United Tribes Technical College

Information Technology Department Policies & Procedures

(Revised 12-2016)

United Tribes Technical College
12/2016

Table of Contents

Introduction

This document establishes computer usage guidelines for the United Tribes Technical College. United Tribes Technical 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 United Tribes Technical 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.

Mission

To provide a stable and secure computer network environment by seamlessly implementing technology (hardware, software, people), so that faculty and staff can focus on enhancing the students' educational experience without any technical difficulties.

Vision

The UTTC Information Technology Department will strive to meet all campus needs in a coordinated effort to lead the campus community into the future with state of the art facilities.

Goals

It is the goal of this department to service UTTC and all other entities in which we have a working relationship with the most efficient and up to date technology at our disposal. It is the goal of this department to keep abreast of all the technology relevant to our job function. It is the goal of this department to seek out and deploy any technology that enhances the above goals. It is the goal of this department to eventually be financially self-sustaining.

I Integrity

T Trust

D Dependability

Access to Information Technology Resources

Eligibility

Information Technology Resources (computer hardware, software, telephone systems, networks, services, data, and other information) are made available at UTTC 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 UTTC IT resources by the Human Resources Director and ITD. The terms of access will be stated at the time access is granted.

Account Activation/Termination

E-mail access at UTTC is controlled through individual accounts and passwords. Each user of UTTC's e-mail system is required to read and sign a copy of this 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 UTTC naming convention for access to electronic systems comprises the first initial of the first name, followed by full last name. If duplicates occur, the subsequent letter(s) in the first name will be used, or in some limited cases, we may use the entire first name, a period (.), and the last name with all spaces removed.

Personal Computers on the Network

Personal computers (desktops, laptops, etc.) on the campus network are strictly prohibited unless approved in writing by ITD. All acceptable use policies and procedures apply to personal computers.

Virus Protection

United Tribes Technical College requires all existing and incoming desktops and laptops to have anti-virus installed and updated to the most recent virus definitions. Failure to do so can result in the loss of connectivity to the United Tribes Technical College network until anti-virus software is installed. AVG anti-virus software is recommended to all **students**. AVG is free software and can be downloaded at http://free.avg.com/. 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 ITD. 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.

VPN Connections

For all campus users the primary access to UTTC computing services is through the campus network.

VPN access is provided upon supervisor and ITD approval.

College Computer Equipment

Purchasing / Licensing

UTTC IT department has established that all purchases involving IT related equipment/software be researched by appropriate IT staff. Purchases over $500.00 require a 3 bid process from prospective vendor(s). All purchases must fall within the fiscal year budget, accommodate the purchase, and have all appropriate signatures. That all purchased software has the corresponding licenses. All IT related equipment/software will be delivered to ITD for processing before being delivered to the appropriate destination.

Procedure

1. Any purchases can be originated either by UTTC staff/instructor or IT staff. If a staff member or instructor initiates the procedure, they must start by entering a Work Order in the Track-IT system.
2. Purchase is researched to find appropriate vendor for said product(s).
3. 3 bid(s) are acquired for product, if over $500.00.
4. Purchase requisition is filled out and signatures are acquired.
5. Purchase is recorded into database/budget spreadsheet.
6. Vendor is contacted and purchase is acquired.
7. When product arrives, it is recorded into inventory with all relevant serial numbers and product keys.

Licensing

This item relates specifically to software. All required licenses are purchased with software. The licensing document will be housed in ITD, both electronically and physically. ITD will ensure that any entity within UTTC has the proper licensing to operate all software within the LAN and UTTC web-site; www.uttc.edu.

Replacement of College Computer Equipment

All college computer equipment, including servers are on a regular replacement cycle of 3 – 5 years. ITD staff will 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. 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 may also 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

United Tribes Technical College has limited quantities of check-out computers. United Tribes Technical College employees can borrow laptop computers for up to 7 consecutive days for uses related to college business. Extended periods of time will be granted with ITD approval. Reservations are required, and should be made at least two business days in advance. For more information, or to make a reservation, contact: ITD by submitting a work order through http://trackit.uttc.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 Vice President of Academics, Career and Technical Education.

Grant Funded Equipment

Individuals pursuing grants for computing equipment should discuss their plans with the Director, ITD, 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 provided. Purchasing of individual printers is prohibited. 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 UTTC-owned computer equipment. Employees will be held responsible for damage to such equipment arising out of their negligence or intentional misconduct. Employees are responsible for ensuring that all computer equipment is accounted for in the event of office relocation.

Upgrades and Renewal

For computer equipment on the replacement plan ITD 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 ITD. ITD then reassigns the machines. UTTC will not upgrade non-UTTC machines.

IT Department Access to UTTC Computers

All UTTC computers, particularly computers that connect to our network, are ultimately the responsibility of the UTTC IT Department. In order to maintain, audit, and support the equipment, all UTTC computers must either be a member of the network domain, or there must be a local user account with administrative rights on the computer, and that account must be controlled by the UTTC IT Department. Without administrative-level access, the IT Department cannot guarantee the integrity of the UTTC equipment or network. Additionally, lacking this access, the IT Department cannot audit software licensing which could lead to UTTC being liable for large fines and/or penalties if unauthorized or unlicensed software is found to be installed on UTTC computers. There shall be NO exceptions to this without the signed permission of the UTTC IT Department.

Repair of Computer Equipment

UTTC Computer Equipment

All college computer equipment is maintained in-house. If a hardware problem is suspected the user should submit a work order through http://trackit.uttc.edu during normal business hours for assistance. If hardware service is indicated, arrangements will be made with the technician.

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.

