number________________.

Text (check if you would like to receive campus alerts) □

Alternate e-mail Address: __________________________

Campus: □ New Town □ Mandaree □ White Shield

□ Faculty

Status: □ Full-Time □ Part-Time □ Adjunct

Department: _________________ Title:_____________

Office Assigned: ________ Phone Extension: _____

Campus: □ New Town □ Mandaree □ White Shield

□ Staff

Status: □ Full-Time □ Part-Time □ Temporary

Department: _________________ Title:__________

Office Assigned: _________ Phone Extension: ____

Campus: □ New Town □ Mandaree □ White Shield

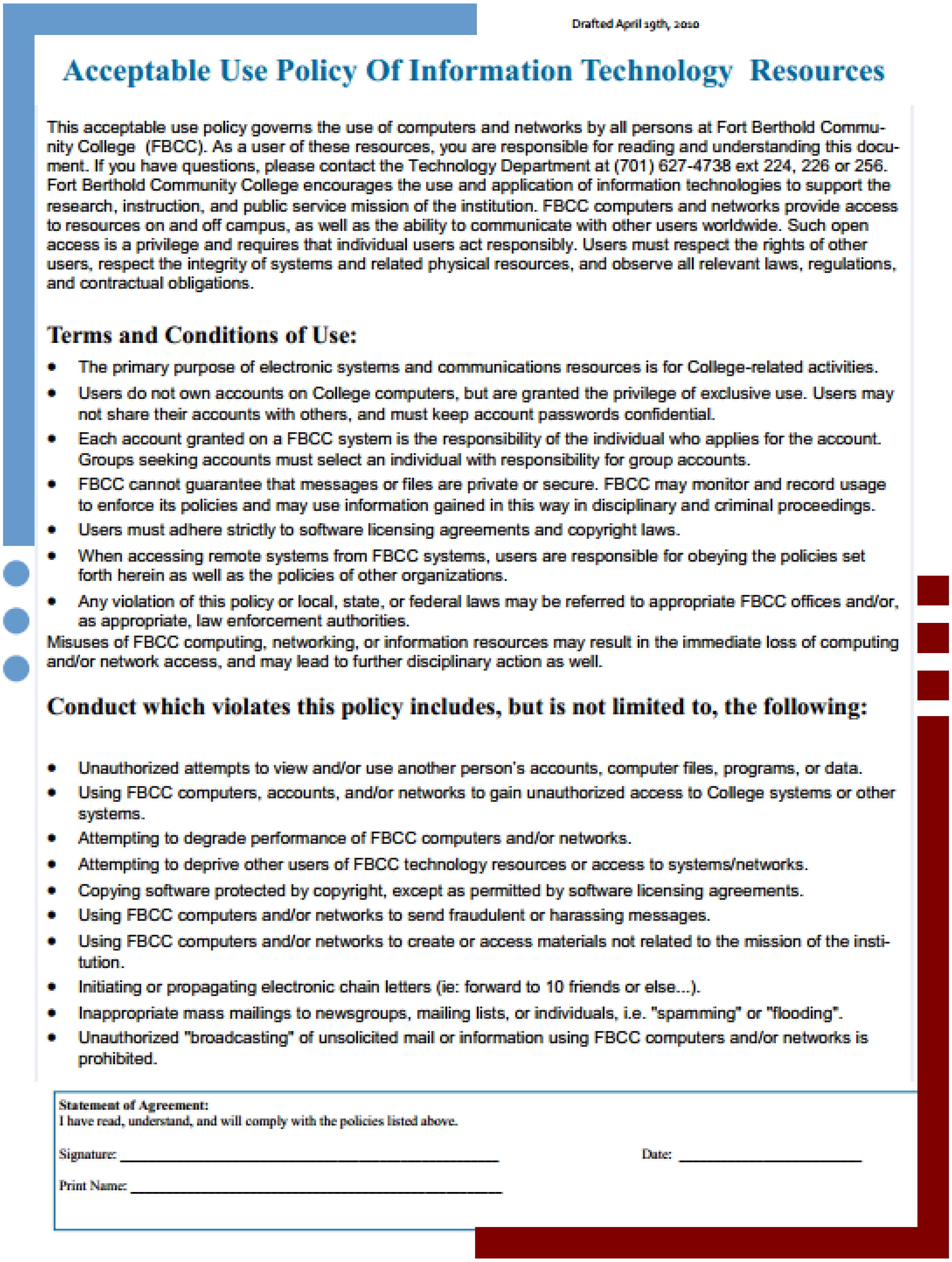
ACCOUNTS ARE SUBJECT TO THE FOLLOWING REGULATIONS:

