IT Policy Guide

For details on the UT Campus IT Policies, check out the CIO/ IT Policies page+

NPL IT Policy Guide

Last update: December 5, 2014

Acceptable use

The policies outlined here cover the use of NPL-owned information technology (IT) resources (for a definition of the term “information technology resources”, see the ITS Glossary). If you log onto a NPL computer or access IT resources belonging to NPL from a non-NPL computer, you are presumed to be aware of and in agreement with these policies as well as UT’s Acceptable Use Policy and other UT IT policies. You also are responsible for ensuring that any students, volunteers, or temporary employees who are under your direct supervision are aware of and in compliance with these policies. Violation of these policies may result in penalties ranging from verbal warnings to criminal prosecution.

1. Limitations on privacy of files and emails: UT and NPL consider your My Documents folder, UT mailbox, and WebSpace storage area to be private, and do not routinely monitor them. However, it is impossible to guarantee that no one will ever become aware of file or email content. For example, desktop support personnel and administrators sometimes have to open files or mailboxes in order to diagnose problems or fulfill user requests, and may become aware of their contents in the process. Files stored on UT computers or network shares and email on UT servers may be subject to subpoenas, search warrants, or open records requests. The NPL administration also has the right to review your files or emails if you are out sick or on vacation for an extended period and we need to recover work-related materials in order to avoid delays in departmental business processes.
2. You are responsible for helping to maintain the security of the resources that you use.
    a. Anything that happens under your logon ID is your responsibility, regardless of who was sitting at the keyboard at the time it occurred.
        i. Passwords and logon IDs that are intended for your sole use may not be shared with other users.
        ii. Under normal circumstances, you should not allow other people to use your computer while you are logged on. If you judge that it is necessary to allow someone else to use your computer, the use should be as brief as possible and you are responsible for monitoring it.
        iii. Computers should be locked or logged off when you expect to be away from them for more than a few minutes.
        iv. Computers should be logged off when you expect to be absent for an extended period.
    b. You are expected to be aware of and apply UT’s Data Classification Standard and associated rules and guidelines relating to protection of work-related data. The following is a brief summary of particularly important points:
        i. Current ITS policy requires the hard drives of all UT laptops to be encrypted, regardless of whether sensitive data is stored on them. Encryption for computers covered by the ITS contract is managed by our ITS support team. For non-contract computers, see the Approved Encryption Methods page. Our department’s customized installer for SecureDoc can be obtained from the NPL TSC.
        ii. Category-I data should not be stored on portable devices (e.g.: removable drives, PDA’s, cell phones) unless it cannot be avoided. If such data has to be stored on a portable device, the file(s) must be encrypted and should be removed from the device as soon as possible. The Approved Encryption Methods page lists the available encryption methods for various portable devices.
        iii. Before storing Category-I data on a portable device or on any personally owned device, ITS policy requires that you get permission in writing from the owner of the data. At a minimum, this means seeking approval from your immediate supervisor and NPL’s director; in some cases, people in other departments may need to be consulted as well.
        iv. If you frequently send or receive email containing Category-I data, we recommend obtaining and installing a University of Texas digital certificate. There is no charge for this service. For sending highly sensitive data to other UT personnel, we recommend using UT’s Secure Messaging System.
    c. Non-UT email services may not be used for work-related email. This is true even if the underlying email address is one provided by UT. The email options available to you depend on your relationship to UT:

Navigation:

Next

Home

Overview Page

Sources of additional information:

- Ann Molineux, NPL Curator
- Angella Thompson, Curatorial Assistant

Primary Author:

- Melissa Winans, TNSC Technical Support Coordinator (TNSC TSC)

Content Editor

- Angella Thompson

Information Technology Services links:

- Help Desk
- Glossary
- Security and Awareness compliance module (CW 170)
- Services and Prices
- Network Operations Manual
- Accounts for Individuals (IF Accounts)

Information Related to Data Protection

- Data Classification Standard
- Approved Encryption Methods for Portable Devices
- Digital Certificates
- Protecting Data on Vulnerable Devices
- Secure Messaging System