Purpose

United Tribes Technical College maintains a Web site to provide information about the College to the campus community and the public at large. In limited situations, certain individuals, departments, divisions, and colleges, at the discretion of the IT Department, may develop and maintain local Web pages within the [www.UTTC.edu] domain. Departments requesting web content are required to work with the IT Department. These guidelines are to insure that Web pages within the [www.UTTC.edu] domain further the purpose of United Tribes Technical College's 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 UTTC presence on the Web. The Committee will determine standards for participation in, and design of, UTTC 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), UTTC employees or students cannot operate their own servers, but to have links created from the UTTC Server to their space on web server must abide by the UTTC policies, procedures, and style guidelines.

Procedures

Members of the United Tribes Technical College community can obtain space on the college web site

for the development of departmental or employee web pages. Any organizations outside the college that are not part of the UTTC may not host their site at UTTC. A content provider is responsible for keeping web information up-to-date and accurate. Failure to maintain accurate pages will result in termination of access to update the website.

Style Guidelines

The first several levels of the UTTC 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 United Tribes Technical 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 United Tribes Technical College departmental or organizational Web pages must be directly related to the stated mission of that department or organization. These links are to be coded to open into a new browser window. 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.

Content Guidelines

The object of these guidelines is to ensure that the content of Web pages accurately represent United Tribes Technical College.

- Content must be consistent with the purpose of United Tribes Technical College's Web site.
- Content must conform to Acceptable Use Policies and United Tribes Technical College's Web Policy so that it is
    - Non-discriminatory,
    - Non-commercial, and
    - Protective of individual privacy.
- Language must be suitable to a public forum.
- Content provided must be appropriately current and accurate.
- 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 United Tribes Technical College.

All Web content submitted must be approved prior to posting. ITD retains the right to edit, request changes, approve, or deny submitted content. 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 United Tribes Technical 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 United Tribes Technical College.

Enforcement

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

Software Standards

Rationale

In UTTC's 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 (PC or Macintosh). Central to making sharing simplistic 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, and databases) is seamless. All purchasing requests will be directed to ITD. This relieves 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

ITD 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 United Tribes Technical College community, since most will be using the same application.

Improved Training

Training teams can focus on developing curricula for levels of user proficiency (introductory, intermediate, and advanced). ITD intends to develop curricula for software that is listed in the software standards list below. Installations and upgrades are the responsibility of ITD. Upgrades can be tested and documented prior to campus wide deployment to reduce potential incompatible and

problems. ITD keeps a central inventory of hardware through the Track-IT software.

Software Standards:

- Microsoft Office
- Internet Explorer
- Google Chrome
- Mozilla Firefox
- Symantec Anti-virus
- Adobe Acrobat Reader/Professional
- Primo PDF
- Altiris Client
- TeamViewer
- Numara Track-IT

For questions about these Policies, Procedures, Plans and Standards, contact: ITD at it@uttc.edu.

Jenzabar Software

History

UTTC has purchased Jenzabar RDBMS software to accommodate the majority of administrative and academic needs. During this purchase and implementation, the UTTC IT department was left out of a functional role because of lack of adequate personnel and physical (network) problems being experienced at that time. Attached are UTTC IT role(s) as it pertains to the strategic plan. This sort of software is now critical to UTTC, and as such requires the collaboration of all involved parties, past, present and future. All specific policy issues relating to Jenzabar will be referenced in the Jenzabar Usage Policy Document. (Appendix G) Access to Jenzabar is granted through filling out a Jenzabar Access form. (Appendix H) With the scheduled implementation of JICS (my.uttc.edu,) this document will need to be updated.

UTTC IT Roles and Responsibilities

- SQL Server Administration and Maintenance
- JICS Server Administration and Maintenance
- Jenzabar System Administrator and task list/ access administration (User Roles)
- Jenzabar EX Module, PowerFAIDS, InfoMaker technical support
- InfoMaker training/support
- Any/all software updates, presently Jenzabar is still on a quarterly update schedule
- In doing any of these functions, UTTC IT staff will follow policy and procedure, internally and per UTTC administrative counsel.
- UTTC IT recognizes the extreme need for information confidentiality and access to the same.

All duties/information pertaining to this function will be documented in a separate manual, because of the complexity of the software itself, which has many procedures.

Telephone and Voicemail Acceptable Use Policy

Purpose

Telephone communications are an essential part of the day-to-day operations of United Tribes Technical College. Telephone and voicemail services are provided to employees of United Tribes

Technical College in order to facilitate performance of United Tribes Technical College work. The goal of this policy is to balance the business need for telephone and voicemail use by United Tribes Technical College with the costs involved.

Scope

This policy applies to all employees of United Tribes Technical College, and all usage of United Tribes Technical College telephone and voicemail services.

Telephone and Voicemail Services

As of the date of the writing of this document the telephone system at United Tribes Technical College is an open source Asterisk based system running FreePBX and Elastix which will be referred to from here on out as "PBX".

Basic Policy

As with all United Tribes Technical College resources, the use of telephones and voicemail should be as cost effective as possible and in keeping with the best interests of United Tribes Technical 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 United Tribes Technical College.
- ITD is responsible for installation and repair of all telephony equipment and administration of telephone and voicemail accounts. Individual departments will be responsible for the cost of repairs and/or replacement of faulty equipment within their department.
- Department supervisors are responsible for overseeing telephone and voicemail use and ensuring policy compliance, as well as ensuring ITD is notified through Track-IT of any adds, moves, or changes required to telephone or voicemail services. AMC's for new employees must come through HR.
- All UTTC employees are eligible to receive a telephone and/or voicemail based on their needs. This need will be determined by their supervisor.
- Most extensions on campus have a direct dial number (DID) associated with them. This will be communicated to the employee via email.
- The number of telephone calls made should be limited in number and duration to that necessary for effective conduct of business.
- 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.
- If a voicemail box is full, no further messages can be recorded. It will be the responsibility of the employee to manage his/her voicemail box so as to maintain adequate space for new voicemails to be recorded.
- If the employee will be away from the office for more than one business day, he/she is 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) is prohibited since a fee is incurred with each use. If you are unsure of a number, please consult print or Internet based telephone directories.
- ITD will bill departments appropriately for any and all telephony services.
- Additional charges may apply for work requests that require an outside vendor. In addition to these charges, a 40% surcharge will be applied to all rush or expedited Add/Move/Change orders that are outside of the work completion times listed below under "Service and Repair"

Unacceptable Use

United Tribes Technical 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.
- Breaking into a voicemail box via unauthorized use 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 United Tribes Technical College.
- Calling 900 phone numbers.
- Calling 411 or any other billable service
- Accepting collect phone calls.
- 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 short duration.