- Accounts are disabled if you leave the university or if not used within 180 days.
- Files from disabled accounts are kept for one semester and then deleted.

Please read the information on the back of this sheet. You are required to sign this statement before receiving an email/network account. Completed forms may be returned to the Technology Department in the Mandan Hall or mailed to PO Box 490, New Town, ND 58763 % Technology.

Technology Department Use Only: FBCC Student ID#: ____________

Username: ______________________ Date Issued:__________ Tech Initials: _____



Drafted April 19th, 2010

Acceptable Use Policy Of Information Technology Resources

This acceptable use policy governs the use of computers and networks by all persons at Fort Berthold Community College (FBCC). As a user of these resources, you are responsible for reading and understanding this document. If you have questions, please contact the Technology Department at (701) 627-4738 ext 224, 226 or 256. Fort Berthold Community College encourages the use and application of information technologies to support the research, instruction, and public service mission of the institution. FBCC computers and networks provide access to resources on and off campus, as well as the ability to communicate with other users worldwide. Such open access is a privilege and requires that individual users act responsibly. Users must respect the rights of other users, respect the integrity of systems and related physical resources, and observe all relevant laws, regulations, and contractual obligations.

Terms and Conditions of Use:

- The primary purpose of electronic systems and communications resources is for College-related activities.
- Users do not own accounts on College computers, but are granted the privilege of exclusive use. Users may not share their accounts with others, and must keep account passwords confidential.
- Each account granted on a FBCC system is the responsibility of the individual who applies for the account. Groups seeking accounts must select an individual with responsibility for group accounts.
- FBCC cannot guarantee that messages or files are private or secure. FBCC may monitor and record usage to enforce its policies and may use information gained in this way in disciplinary and criminal proceedings.
- Users must adhere strictly to software licensing agreements and copyright laws.
- When accessing remote systems from FBCC systems, users are responsible for obeying the policies set forth herein as well as the policies of other organizations.
- Any violation of this policy or local, state, or federal laws may be referred to appropriate FBCC offices and/or, as appropriate, law enforcement authorities.

Misuses of FBCC computing, networking, or information resources may result in the immediate loss of computing and/or network access, and may lead to further disciplinary action as well.

Conduct which violates this policy includes, but is not limited to, the following:

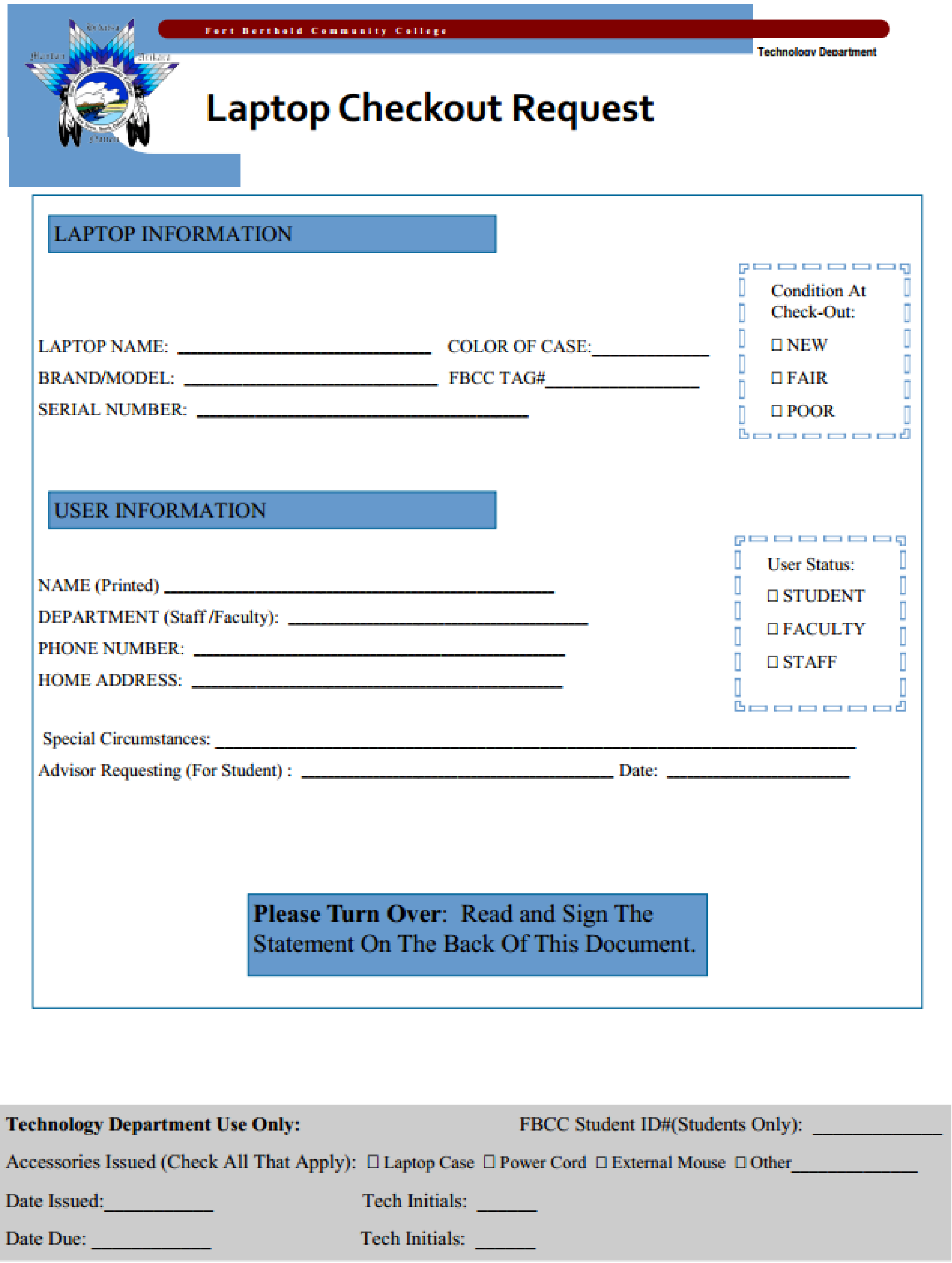
- Unauthorized attempts to view and/or use another person's accounts, computer files, programs, or data.
- Using FBCC computers, accounts, and/or networks to gain unauthorized access to College systems or other systems.
- Attempting to degrade performance of FBCC computers and/or networks.
- Attempting to deprive other users of FBCC technology resources or access to systems/networks.
- Copying software protected by copyright, except as permitted by software licensing agreements.
- Using FBCC computers and/or networks to send fraudulent or harassing messages.
- Using FBCC computers and/or networks to create or access materials not related to the mission of the institution.
- Initiating or propagating electronic chain letters (ie: forward to 10 friends or else...).
- Inappropriate mass mailings to newsgroups, mailing lists, or individuals, i.e. "spamming" or "flooding".
- Unauthorized "broadcasting" of unsolicited mail or information using FBCC computers and/or networks is prohibited.