UT Email Services & Communication Guidelines

- Austin Exchange Messaging Service (AEMS)
- UTmail
- UT Institutional Rules, Chapter 13: Speech, Expression, and Assembly
- UT Social Media Guidelines
- Virtual servers

UT Software and Special Discounts

- BevoWare

i. Students and student workers have the option of using UTmail (a Google-supported service) for work-related email, but also may continue to use a non-UT account as their official address.
ii. Faculty and staff will be expected to use the Austin Exchange Messaging Service (AEMS), if they routinely handle Category I data or any data which must remain on US soil, or if they use digital certificates or email encryption. A plan is underway to allow staff whose email does not typically involve any of the considerations outlined above to use UTmail (a GoogleApps service) instead, but this has been delayed pending resolution of a few legal issues. Staff wishing to use UTmail should get approval in writing from the director, with a copy to the NPL TSC.

d. Access to NPL IT resources by persons other than permanent NPL staff must be authorized in advance.
   i. Authorization requests should be made by email and routed through the NPL TSC. Turnaround time on requests typically is short, but we recommend getting requests in before the last minute. The request should give the individual’s full name, EID, role in your department, and a list of the resources to which you wish this person to have access. Individuals who do not have an EID should use the UT EID Self-Service Tools to obtain one.
   ii. Authorizations should be revoked promptly when no longer needed, or when the individual’s connection to NPL ends. We do not recommend keeping people who currently are inactive but may be back someday on the active list; it is easy to re-authorize them later if necessary.
   iii. Volunteers and other people who lack a formal affiliation with UT, and whose work requires regular access to NPL IT resources, should have Affiliated Worker appointments in the HRMS system.

3. Remember that network resources are limited.
   a. Activities which have the potential to use a lot of network bandwidth (e.g.: serving streaming video, peer-to-peer applications, web servers, data servers) require prior approval from the NPL TSC, the director, and possibly from ITS.
   b. Any increase in the total number of computers, printers, or other devices to be permanently plugged into the wired network requires advance approval from the NPL TSC. The purpose of this check is to ensure that the network is not overloaded by the increased demand.
   c. ITS networking policy (page 4) provides that individual users “must not extend university networks by any means … without authorization from Department network personnel or ITS Networking”. Practically speaking, this means that:
      i. You must get approval from the NPL TSC before plugging a switch or similar device into the wired network to allow a single outlet to support multiple devices. The purpose of this check is to maintain a record of where switches have been added and ensure that the network is not overloaded by the increased demand.
      ii. The addition of non-ITS wireless access points or wireless routers is strictly forbidden. If you believe that there is a need for wireless service in your area, contact the NPL TSC for assistance in arranging for ITS-managed service.
4. Limited use of NPL resources for personal purposes is permitted with the following restrictions:
   a. Personal files and email that are stored on UT computers, network shares, or email servers are subject to the same limitations on privacy as work-related files and email, including being subject to open records requests. This is true even if the service is being paid for using an ITS Individually Funded Account. We strongly advise finding some other place to store confidential personal data.
   b. Your personal use should not result in direct cost to NPL, including, but not limited to, printing and storage costs. ITS services for which there is a charge (including disk storage) should be paid for using an ITS Individually Funded (IF) Account.
      i. Personal files may not be stored in your NPL-funded My Documents folder, or in other NPL-funded shares on Austin Disk Services. Alternative storage locations include your computer’s hard drive (but only if the total volume of files does not impact the computer’s functioning) or a personal share paid for by an ITS IF Account.
      ii. Printing of personal documents on NPL printers should be limited to urgently needed items.
      iii. Although UT policy does not forbid using UT email addresses for personal mail, NPL advises against doing so. It is difficult to apply the “incidental use” policy to email; once you send a message from a particular address, your correspondent tends to think of that as your identity, and all further correspondence to/from that individual flows through that path. This has the potential to create a considerable draw on both storage space and user time. If you do choose to use your UT email address for personal correspondence, all personal mailboxes should be stored on either your own computer or a share paid for by an ITS IF Account.
   c. Your personal use should not interfere with the normal performance of your duties, or negatively impact other users’ access to NPL resources.
   d. Any personal use must be in compliance with UT’s Acceptable Use Policy.
5. Use of NPL IT resources from a non-UT computer is subject to all of the policies that apply to use of these resources while at work, as well as the following special rules:
   a. Non-UT computers that are used to access NPL computers and data should be up to date on critical operating system patches, have up to date virus protection (Microsoft Forefront is available at no charge from BevoWare), and have a functional firewall.