Any personal long-distance calls that must be made (except toll-free 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 United Tribes Technical College, the employee should receive permission from a supervisor to make the call first. Regardless, employees are expected to reimburse United Tribes Technical College for the cost of any long-distance calls within 2 days of receipt of the relevant bill.

Monitoring

United Tribes Technical 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 United Tribes Technical College:

- Date, time, length of call, number called, caller ID number
- Costs per call
- Type of usage

Privacy

To assure an individual's right to privacy, ITD protects telephone call records from routine disclosure except when needed by:

- Departments to review monthly bills and charges for validity.
- The UTTC Internal Audit Office for audit of record keeping procedures or for investigative purposes.
- The UTTC Security Department for investigative purposes.
- UTTC Administrative Counsel for investigative or legal purposes.

Exceptions to this policy must be approved by the Communications Administrator and the Vice President of Student & Campus Services.

Tracing or trapping of calls may be performed in the case of threats to life or property. Such traces or traps must be authorized by a Vice President or the President.

Service and Repair

ITD requests that at least 3 days' notice be given to set up standard telephone service and voicemail through TRACK-IT (actual installation time may vary depending on scope of work to be performed).

If there is a problem with an existing telephone or voicemail box, contact ITD by submitting a work order through TRACK-IT. Repairs to existing extensions are typically made within 1 day.

To facilitate prompt service, employees must use TRACK-IT for all Adds/Moves/Changes or trouble issues. ITD will not be responsible for the successful completion of work if it is reported outside of TRACK-IT.

Pricing

Pricing for telephones or related equipment or services will be issued on a case by case basis.

Purchasing

All telephones and or related items must be purchased and/or approved through ITD.

Access to Plant Facilities

To avoid damage to the system or disruption of services to customers, only personnel authorized by ITD may have access to distribution closets and switch rooms for installation, maintenance, or repair purposes. Exceptions to this policy must be approved by the Communications Administrator and the Vice President of Student & Campus Services.

Telephone Directory

The official telephone directory for the campus can be located here. The directory is serviced and maintained by ITD. If a discrepancy is found in the directory, a work order can be placed through Track-IT requesting the discrepancies be amended. You may also use the directory located in your email.

Cellular Telephones

All United Tribes Technical College supplied Cellular telephones are handled by the Communications Administrator. A mobile devices policy and procedure manual can be located here.

Placing your work email on your personal cellular phone is allowed, but falls under any and all United Tribes Technical College rules associated with email and/or telephony communications including voicemail. Beyond providing the email settings here.

Note: If you change your computer password, you will have to change it in the email settings on your cellular phone as well.

Long Distance Access

All access to long distance telephone service requires the use of a PIN number. PIN numbers are distributed by the Communications Administrator. If an employee needs access to long distance telephone service, he/she should request this through their supervisor.

Fax and Fax Services

Departments requiring fax services will be provided with an analog phone line and fax number. Because of a lack of analog lines to certain areas of campus, not all requests for fax lines will be able to be fulfilled. Fax to email services are available as an alternative in this case. Fax machines must be purchased by the requesting department. This purchase must be made through ITD.

Telephone Procedures

All employees that receive a telephone also have access to the manual on how to operate their phone, which is located here. It is the employee's responsibility to learn how to operate their phone. If after reading the appropriate manual(s) the user is still having troubles, the user can request support by submitting a work order at http://trackit.uttc.edu

Voicemail Procedures

A welcome email is sent out to all new users. There will be instructions in the email on how to use the phone and setup voicemail. There will also be a copy of the phone and voicemail instruction manuals in the email.

Printer Policy

Purpose

Printers represent one of the highest equipment expenditures at United Tribes Technical College. The goal of this policy is to facilitate the appropriate and responsible business use of United Tribes Technical College's printer assets, as well as control United Tribes Technical 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 United Tribes Technical College, as well as any contract employees in the service of United Tribes Technical College who may be using United Tribes Technical College networks and equipment.

Supported Printers

United Tribes Technical 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

- Printers are to be used for documents that are relevant to the day-to-day conduct of business at United Tribes Technical College. United Tribes Technical College printers should not be used to print personal documents.
- Installation of personal printers is not condoned at United Tribes Technical College due to the cost of maintaining and supporting many dispersed machines. Personal is defined as single-desktop use printers.
- 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 there is a copier connected to the network in your area, please print to this copier directly, rather than making 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.
- Avoid printing large files, as this puts a drain on network resources and interferes with the ability of others to use the printer.
- 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). This does not apply if this is a secure print job.
- 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.
- Avoiding printing a document just to see what it looks like. This is wasteful.
- Avoid re-using paper in laser printers, as this can lead to paper jams and other problems with the machine.
- 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 ITD 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.
- Printer paper is available at all departments. Toner cartridges are available at all departments and are the responsibility of your department. These items can be obtained through Property & Supply.
- 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 ITD or ask a trained co-worker for help.
- Report any malfunction of any printing device to ITD 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 United Tribes Technical 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 United Tribes Technical College Virtual Private Network).
- Wireless gateways on United Tribes Technical College premises.
- Third-party wireless Internet service providers (also known as "hotspots").

