

Information Technology Services

TEXAS A&M UNIVERSITY AT QATAR

Information Technology Employee Security Code of Conduct

Information Technology Services (ITS) provides a wide variety of information technology support for Texas A&M University at Qatar, other components of Education City, as well as for various State and Federal agencies, educational institutions, and other approved entities.

Because ITS has unique responsibilities with regard to safeguarding the privacy and security of data for our authorized customers, employees assigned to ITS (full time and part time, including temporary employees and student workers) are expected to adhere to a code of conduct aimed at safeguarding the privacy, use, and security of data. This code of conduct serves to not only inform our employees of their special responsibilities with regard to security and privacy issues, but also to provide our customers with an understanding of our obligations to them as an information technology service provider. These responsibilities include not only our employees' accounts and access, but also those of our authorized end users.

Definitions:

Confidential Information -- Information that is excepted from disclosure requirements under the provisions of applicable state or federal law, e.g. the Texas Public Information Act. Confidential information is not to be disclosed without appropriate authorization.

Owner of an Information Resource – An entity responsible for a business function and for determining controls and access to information resources supporting that business function.

Code of Conduct:

- A. ITS employees are to comply with the information security rules and procedures of Texas A&M University. (See University Rules <http://rules.tamu.edu/>, specifically 24.99.99.M1 "Security of Electronic Information Resources" <http://rules.tamu.edu/urules/200/249999M1.htm>). ITS employees are to also comply with ITS policies and procedures as documented in the ITS Policies and Practices guide at <http://technology.qatar.tamu.edu>.
- B. Data and information that is specifically addressed by various privacy laws (e.g. Family Educational Rights and Privacy Act (FERPA), The Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA)) shall be treated as confidential information and in accordance with those laws. Any unauthorized/inappropriate disclosure of confidential information is to be reported to the office of the Chief Information Officer - Qatar.
- C. Confidential information stored on thumb drives or USB flash memory devices shall be encrypted. This protects the confidentiality of the information should the device be lost.
- D. Programs, files, E-mail, telecommunications logs, or any other data belonging to others will not be accessed, altered, or copied without prior authorization from the owner. Routine maintenance is exempted from this requirement. In most cases where system integrity is an issue, immediate intervention may be taken. Such intervention is to be limited in its scope and is to be reported to the employee's respective Director as soon as practical. Except as necessary to perform your assigned duties, system/application data should not be divulged unless permission is granted by the owner. In general, authorizations from the owner must be in writing.
- E. Computer and telecommunications accounts:
 1. Computer and telecommunications accounts are to be used only by the authorized user of the account.

2. Your computer and telecommunications accounts are to be used only to support the completion of your assigned duties as an employee. Incidental personal use of computing resources is permitted as defined in University Rules 33.04.99.M3 (<http://rules.tamu.edu/urules/300/330499m3.htm>). Incidental personal use of other TAMUS property is permitted as defined in Texas A&M University System Policy 33.04 (<http://sago.tamu.edu/policy/33-04.htm>). Personal use of computing resources, which cannot be categorized as incidental, should be guided by System Ethics Policy 07.01.4.4 "Other TAMUS Equipment" (<http://sago.tamu.edu/policy/07-01.htm>).
3. Restrictions associated with the computer account authorized for your use will be followed.
4. Computer accounts, whether for individuals or batch programs, are created and managed through the IT Administrator. ITS employees are not to create accounts on any platform, for any reason, nor are they to elevate the privileges of an account unless requested in writing by the IT Administrator and data owner.

F. Account passwords:

1. Employee's assigned passwords for accounts (computing and telecommunications), are not to be given to any other person.
2. Each employee is responsible for selecting and changing his or her passwords in accordance with the information security rules and procedures of Texas A&M University at Qatar.
3. Each employee will not request a customer to disclose his or her password to anyone. If the requested service is impossible to provide without the customer's password, then the customer must change the password as soon as the ITS employee has completed the requested service.
4. Manual password resets are the responsibility of the IT Administrator. ITS employees are not to reset the passwords of any account, regardless of whether the accounts are user accounts or accounts for batch programs.

G. In those cases where law enforcement agencies (e.g., University Police, other police, FBI) request access in conjunction with an investigation, the request should be in writing (e.g., subpoena, court order) and reported to the office of the Chief Information Officer – Qatar upon receipt and before any action is taken.

H. Information related to the security of customer systems is to be treated as confidential information and will not be discussed or divulged except as necessary to perform your assigned duties.

I. Information regarding the secure operation of the information technology infrastructure will not be divulged to anyone without a demonstrated *need-to-know*.

J. Each employee must comply with software license and copyright restrictions and protocols.

ITS employees who violate this code of conduct may be subject to disciplinary action to include termination. Depending on the seriousness of the violation, such actions may also include financial restitution for unauthorized use of services as well as civil and criminal penalties.

Certification

I have read the preceding Employee Code of Computing Ethics and understand the standards of conduct expected of me as an employee of Texas A&M University at Qatar.

Name, printed

UIN

Signature

Date