- ITS Software & Hardware page

b. Access to data stored on Austin Disk Services requires use of one of UT’s VPN Clients or the IPSec configuration package (both available from BevoWare).
c. If you frequently bring a non-NPL computer to work and plug it into an Ethernet port in one of our buildings, we need to know about it. Please inform the curator or NPL TSC.

6. Use of social media by faculty and staff is subject to the following limitations:
    a. UT’s rules about speech and expression give faculty and staff a wide degree of latitude to express their opinions as long as they are clearly identified as personal opinion rather than UT policy. Be sure to read the “For Faculty and Staff” section of the Social Media Guidelines before posting.
    b. Use of social media for a work-related purpose must be approved in writing by your department head and the director. Users will be expected to adhere to the Social Media Guidelines.

Funding for IT costs

Each NPL department is responsible for expenses related to the computers, software, data storage, and other IT resources used by its staff, students, and volunteers. At the beginning of FY 2010-2011, departmental budgets received a permanent transfer of funds to offset these costs. Prices for most ITS-provided services are listed on the ITS Price List page. The NPL TSC can provide assistance in pricing non-ITS goods and services.

1. Each department is free to decide how its IT funds will be allocated. As outlined in other sections, some changes in services may require the approval of one or more people outside of the department.
2. Departmental budgets must bear the cost of any expenses over and above the original budget allocation. Exceptions may be granted on a case by case basis for emergencies or cost sharing.
3. If a department’s IT costs decline due to changes in usage or prices, the surplus funds remain with the department. These surplus funds may be reallocated as the department sees fit. However, IT funds which the department chooses to divert to non-IT purposes will not be replaced with new funding in future years.
4. Departments have the option of “banking” IT funds or budget surpluses with NPL for anticipated future IT expenses. For details, check with the Director for Museum Operations.

Computers and computer support

Departments have the option of participating in NPL’s ITS Desktop Support contract (listed as “ITS User Services” in the ITS price list), or of managing some or all of their computers themselves. A summary of each option appears below; contact the NPL TSC if you need more information.

1. Contract computers are entitled to a broad range of support for software and hardware installation, updates, and troubleshooting. Support prices are based on the criteria listed on the ITS User Services pricing page. Any computer which fits two or more of the listed criteria may be classified as “complex” and charged at a substantially higher annual rate (we have been informed that ITS considers ArcGIS to be a “complex third-party application”). NPL’s support contract is managed by the NPL TSC, who should be consulted about service problems, decisions to add, remove, or replace contract computers, and changes in the contract requirements. Neither ITS nor the NPL TSC guarantee to provide support for computers or other devices purchased without a compatibility check, or for which up to date drivers are not available.
    a. Purchases of contract computers should be routed through the NPL TSC, who will work with the department or user to ensure that the computer meets the buyer’s needs while remaining in compliance with contract requirements. The preferred source for contract computers is an ITS-approved list of Dell configurations which are available at deeply discounted prices. Exceptions can be requested for cases where there is a functional reason for purchasing something else (please note that ITS may classify such computers as “complex”).
    b. The ITS contract calls for a five-year replacement cycle on all contract computers. Computer ages are checked at the end of each fiscal year, and the owning department will be asked to decide whether to replace the computer, drop it from the contract, or keep it on the contract at a potentially higher price (age is one factor than may cause a computer to be reclassified as “complex”). We strongly recommend replacing computers after the fifth year, both for reasons of functionality and to reduce your financial risk in case of hardware failures. However, the final decision is yours.
    c. The ITS contract does not cover repair costs, which must be paid by the department. To insulate your budget against unexpected repair bills and lost time, we strongly recommend opting for the 5-year basic on-site repair contract for all new Dell computers and adding the damage-protection option for laptops. Similar on-site repair options may also be available from other vendors.
    d. The ITS contract specifies that individual users may not have administrative accounts on their computers. Exceptions can be requested for computers which frequently operate off the UT network. To request an exception, send an email to the NPL TSC outlining the reasons for your request. Having an administrative ID on your computer may result in your computer being charged the higher “complex” rate.
    e. Before making modifications or additions to managed computers or their software, we strongly recommend requesting a compatibility check from the NPL TSC. Neither ITS