Statement of Agreement:
I have read, understand, and will comply with the policies listed above.

Signature: ____ Date: ______________________

Print Name: ____

14 Appendix 2 – Laptop Checkout Request



Fort Berthold Community College

Technology Department

Laptop Checkout Request

LAPTOP INFORMATION

LAPTOP NAME: ________________________ COLOR OF CASE:__________

BRAND/MODEL: ________________________ FBCC TAG#____________

SERIAL NUMBER: ________________________________

Condition At Check-Out:
□ NEW
□ FAIR
□ POOR

USER INFORMATION

NAME (Printed) _____________________________________

DEPARTMENT (Staff /Faculty): ____________________________

PHONE NUMBER: ___________________________________

HOME ADDRESS: ___________________________________

User Status:
□ STUDENT
□ FACULTY
□ STAFF

Special Circumstances: ____

Advisor Requesting (For Student) : ______________________________ Date: _________________

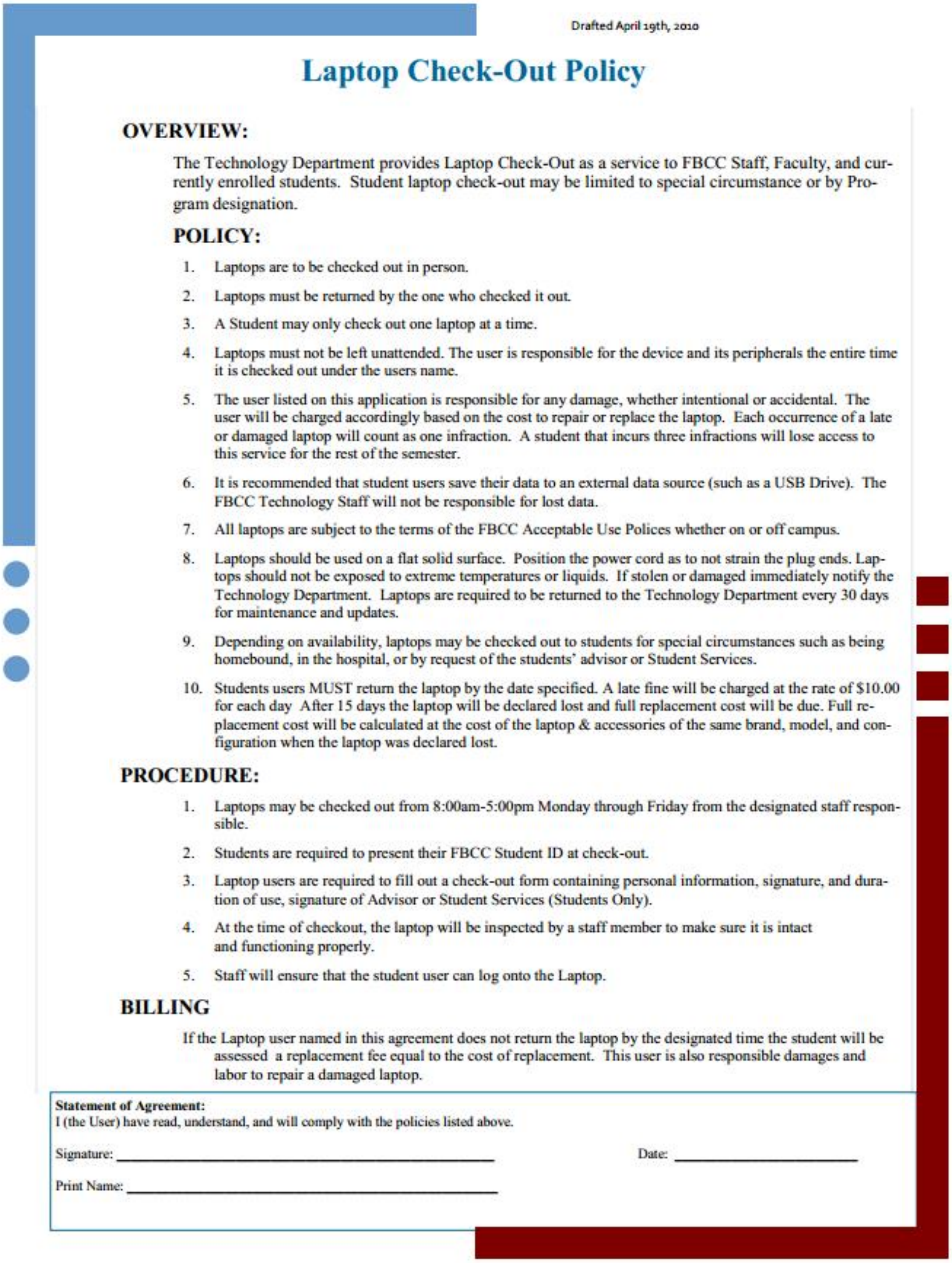
Please Turn Over: Read and Sign The Statement On The Back Of This Document.