The policy applies to any equipment used to access United Tribes Technical College resources, even if said equipment is not United Tribes Technical College, owned, or supplied. The overriding goal of this policy is to protect United Tribes Technical College's technology-based resources (such as United Tribes Technical 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 United Tribes Technical College technology resources must adhere to company-defined processes for doing so.

Scope

This policy applies to all United Tribes Technical 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 United Tribes Technical 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. Non-secured 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 United Tribes Technical College facilities will be managed at the sole discretion of ITD. Unauthorized installations of wireless equipment, or use of unauthorized equipment within the organizational campus, are 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 United Tribes Technical College firewall will be centrally managed by United Tribes Technical College's ITD and will utilize encryption, strong authentication, and other security methods at ITD's discretion. Although ITD 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

United Tribes Technical College currently maintains two wireless networks. These include a network called "UTTC" which is the public wireless network. This is an open network and anyone has access to use it. The second network is called "UTTC_Secured_Data" which is the secured wireless network.

Access to this network requires a domain account for the computer and user.

Policy and Appropriate Use

It is the responsibility of any employee of United Tribes Technical 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 United Tribes Technical 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:

- General access to the organizational network through the Internet by residential remote users through United Tribes Technical 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 United Tribes Technical College's Internet acceptable use policies.

- 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 United Tribes Technical 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 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 United Tribes Technical 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 United Tribes Technical College's IT Department. Antivirus signature files must be updated in accordance with existing company policy.

- 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 United Tribes Technical College's IT Department.

- The wireless access user agrees to immediately report to his/her manager and United Tribes Technical 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.

- The wireless access user also agrees to and accepts that his or her access and/or connection to United Tribes Technical 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.

- IT reserves the right to turn off without notice any access port to the network that puts the college'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.

End-User Backup Policy

Introduction

Data is one of United Tribes Technical 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 ITD backs up servers, please refer to United Tribes Technical College's Server Backup Policy.

Backup Schedule

Full backups are conducted on every Sunday evening with Incremental backups being conducted on a daily basis. Full Data Backups are stored off-site at a secure location once a week or whenever a full backup is completed.

Data Storage

It is United Tribes Technical College's policy that ALL United Tribes Technical 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:** United Tribes Technical College data, especially works-in-progress, should be saved. This ensures that data will be backed up when the servers are backed up. United Tribes Technical College's policy states that all data must be saved on the user's "My Documents" or the "Share" drive. Saving of documents to any other location, than those previously listed, is not approved.

- **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 from that week's tapes IT will then use prior week until job is finished. As a result, it's essential that ITD regularly test ITD 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:

- The individual responsible for overseeing backup and restore procedures is ITD Network Administrator. If a user has a restore request, they can contact ITD by submitting a request form via http://trackit.uttc.edu.
- 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 United Tribes Technical College's IT Department via http://trackit.uttc.edu. ITD will walk the user through the restore procedure for their mobile device.
- In the event of unplanned downtime, attack, or disaster, United Tribes Technical College's full restoration procedures will take place.
- In the event of a local data loss due to human error, the end-user affected must contact ITD 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.
- 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.
- 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.

New Users / Security Access

Policy

ITD will have a process for the entering of new employees into the UTTC network and provide user(s) with the appropriate user/security rights as they pertain to their position within the organization. ITD recognizes the extreme need for confidential information and will take all precautions when providing user access rights. All access rights will be approved by the Vice President of the involved user, Human Resources, and Network manager.

Process

ITD will only recognize new employees by notification from the UTTC HR department. Notification will come in the form of the Information Technology Request for Network Access\ E-Mail (Form IT-N, Appendix c). The appropriate IT staff will then:

1: Verify form IT-N with HR department.

2: Create User account within the UTTC Active Directory Domain (UnitedTribesTech.net) with the following naming conventions:

- First initial of first name and complete last name = example: John Doe = jdoe
- Password requirement = minimum of 5 characters with 1 capital letter and 1 numeral digit = example = itW1user
- Password Changes: Currently network password changes are required every 3 months

3: An email address is automatically created on the Exchange server with the email address being comprised of the network username@uttc.edu

4: A departmental/organizational user folder will be created. The folder access rights will be limited to the user, department head, and network administrator. All information access is verified by new user supervisor, Vice President, network administrator and any/all federal, state, UTTC entities.

5: **The network administrator has access rights to all objects within the network to effectively manage the network**.

6: The new user is notified of username and password.

7: New user is made aware of directory structure that pertains to their department.

8: New user is issued a desktop PC, laptop and any other IT equipment to fulfill their job function. In most cases, the equipment is already physically at the department. This information is entered into the IT database.

All information that is stored in any network server is the property of UTTC. User access rights are assigned as needed to fulfill their specific role within the college.

Student Email / Domain Account

Policy

ITD will have a process for the entering of new students into the UTTC network and provide user(s) with the appropriate user/security rights as they pertain to their education within the campus. ITD recognizes the extreme need for confidential information and will take all precautions when providing user access rights.

Process

ITD will only recognize new students by notification from their advisor. Notification will come in the form of the Student Email Request Form. The appropriate IT staff will then:

1: Create User account within the UTTC Active Directory Domain (Student.UnitedTribesTech.net) with the following conventions:

- Student ID Number = example: student\XXXXX
- Password requirement = minimum of 5 characters with 1 capital letter and 1 numeral digit = example = itW1user
- Password Changes: Currently network password changes are required every 3 months

2: An email address is automatically created on the Exchange server with the email address being comprised of Last Name.First Name@stu.uttc.edu

3: **The network administrator has access rights to all objects within the network to effectively manage the network**.