nor the NPL TSC guarantee to provide continued support for computers which are modified without a compatibility check. Please note that software packages which have the potential to require extra support from ITS may cause the computer to be reclassified as “complex”.

    f. Removal of a computer from the management contract requires prior approval from the department head and the NPL TSC. For purposes of documentation, the request should be made via email, and should identify the staff member who will be assigned to manage the computer. The computer will be resigned from the Austin domain, the drive will be wiped, and all software that came bundled with the computer or was purchased later will be turned over to the department. It will then be the department’s responsibility to install a new copy of the operating system, drivers, and other software as needed. Licenses for software that previously was installed on the computer remain the property of the department unless they no longer are needed.

2. Department-managed computers are not eligible for support from ITS or the NPL TSC. However, their users are entitled to the basic level of Help Desk support that is available to all UT staff and students. The managing department is solely responsible for management, tech support, and problem solving.
    a. Department-managed computers can be purchased via procurement card or routed through the NPL purchasing office. Departments have the option of purchasing from the ITS Dell discount list or any other source. For information about vendors with which ITS has blanket purchase orders, see the ITS Software & Hardware page. The NPL TSC can provide advice and information about sources and compatibility issues.
    b. To insulate your department against unexpected repair bills, we strongly recommend opting for the 5-year basic on-site repair contract for all new Dell computers and adding the damage-protection option for laptops. Similar on-site repair options may also be available from other vendors.
    c. A specific staff member should be assigned as the manager of each department-managed computer. This can be a single person for all computers in the department or a separate person for each computer. The person designated as manager is responsible for familiarizing him/herself with applicable UT and NPL policies and guidelines, and for ensuring that each computer is in compliance with them.
    d. A department-managed computer may be joined to the “Austin” domain or be managed locally. If joined to the domain, it will have access to the EID logon system, but also will be subject to many of the same security and policy restrictions as contract computers. If not joined to the domain, a computer’s security settings and logon IDs must be managed locally by the designated staff member. Non-domain computers will require the VPN client or IPSec (available from the BevoWare site) to access certain network resources, including Austin Disk Services.
    e. The computer’s manager and the NPL TSC are jointly responsibility for the computer’s presence on the UT network. The manager should provide the NPL TSC with the information listed below for each department-managed computer.
    f. Adding a department-managed computer to the ITS contract requires prior approval from the department head, the NPL TSC, and possibly from ITS. For purposes of documentation, the request should be made via email. To ensure compliance with contract standards, it may be necessary to wipe the drive and install a fresh image of the operating system and other software. All software that came bundled with the computer or was purchased later should be turned over to the NPL TSC. The department also should provide the TSC with documentation that it holds valid licenses for all software that did not come bundled with the computer.

Required information for department-managed computers, personal computers, and other networked devices being used on the NPL network:

- Computer name assigned by you during the operating system setup, or device type if this is not a computer
- MAC Address(es) (see http://www.wikihow.com/Find-the-MAC-Address-of-Your-Computer for instructions on how to find this)
- IP Address (if statically assigned)
- UT Inventory Tag (if assigned)
- System Serial Number (if it exists)
- Name of the staff person responsible for managing the computer or device
- Name of primary user (if different from the manager)
- Building and room
- Ethernet port number (if plugged into a wired port) . This 4-digit number is printed on a label attached to the cover plate of the port

For computers or other devices purchased with NPL funds (including grants):

- Item cost
- How purchased (procurement card or purchase order), when, and by whom
- Brand and model

Hardware other than computers

Decisions about what to purchase, and from what source, are at the discretion of the department. The NPL TSC can provide advice and information about sources and compatibility issues. Neither ITS nor the

NPL TSC guarantee to provide support for devices purchased without a compatibility check, or for which up to date drivers are not available.
Software: Where possible, we recommend using software which will be compatible with what other NPL staff are using. However, the final decision about what to use is at the department's discretion. The NPL TSC can provide information about compatibility and sources for educational discounts, and may have no- or low-cost licenses already available for some products. Neither ITS nor the NPL TSC guarantee to provide support for software purchased without a compatibility check.