Technology Department Use Only: FBCC Student ID#(Students Only): ____________

Accessories Issued (Check All That Apply): □ Laptop Case □ Power Cord □ External Mouse □ Other____________

Date Issued:__________ Tech Initials: _____

Date Due: ___________ Tech Initials: _____



Drafted April 19th, 2010

Laptop Check-Out Policy

OVERVIEW:

The Technology Department provides Laptop Check-Out as a service to FBCC Staff, Faculty, and currently enrolled students. Student laptop check-out may be limited to special circumstance or by Program designation.

POLICY:

1. Laptops are to be checked out in person.
2. Laptops must be returned by the one who checked it out.
3. A Student may only check out one laptop at a time.
4. Laptops must not be left unattended. The user is responsible for the device and its peripherals the entire time it is checked out under the users name.
5. The user listed on this application is responsible for any damage, whether intentional or accidental. The user will be charged accordingly based on the cost to repair or replace the laptop. Each occurrence of a late or damaged laptop will count as one infraction. A student that incurs three infractions will lose access to this service for the rest of the semester.
6. It is recommended that student users save their data to an external data source (such as a USB Drive). The FBCC Technology Staff will not be responsible for lost data.
7. All laptops are subject to the terms of the FBCC Acceptable Use Polices whether on or off campus.
8. Laptops should be used on a flat solid surface. Position the power cord as to not strain the plug ends. Laptops should not be exposed to extreme temperatures or liquids. If stolen or damaged immediately notify the Technology Department. Laptops are required to be returned to the Technology Department every 30 days for maintenance and updates.
9. Depending on availability, laptops may be checked out to students for special circumstances such as being homebound, in the hospital, or by request of the students' advisor or Student Services.
10. Students users MUST return the laptop by the date specified. A late fine will be charged at the rate of $10.00 for each day After 15 days the laptop will be declared lost and full replacement cost will be due. Full replacement cost will be calculated at the cost of the laptop & accessories of the same brand, model, and configuration when the laptop was declared lost.

PROCEDURE:

1. Laptops may be checked out from 8:00am-5:00pm Monday through Friday from the designated staff responsible.
2. Students are required to present their FBCC Student ID at check-out.
3. Laptop users are required to fill out a check-out form containing personal information, signature, and duration of use, signature of Advisor or Student Services (Students Only).
4. At the time of checkout, the laptop will be inspected by a staff member to make sure it is intact and functioning properly.
5. Staff will ensure that the student user can log onto the Laptop.

BILLING

If the Laptop user named in this agreement does not return the laptop by the designated time the student will be assessed a replacement fee equal to the cost of replacement. This user is also responsible damages and labor to repair a damaged laptop.

Statement of Agreement:
I (the User) have read, understand, and will comply with the policies listed above.

Signature: ______________________________ Date: ______________

Print Name: ______________________________