

Computer Policies

Dept. of Statistics, Texas A&M University
Revision: June 11, 2010

In order to comply with Texas A&M University and State of Texas rules governing computer use, the Department of Statistics has developed the following set of rules governing access to its computing system. Users of the computing facilities are expected to abide by the following set of rules.

- Policies are regularly updated. The latest version of this document can be found here:

<http://www.stat.tamu.edu/policy>

- Users agree to abide by all laws, rules, regulation and policies that govern the use of computers at Texas A&M University. See here to get started:

TAMU Rules: <http://rules-saps.tamu.edu>

TAMU Student Rules: <http://student-rules.tamu.edu>

[Texas Administrative Code](#), but especially [TAC Chapter 202](#)

Please see later in this document for some specific references to computer related rules.

- Users are advised that almost all university documents (including email) are subject to the **Texas Open Records Act** and could, after proper procedure is followed, become public.
- When possible, IT support requests should be sent by email to support@stat.tamu.edu. The IT staff must be notified at least one week ahead of time regarding all requests for computing and related equipment (laptops, projectors, etc.). If you do not know the precise time and location, tell us as much as you do know, such as the approximate date, time and location.
- Sharing accounts with another user or allowing another user to use your account is strictly prohibited. Violation of this policy may result in account suspension or other disciplinary action. Using multiple accounts to bypass departmentally imposed account and computer usage restrictions is considered a severe violation of the rules.
- Security policies:
 - You may not attempt to subvert any security measures on any computer system (including file permissions, access controls, automatic patching, anti-virus software, firewalls, logging software, monitoring software, etc.).
 - You may not attempt to interfere with the operation of computing facilities.

- You may not probe the computer system for vulnerabilities or perform network, computer or file system scans on resources that do not belong to you.
 - Computer use may be monitored.
- All computer systems under the administrative control of the IT Staff are scheduled for maintenance and downtime on the first Saturday morning of each month. Simulations and other tasks may be interrupted, killed or deleted on that day without further notice.
- All software, multimedia or data installed, downloaded or stored on departmental computers must be properly licensed or purchased. You may not install software on our systems unless you have a valid license to do so. You may not download mp3 or other music, video, pictures or data files unless you own them or are otherwise properly authorized to use them.
- Backup policy:
 - Some of the data on our system is backed up on a regular schedule (generally daily or weekly). Please contact IT support if you want to know if some specific data is being backed up.
 - Backups can and do fail, so we strongly recommend users implement personal backup measures for important material.
 - Backup retention varies depending on the nature of the data, but all backups are subject to deletion after two months.
 - Temporary backups (e.g. system moves, re-installations, etc.) made by IT are subject to deletion after their purpose has been fulfilled. In general we do not keep temporary backups for more than two weeks.
- Document retention (including email) is the responsibility of the individual users. University rules and regulations require documents to be retained for a certain amount of time. The IT staff does not handle document retention and the regular backups are not designed or intended to meet document retention requirements.
- Email policy:
 - Email on this system is filtered. For example, an email that contains viruses, is deemed unsolicited commercial email (i.e. spam), does not follow proper email protocols, contains certain types of high-risk attachments, or is too large may not be delivered to the intended recipient.
 - Quotas are in force on all email accounts. Once an email account is over quota email will not be delivered until the user deletes or moves sufficient email to be under their email quota again.
 - Deleted email (e.g. email stored in folders such as "Trash", "Deleted Items", etc.) may be purged from the system after 30 days.
 - Junk or spam email (e.g. email stored in folder such as "Junk E-Mail", "Spam", etc.), may be purged from the system after 30 days.

- Email accounts are closed for users no longer affiliated with our department. We will forward email to an alternate account. Please email support@stat.tamu.edu to request that email forwarding be enabled for your account.
- Important information concerning the use of our computer system will be periodically distributed by email to all users. Users are expected to access their accounts on a regular basis and, if requested, respond to email concerning your account. Due to the large number of users, we plan to use email contact to verify the activity of user accounts and may use the failure to respond to email as an indication that an account is no longer active.
- All computer accounts expire on October 1 of each year. As long as faculty and staff remain employed by this department and graduate students are currently enrolled students of this department, their computing accounts will be renewed on a year-to-year basis. The exact method of renewal will be made known before the account expires; though for most users the process will be transparent as the department will determine eligibility annually. However, accounts may be closed, modified or deleted without warning for the following reasons:
 1. if a user is found to be ineligible or unauthorized to have a Texas A&M computer account;
 2. if a user's job responsibility changes (requiring a new account or a different level of account access);
 3. if, after repeated attempts, we are unable to contact the account holder; or
 4. at the direction and discretion of the department head.

Please note that all applications for an account used by "affiliated users" need a faculty sponsor.

- All printing may be logged. No multiple copies of any document may be made using public printers. This includes multiple copies of handouts for classes, papers, dissertations, etc. If more than one copy of a document is required, you can use the copier in the workroom (for university-approved purposes) or use a commercial copying service such as Kinko's across the street (dissertations). Some users may have the quantity of printing they can do on departmental printers restricted.
- Due to the Texas A&M firewall, accessing our computing system may require the use of VPN services provided by the university. More information on VPN is available at

http://nis.tamu.edu/Home/Networking/Virtual_Private_Networks.php

In the following section we reference some of the rules and SAP's (Standard Administrative Procedures) that govern the use of computers at Texas A&M and highlight and summarize some of the provisions in the SAP's. If our summary conflicts with the SAP, follow the SAP! At other times we provide additional information and procedures specific to our department:

- The term **Information Resource** is defined in the TAMU SAP's, but among other items it refers to computer systems such as a desktop computer, laptop, server system, PDA, etc. This document may abbreviate **Information Resource** as **IR**.
- Acceptable Use of an Information Resource is described in SAP: [29.01.99.M1.02](#)
 - In general, incidental personal use of an IR is permitted.
 - In general, business use of an IR is not permitted.
- Administrator or Special Access is governed by SAP: [29.01.99.M1.04](#).
 - If you have administrator or special access to an information resource, you must follow the procedures outlined in this SAP. Any reporting requirements need to be done in email to support@stat.tamu.edu.
 - If, by virtue of your own access privileges (e.g. you have administrator access) or by being the custodian of an IR (e.g. a university owned laptop), you give administrator or special access privileges to anyone, you must email support@stat.tamu.edu to report the matter.
- Installation and use of authorized software is governed by SAP: [29.01.99.M1.05](#).
 - You may not use or install licensed software unless you have a valid license to do so.
- Email use is governed by SAP: [29.01.99.M1.08](#).
- Incident management procedures are described in SAP: [29.01.99.M1.09](#).
 - Security incidents such as malicious code detection; unauthorized use of computer accounts and computer systems; theft of computer equipment or theft of information; accidental or malicious disruption or denial of service as outlined in security monitoring procedures, intrusion detection procedures, internet/intranet procedures, and acceptable use procedures must be reported to support@stat.tamu.edu.
- Internet/Intranet use is governed by SAP: [29.01.99.M1.10](#).
 - No university confidential information shall be made available via university web sites without ensuring that material is accessible to only authorized individuals or groups.
 - Most users have a personal web site with the URL:

<http://www.stat.tamu.edu/~userid>

This web site is located in the users Linux home directory `~/`.html and all contents in that directory are by default are publically accessible through the web. Please contact support@stat.tamu.edu if you need help setting up a restricted web site.

- With the exception of a user's public web site and certain shared resources (such as temporary directories), account files should, by default, be protected from the public or unauthorized users. We strongly encourage the user to verify this and to learn how to protect and unprotect files using file system permissions and encryption.
- Network access is governed by SAP: [29.01.99.M1.12](#).
 - You may not attach a network enabled device to the TAMU network without receiving authorization to do so. Authorization might be granted through a login mechanism (e.g. wireless access authenticates access using your NetID). Alternatively, email support@stat.tamu.edu to receive such authorization. You will need to submit a **Network Access Request** form.
 - You may not connect a router, switch, wireless router, etc. to the network, unless you have permission to do so.
- Network configuration is governed by SAP: [29.01.99.M1.13](#).
 - All IP and DNS hostname requests for a Statistics IR on the TAMU network (e.g. a laptop, desktop, network printer, or other network enabled device) must be submitted to support@stat.tamu.edu.
- Passwords and authentication is governed by SAP: [29.01.99.M1.14](#).
 - Passwords are confidential and must not be shared.
 - Passwords used to log in to system that authenticate against the Statistics domain (most Linux and Windows desktop systems in our department) must be changed every 180 days.
 - Password on all other systems containing confidential data (e.g. a laptop containing student grades, etc.) must be changed every 90 days.
 - Passwords protecting confidential data must meet certain complexity requirements. Even though (when possible) we enforce some password complexity, we do not enforce the complexity as required by this SAP. Every user must ensure their password(s) meet the TAMU password complexity requirements.
 - All password protected sites must use encryption such as SSL (e.g. a password protected web site must use https://). Email support@stat.tamu.edu for information on how to force/require SSL use on a web site.

- No confidential information may be made accessible, unless it is encrypted and username and password protected.
- Information security on portable devices is governed by SAP: [29.01.99.M1.16](#).
 - You must protect confidential information on any portable device by passwords, encryption or other means.
 - You must encrypt confidential information on portable devices.
- Information Resource privacy is governed by SAP: [29.01.99.M1.17](#).
- Information Resource security monitoring is governed by SAP: [29.01.99.M1.18](#).
 - All Information Resources may be monitored for security.
 - A user shall not attempt to circumvent security monitoring.
- Information Resource security awareness and training is governed by SAP: [29.01.99.M1.19](#).
 - The university requires users to take periodic online security training courses. The courses are required by the State of Texas and it is important you complete them.
- Information resources rules and procedure regarding malicious code are governed by SAP: [29.01.99.M1.23](#).
 - When appropriate and possible (e.g. Windows PC's or Mac's), IR's must have anti-virus, anti-spyware and firewall software installed and enabled.
 - You must report any malicious code (virus, spyware, etc.) to support@stat.tamu.edu.
- Notification of Unauthorized Disclosure of Sensitive Personal Information is governed by SAP: [29.01.99.M1.24](#).
 - You must email support@stat.tamu.edu if you suspect confidential information has been compromised.
- Peer-to-Peer File Sharing Software is governed by SAP: [29.01.99.M1.25](#).
 - Not all Peer-to-Peer software is illegal, but to ensure compliance with this SAP, you must email support@stat.tamu.edu and receive authorization to install peer-to-peer software on any university owned IR.
- Required Risk Mitigation Measures are governed by SAP: [29.01.99.M1.27](#).

- If you have administrator access to an IR (e.g. a laptop configured to permit you to install software), you must complete either ISAAC-EU or ISAAC on a yearly basis.
 - Data Classification and Protection are the subject of SAP: [29.01.99.M1.29](#).
 - Confidential information is defined in the SAP. The most common form of confidential information users will access are student grades of the classes they teach.
 - Access to confidential information requires special security precaution.
 - No confidential information may be made accessible, unless it is encrypted and protected by username and password.
 - You may not retain or store Social Security Numbers (SSN's) except those that belong to you or your immediate family.
 - All IR must be scanned for SSN's on a yearly basis.
 - Wireless access is governed by SAP: [29.01.99.M1.30](#).
 - You may not attach a wireless router to the TAMU network.
-