6: The student's advisor is notified of username and password.

All information that is stored in any network server is the property of UTTC. User access rights are assigned as needed to fulfill their specific role within the college.

Students will abide by the acceptable use standards as outlined in Appendix B.

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.

- 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, Jenzabar) will need to be deactivated at a particular date and time. Ideally, in the event of involuntary termination, deactivation should take place immediately before or while the employee is being notified of his or her termination.
- List in advance any equipment and files that should be in the employee's possession and must be returned.
- Have all work-related computer files transferred to a location determined by ITD for secure review by the departing employee's successor or supervisor. These files will be deleted, stored, or forwarded to the appropriate United Tribes Technical College staff member
- If requested, ITD may arrange for return of personal print and computer files to the employee.
- 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. United Tribes Technical 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 United Tribes Technical 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 United Tribes Technical 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 United Tribes Technical 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 United Tribes Technical College's Property & Supply. United Tribes Technical 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. ITD is in charge of selecting and approving external agents for recycling hardware and/or sanitizing hardware of harmful toxins before shipment to landfills.

Policy

Acceptable methods for the disposal of IT assets include, but may not be limited to:

- In accordance with the property disposal policy of this college, ITD will coordinate with Property & Supply.

It is the responsibility of any employee of United Tribes Technical 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 United Tribes Technical College are done appropriately, responsibly, and ethically, as well as with company resource planning in mind.

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.

Please submit a Track-IT work order to request a quote from ITD for any technology equipment.

IT Equipment Borrowing

Equipment Borrowing Policy

IT Equipment may be borrowed by:

- Staff and Faculty.
- For the use of: research, instruction, presentations, and practicum use.
- For the period of: 7 days and if longer will need approval from Department Supervisor and ITD.

NOTE: BORROWING TIMES MAY BE SHORTENED AT ANY TIME IN CASE OF SIGNIFICANT DEMAND. In order to borrow IT equipment, proper procedures must be done:

- Fill out the corresponding equipment sign-out sheet with printed name, signature, 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 United Tribes Technical College network. However, network-enabled portable computers also pose the risk of data theft and unauthorized access to our United Tribes Technical College network. Any device that can access the United Tribes Technical 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 United Tribes Technical 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.

- Anti-virus software must be installed.
- Software must have active scanning and be kept up-to-date.

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.

Security Audit's

ITD reserves the right to audit any laptop used for company business to ensure that it continues to conform to this certification policy. ITD 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, USB drives, 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 United Tribes Technical College in terms of lost data, lost staff productivity, and/or lost reputation. As a result, one of the goals of United Tribes Technical 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 United Tribes Technical College employees to help achieve effective virus detection and prevention.

Scope

This policy applies to all computers that are connected to the United Tribes Technical 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 United Tribes Technical College network. The definition of computers includes desktop workstations, laptop computers, handheld computing devices, and servers.

General Policy

Currently, United Tribes Technical College has Symantec Endpoint Protection anti-virus software in use. The most current available version of the anti-virus software package will be taken as the default standard. All computers attached to the United Tribes Technical 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 ITD virus definition files kept up to date. Any activities with the intention to create and/or distribute malicious programs onto the United Tribes Technical 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 ITD 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 United Tribes Technical 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 removable media 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 United Tribes Technical College IT Department:

- ITD is responsible for maintaining and updating this Anti-Virus Policy.
- ITD will keep the anti-virus products it provides up-to-date in terms of both virus definitions and software version in use.
- ITD will apply any updates to the services it provides that are required to defend against threats from viruses.
- ITD will install anti-virus software on all United Tribes Technical College owned and installed desktop workstations, laptops, and servers.
- ITD will assist employees in installing anti-virus software according to standards on personally owned computers that will be used for business purposes.
- ITD will not provide anti-virus software in these cases.
- ITD will take appropriate action to contain, remove, and assist in recovery from virus infections. In order to do so, ITD may be required to disconnect a suspect computer from the network or disconnect an entire segment of the network.
- ITD will perform regular anti-virus sweeps.
- ITD will attempt to notify users of United Tribes Technical 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 United Tribes Technical 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 United Tribes Technical 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.

Consultant Agreements

Policy

During the course of activities of UTTC and the technology industry, it will be imperative that UTTC IT procure the expertise of outside consultants.

Procedure

When the services of outside consultants pertaining to computer/telephony technologies are needed, UTTC IT will:

Have a RFP prepared; outlining our specific needs, this RFP will be approved by UTTC administrative counsel or relevant Dean.

- Consultant(s) will be researched, reviewed and recommended by UTTC IT
- UTTC IT will be responsible party in terms of seeing that any/all specified work is completed satisfactory in terms of time and expertise.

Consultant(s) will provide UTTC IT a detailed and timely report on their rendered services.

Training / Professional Development

Policy

ITD will have a schedule and agenda for the professional development of all IT staff.

Procedure

For each ITD employee, in accordance with their job title, ITD will:

Budget funds for professional development of IT staff

- Create a PD plan for 1 year (fiscal) and long range
- Be certain that it fits into the needs of UTTC and the individual
- All PD plans will be agreed upon and signed on an individual and fiscal basis
- ITD will pay for any certification testing fees a total of 1 time(s), the individual is responsible for testing fees beyond that
- All PD plans will be made no later than January 15th of each calendar year

All PD plans will be reviewed and approved by the Vice President of Student and Campus Services

Billable Services

Policy

ITD will bill back to UTTC departments certain services we provide. ITD will also have a procedure for billing their services to out-side entities.