1. Software installed on contract computers is subject to periodic inventories and compatibility checks. We cannot prevent individual users from installing software that does not require administrative privileges. However, we reserve the right to remove user-installed software at any time if security, compatibility, or functionality issues arise.
2. All software installed on NPL computers must have a valid license. Licenses for contract computers are managed by the NPL TSC. Licenses for department-managed computers are managed by the department, but are subject to periodic audits for compliance. Departments have the option of availing themselves of existing site licenses managed by the NPL TSC or of making their own purchases.
3. Departments have the option of moving software packages to a different computer at any time as long as doing so does not violate the provisions of the licensing agreement. Licenses that are no longer needed can be returned to NPL's central pool of unallocated licenses, or retained for future use. When a computer is replaced, software that was installed on the old computer can be reinstalled on the new one, assuming that the licensing agreement permits licenses to be transferred.

   Check with the NPL TSC about specific licensing questions.

Data storage and backups

Individual users or departments are responsible for setting a backup policy and assuring that it is adhered to. The Information Security Office offers guidance on planning a backup strategy and the NPL TSC also can provide advice and assistance in developing backup strategies. In cases where backups are not part of the storage cost, backup costs are paid by the department. Austin Disk Services ITS now offers a centralized backup service at a nominal cost for those who do not wish to maintain their own backup media. Check with the NPL TSC for details.

1. Austin Disk Services: This is the preferred storage location for most data because backups are provided by ITS at no additional charge. The minimum retention period for these backups is two weeks. If archival copies of Austin Disk services files need to be kept longer than this, you are responsible for creating copies in another secure location.
   a. My Documents folders should be used only for files which do not need to be accessible to other users. The initial allocation for a new user's My Documents folder is 1GB, and the maximum possible allocation is 20GB. Increases in a user's My Documents allocation must be requested in writing, with copies to the department, the director, and the NPL TSC, and must include a justification for the increase.
   b. Departmental bulk storage folders should be used for files to which multiple users in the department or within NPL need to have access. Practically speaking, the only limit to the bulk storage is the department's budget, but storage allocations over the maximum allocation size (currently 2,000GB) may require splitting the data between multiple folders. Increases in departmental bulk storage allocations must be requested in writing, with copies to the department, the director, and the NPL TSC.
3. Other UT-based storage options: Departments or individual users may elect to use other storage locations. Doing so requires the approval of the director and the NPL TSC.
   a. The department or user is responsible for ensuring that backups of their data meet the standards set by the department. NPL data that is stored in locations other than Austin Disk Services, and backup costs are paid by the department. ITS now offers a centralized backup service at a nominal cost for those who do not wish to maintain their own backup media. Check with the NPL TSC for details.
   b. Other UT departments may provide storage for data related to certain projects. Backup policies vary from department to department; you are responsible for finding out what they are, and if necessary making provisions for additional backups. Your department, the director, and NPL TSC must be notified in writing of the details of any such arrangement.
   c. Large-scale bulk storage is provided by ITS for departments or individuals that need 1,000GB or more and are willing to maintain an ITS virtual server to manage it. Because ITS does not provide backup service, the annual cost of this storage is much lower than Austin Disk. However, the department or individual user must be willing to manage the server and do backups.
   d. Local hard drives of NPL computers can be used for storage of data related to programs stored on that computer. Backups are the responsibility of the department or individual user.
4. Non-UT storage locations: Storage of primary or backup copies of NPL data on a non-UT service requires prior approval from the director and the NPL TSC.

ITS_sigPage.doc

Computer Lab Main page Home Next