Procedure

ITD has seen fit to charge back to UTTC departments certain services (billable), these services are:

- Full scale cabling
- Telephony
- Research
- Acquisition, installation (all)
- Repair above and beyond normal maintenance
- Server/Network Configuration

Student & Employee Handbook

Use of Telephone and E-mail Systems

Employees may be required to reimburse UTTC for any charges resulting from their personal use of the telephone. Employees are asked to keep personal calls to a minimum. Excessive use of the telephone for personal calls may result in disciplinary action.

The use of postage paid for by UTTC for personal correspondence is not permitted. To assure effective telephone communications, employees should always speak in a courteous and professional manner. Each employee should confirm information received from the caller, and hang up only after the caller has provided that confirmation.

E-mail, the Internet, and Other Electronic and Telephonic Communications

All electronic and telephonic communication systems and all communications and information transmitted by, received, or stored in these systems are the property of UTTC and as such are to be used for job-related purposes. The use of any software and business equipment, including, but not limited to, facsimiles, telecopy's, computers, UTTC e-mail system, the Internet, and copy machines for private purposes is prohibited, except for emergencies. Use of the Internet for criminal purposes under any applicable state or Federal law, including, but not limited to, theft of software, rights to money, or any other service or good provided on or over the Internet; deception or fraud; copyright and trademark violation; criminal solicitation; unlawful destruction, interference or entrance into Internet sites ("hacking"); theft of personal information such as credit card numbers; spreading or insertion into other software or data destructive, disruptive or invasive software (known as "viruses"), whether or not time delayed; purveying or obtaining pornographic materials in violation of any Federal law; and making threats or creating a conspiracy to commit a criminal act subjects the employee to immediate termination. Employees using UTTC equipment for personal purposes do so at their own risk, and are subject to appropriate discipline. Further, employees are not permitted to use any code that accesses information about UTTC, access UTTC files protected by security codes or other devices, or retrieve any UTTC communication stored for the benefit of any employee other than his or her own information or otherwise stored for persons other than the employee unless authorized to do so or unless they have prior clearance from an authorized UTTC representative. All pass codes are the property of UTTC. No employee may use a pass code or voice-mail access code that has not been issued to that employee or that is unknown to UTTC. Moreover, improper use of the E-mail system (e.g., spreading offensive jokes or remarks), including using the Internet to do so, will not be tolerated. Employees who violate this policy are subject to disciplinary action, up to and including termination of employment, in accordance with the disciplinary procedures stated in Section 7-1 of this Handbook.

To ensure that the use of electronic and telephonic communications systems and business equipment is consistent with UTTC legitimate business interests, authorized representatives of UTTC may monitor the use of such equipment from time to time. This includes monitoring Internet usage of any kind and listening to stored voice-mail messages.

Internet Policies

UTTC provides access to the Internet. The Internet represents a useful tool for UTTC, but like any other tool, it must be used properly. For purposes of this policy, Internet includes any public electronic data communications network.

Internet E-mail offers broadly similar capabilities to other College E-mail systems, except that correspondents are external to UTTC. External E-mail messages may carry one or more attachments. An attachment may be any kind of computer file, such as a word processing document, spreadsheet, software program, or graphic image. Just as UTTC has an official Internet Web site, so do other organizations. Most public Web sites are "read only", meaning that they permit a person who visits the site to read material posted on the Web site but not to leave a message.

The following rules apply with respect to Internet usage:

- No Downloading of Non-Business Related Data: UTTC allows the download of files from the Internet in certain circumstances and by certain individuals. However, downloading files are limited to those which relate directly to UTTC business or otherwise relate to activities conducted on campus, including files which are related to a specific classroom teaching purpose.
- No Downloading of Application Programs: UTTC does not permit the download or installation of application software from the Internet on UTTC computers, except as necessary to access information necessary to conduct UTTC business or to protect information on the user's computer. Before any application software is downloaded, consult with a UTTC computer technician. Such software may not only contain embedded viruses, but also may be untested and may interfere with the functioning of other software used by UTTC.
- No Participation in Web-based Surveys Without Authorization: When using the Internet, the user implicitly involves UTTC as the source of the transmission of data over the Internet. Therefore, users should not participate in Web or E-mail based surveys or interviews without authorization.
- No Use of Subscription-based Services Without Prior Approval: Some Internet sites require that users subscribe before being able to use them. Users should not subscribe to such services using UTTC equipment, computers or Internet services without the express approval of a UTTC computer technician or as otherwise approved by the appropriate administration official.
- No Violation of Copyright: Many of the materials on the Internet are protected by copyright. Even though they may seem to be freely accessible, copyright laws that apply to print media also apply to software and material published or made available on the Internet. Employees are permitted to print out Web pages and to download material from the Internet for informational purposes as long as the purpose for such copying falls into the category of "fair use". Please do not copy or disseminate material that is copyrighted. Employees having any questions regarding such materials should contact their supervisor.

Employees who violate any aspect of this policy are subject to disciplinary action in accordance with the disciplinary procedures stated in Section 7-1 of this Handbook, up to and including termination of employment.

Emergency Procedures

During the normal working hours, notify UTTC IT of any emergency or conditions requiring immediate attention. Call extension 1230 or extension 1604

Emergency procedures described below are invoked during off-work hours. Off-work-hours are defined as hours outside normal working days, 8:00 a.m. - 5:00 p.m.

Finance Department

- **Problems in finance.** During off work hours, the finance personnel will contact the UTTC IT staff cell phone number. (226 7788) Secondary number (426 4650)

All Other UTTC Network Users

- **Users on the UTTC network** will contact Campus Security if they are unable to login. If either three users is not able to login at the same time, or one user from at least three different connections within the administrative department are unable to login, Campus Security will call and inform a UTTC IT staff cell phone number. (266 7788) Secondary number (426 4650)

Telephone

- **If the problem is urgent and needs immediate attention**, users will contact Campus Security. Campus Security will then call and inform the UTTC Communications Administrator emergency line at (224-7234) Secondary number (426 4650)

Other UTTC Emergency Service Assistance Phone Numbers

Security	**UTTC**	**701 221 1700**
Advanced Mechanical (Server Room)	**Heat/Cool**	**701 223 4328**
Eaton (George J) (Server Room)	**UPS/Battery Backup**	**320 267 6530**
Alarm Dialer (Server Room)	**ID and Clear** Alarm Clear (555)	**701 530 0631**
Doug Kilber	**Manager**	**701 220 7415**
Dell-Comm	**Office**	**701 222 2887**
Qwest (T1-PRI)	**Telephone** (2) (4) (1)	**800 223 7508**
Midco (No incoming calls)	**Telephone**	**800 888 1300**

APPENDICES

Appendix A: UTTC Computer Release Form

United Tribes Technical College
Computer Release Form

I understand and agree to the following conditions governing the use and care of microcomputer hardware and software assigned to me.

I agree to abide by the license agreement between the proprietor of the software and United Tribes Technical College and I understand that the improper reproduction of proprietary software by any means is prohibited.

I will not use proprietary software which is NOT the property of UTTC on any computing devices unless I have specific authorization to do so.

I understand that safeguarding the software is my responsibility.

I have read the policies and procedures in the employee policies handbook and agree to abide by them.

I will only access UTTC's local area network with my user ID and password. I will not use unauthorized codes or passwords to gain access to other employee's files.

I understand that Internet and World Wide Web access should be used for work-related purposes.

I understand that the e-mail system is designed to facilitate business communication among employees and other business contract. In addition, I understand the following about the e-mail system:

- E-mail communications may be considered UTTC's documents and may be subject to review.
- The e-mail system is not to be used for personal gain or to solicit outside business ventures or political or religious causes.
- UTTC reserves the right to review the contents of employee's e-mail when necessary for business purposes.
- Foul, in-appropriate, or offensive messages are prohibited.
- E-mail messages are capable of being forwarded without the express permission of the original author. Accordingly, due caution should be exercised when sending e-mail messages.

United Tribes Technical College employees who violate any of these guidelines are subject to disciplinary actions or dismissal.

_____ _____

Employee Signature Date

Appendix B: Acceptable Use Policy

United Tribes Technical College
Technology Acceptable Use Policy

All electronic and telephonic communication systems and all communications and information transmitted by, received, or stored in these systems are the property of UTTC and as such are to be used solely for job-related purposes. The use of any software and business equipment, including, but not limited to, facsimiles, tele-copiers, computers, UTTC E-mail system, the Internet, and copy machines for private purposes is strictly prohibited.

Employees using this equipment for personal purposes do so at their own risk. Further, employees are not permitted to use a code, access a file, or retrieve any stored communication unless authorized to do so or unless they have prior clearance from an authorized UTTC representative. All pass codes are the property of UTTC. No employee may use a pass code or voice-mail access code that has not been issued to that employee or that is unknown to UTTC. Moreover, improper use of the Email system (e.g., spreading offensive jokes or remarks), including using the Internet, will not be tolerated. Employees who violate this policy are subject to disciplinary action, up to and including discharge, in accordance with the disciplinary procedures stated in Section 6-17 of this Handbook.

To ensure that the use of electronic and telephonic communications systems and business equipment is consistent with UTTC legitimate business interests, authorized representatives of UTTC may monitor the use of such equipment from time to time. This includes monitoring Internet usage of any kind, listening to stored voice-mail messages, and the logging of computer user account activities into databases.

UTTC provides access to the Internet. The Internet represents a useful tool for UTTC, but like any other tool, it must be used properly. For purposes of this policy, Internet includes any public electronic data communications network.

Internet E-mail offers broadly similar capabilities to other Company E-mail systems, except that correspondents are external to UTTC. External E-mail messages may carry one or more attachments. An attachment may be any kind of computer file, such as a word processing document, spreadsheet, software program, or graphic image.

Just as UTTC has an official Internet Web site and so do other organizations. Most public Web sites are “read only”, meaning that they permit a person who visits the site to read material posted on the Web site but not to leave a message.

The following rules apply with respect to Internet usage:

- No Downloading of Non-Business Related Data: UTTC allows the download of files from the Internet. However, downloading files must be limited to those, which relate directly to UTTC business.

- No Downloading of Application Programs: UTTC does not permit the download or installation on UTTC computers of application software from the Internet, except as necessary to access information necessary to conduct UTTC business. Before any application software is downloaded consult with a UTTC computer technician. Such software may not only contain embedded viruses, but also is untested and may interfere with the functioning of standard UTTC applications.
- No Participation in Web-based Surveys Without Authorization: When using the Internet, the user implicitly involves UTTC as the source of the transmission of data over the Internet. Therefore, users should not participate in Web or E-mail based surveys or interviews without authorization.
- No Use of Subscription-based Services Without Prior Approval: Some Internet sites require that users subscribe before being able to use them. Users should not subscribe to such services without the express approval of UTTC management.
- No Violation of Copyright: Many of the materials on the Internet are protected by copyright. Even though they may seem to be freely accessible, many of the intellectual property laws, which apply to print media, still apply to software and material published on the Internet. Employees are permitted to print out Web pages and to download material from the Internet for informational purposes as long as the purpose for such copying falls into the category of "fair use." Please do not copy or disseminate material, which is copyrighted. Employees having any questions regarding such materials should contact their supervisor.
- No Viewing or Displaying of Pornographic, Violent, or Otherwise Offensive Materials: Visiting websites that contain such content and downloading, displaying, or viewing such materials is forbidden. The Internet Protocol (IP) numbers used by your computers are the property of UTTC and are recognized worldwide as belonging to UTTC. Therefore, using UTTC computer equipment and IP numbers to view illegal, immoral, offensive, or otherwise discriminatory websites will not be tolerated.

Employees who violate this policy are subject to disciplinary action in accordance with the disciplinary procedures stated in Section 6-17 of this Handbook, up to and including discharge.

I have read and understand the UTTC Acceptable Use policy. I agree to abide by this policy.

_____ _____

Employee Signature Date

Acknowledged by:

_____ _____

Human Resource Representative Date

Appendix C: IT Checkout Form

IT Equipment Checkout Sheet

OTHER

This laptop is the property of United Tribes Technical College. By signing your name below, you agree to assume all responsibility for the laptop that you have checked out, and that you will do everything possible to return the laptop in the same condition as it was given to you. Your signature also represents your agreement to assume responsibility for any and all replacement and/or repair costs incurred if this laptop is stolen, lost, or damaged. You agree that this laptop computer has been assigned to you on a temporary basis, and must be returned on the request of the IT Department. Thank you.

Date Checked Out	Name	Signature	IT Initials	Date Returned	IT Initials

Appendix D: Harassment Policy

Harassment, Including Sexual Harassment, and Fraternization

Prohibition of harassment, including sexual harassment:

Harassment, including sexual harassment, is contrary to basic standards of conduct that are expected of all UTTC employees. Any employee who engages in any of the acts or behavior defined below is subject to corrective action up to and including immediate discharge. Any employee who feels that he or she has been the victim of harassment as defined in this section should immediately report the facts concerning the harassment under the procedure as described herein. With respect to harassment, including sexual harassment, UTTC prohibits the following:

1. Verbal, physical or visual conduct of a racial, ethnic, religious or other nature which impairs the employee's ability to perform his or her job, or which is calculated to or does cause the employee embarrassment, mental anguish, or physical discomfort or injury.
2. Unwelcome sexual advances; requests for sexual favors; and all other verbal or physical conduct of a sexual or otherwise offensive nature, especially where:
    a. Submission to the conduct is made either explicitly or implicitly a term or condition of employment;
    b. Submission to or rejection of the conduct is used as the basis for decisions affecting an individual's employment; or
    c. The conduct has the purpose or effect of creating an intimidating, hostile, or offensive working environment.
    d. The conduct is between a staff member, including faculty and a student, where the staff member or faculty person involved is in a position of authority over the student, such as, but not limited to, the relationship between an instructor and a student, administration official and a student, or security guard and a student,
3. The prohibited conduct includes, but is not limited to:
    a. Visual conduct such as leering; making sexual gestures; displaying sexually suggestive pictures or objects, cartoons, or posters; suggestive or obscene letters, notes, or invitations, including any kind of offensive communications transmitted or shown on a computer;
    b. Verbal conduct such as derogatory comments, epithets, slurs or sexual innuendo; sexually related jokes; graphic verbal commentaries about an individual's body; or using sexually degrading words;
    c. Physical conduct such as unwanted, suggestive or offensive touching; assault, impeding or blocking movement. Offensive comments, including, but not limited to, jokes, innuendoes, and other sexually oriented statements.

Prohibited relationships (fraternization)

The following relationships are strictly prohibited:

A sexual or intimate relationship between a staff member (including a faculty member) and a student, where the staff or faculty member is in a position of authority over the student, such as, but not limited to, the relationship between an instructor and a student, administration official and a student, or security guard and a student. This is often referred to as "fraternization", and such conduct is prohibited even if

consensual, unless the parties involved are married or involved in an intimate relationship prior to the staff or faculty member assuming a position of authority over the student.

The following relationships are generally discouraged:

Personal relationships between a staff member (including a faculty member) and a student, where the staff member or faculty member is in a position of authority over the student, such as, but not limited to, the relationship between an instructor and a student, administration official and a student, or security guard and a student. A personal relationship includes, but is not limited to: lending students money; employing students for personal services, such as babysitting, unless there is a specifically approved UTTC program for such services; hosting or allowing parties to take place at which students are present, unless specifically approved in advance by UTTC; and similar situations where the staff or faculty member and students are present in a potential compromising situation.

Complaint Procedure

Each official of UTTC is responsible for creating an atmosphere free of discrimination and harassment, sexual or otherwise. Further, employees are responsible for respecting the rights of their coworkers.

An employee should immediately report any incident of discrimination or harassment (sexual or otherwise), to the appropriate supervisor or to the Human Resources Director. Examples of harassment include (but are not limited to):

- Any job-related harassment based on an employee's sex, race, national origin, disability, or any other factor.
- An employee feels he or she has been treated in an unlawful, discriminatory manner.
- If the employee believes it would be inappropriate to discuss the matter with the appropriate supervisor or with the Human Resources Director, he or she may report the incident directly to the next person in the administrative chain of command, who could be the department director, Vice President or the President of the College, as may be appropriate. The person to whom the incident is reported will be responsible to provide the necessary information to the Human Resources Director to begin the appropriate investigation.

It shall generally be the responsibility of the Human Resources Director to investigate the matter, unless the employee believes it would be inappropriate for that person to do so. Each complaint made by any employee will be kept confidential and only be revealed to those persons authorized to investigate the complaint or to decide what remedies should be provided to the complaining employee, if any.

UTTC prohibits any form of retaliation against any employee for filing a bona fide complaint under this policy or for assisting in a complaint investigation. However, if, after investigating any complaint of harassment or unlawful discrimination, UTTC determines that the complaint is not bona fide or that an employee has provided false information regarding the complaint, disciplinary action may be taken against the individual who filed the complaint or who gave the false information, in accordance with the disciplinary procedures stated in Section 7-1 of the Employee Handbook.