

**UNIVERSITY PROCEDURES**  
**TEXAS A&M UNIVERSITY-CORPUS CHRISTI**

---

**21.01.06.C2.04 Administrator/Special Access**

*Approved June 11, 2007*

*Supplements University Rule 21.01.06.C2*

1. GENERAL

Technical support staff, security administrators, system administrators, and others may have special access account privilege requirements compared to typical users. Administrator accounts and other special access accounts have extended and overarching privileges in comparison with typical users. Thus, the granting, controlling, and monitoring of these accounts is extremely important to an overall security program. The purpose of the university administrator/special access management procedure is to establish the process for the creation, use, monitoring, control, and removal of accounts with special access privilege.

2. APPLICABILITY

This university procedure applies to all information resources managed by the university.

The purpose of the implementation of this university procedure is to provide a set of measures that will mitigate information security risks associated with administrator/special access management. There may also be other or additional measures that will provide appropriate mitigation of the risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the information resource owner or their designee. In accordance with Texas Administrative Code 202 - Information Security Standards, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided in this university procedure based on information security risk management decisions and business functions. Such risk management decisions must be documented in the annual security assessment report (See University Rule 21.01.06.C2 Security of Electronic Information Resources).

The intended audience is all university staff responsible for information resources.

3. DEFINITIONS

Please refer to University Procedure 21.01.06.C2.01 Definitions.

4. PROCEDURES

4.1. University departments must submit to Media and Computer Services a list of administrative contacts for their systems that are connected to the university network.

## **UNIVERSITY PROCEDURES**

### **TEXAS A&M UNIVERSITY-CORPUS CHRISTI**

---

- 4.2. All users must sign the university information resources security acknowledgement form and nondisclosure agreement before access is given to an account.
- 4.3. All users of administrative/special access accounts must have account management instructions, documentation, training, and authorization.
- 4.4. Each individual that uses administrative/special access accounts must refrain from abuse of privilege and must only do investigations under the direction of the Information Resource Manager or representatives of this office.
- 4.5. Each individual that uses administrative/special access accounts must use the account privilege most appropriate with work being performed (i.e., user account vs. administrator account).
- 4.6. Each account used for administrative/special access must meet the University Procedure 21.01.06.C2.15 Password.
- 4.7. The password for a shared administrator/special access account must change when an individual with the password leaves the department or university, or upon a change in the vendor personnel assigned to the university contract.
- 4.8. In the case where a system has only one administrator there must be a password escrow procedure in place so that someone other than the administrator can gain access to the administrator account in an emergency situation.
- 4.9. When temporary access accounts are needed for internal or external audit, software development, software installation, or other defined need, they:
  - (1) must be authorized by the system owner,
  - (2) must be created with a specific expiration date, and
  - (3) must be removed when work is complete.

#### **5. CONSEQUENCES FOR VIOLATIONS**

All university employees to include staff, tenured and non-tenured faculty, graduate assistants, student workers, interns, guests, volunteers, and probationary, temporary, or wage employees as well as contractors, consultants, and vendors required to adhere to this university procedure may be subject to criminal, civil, or disciplinary actions consistent with federal and state laws, system policies, and university rules.

Individuals found in violation of this university procedure are subject to loss of access privileges to university information resources (e.g. servers, workstations, email, etc). In

**UNIVERSITY PROCEDURES**  
**TEXAS A&M UNIVERSITY-CORPUS CHRISTI**

---

addition, contracts associated with contractors, consultants, or vendors are subject to review and possible termination. Any device, system, or software found in violation of this procedure may be confiscated and temporarily stored by the Information Resources Manager or a representative of the office.

Additional guidance may be found, but is not limited to, the following policies and rules.

- Texas A&M System Policy
  - 01.03 Appointing Power and Terms and Conditions of Employment
  - 07.01 Ethics Policy, TAMUS Employees
  - 32.02 Discipline and Dismissal of Employees
  - 32.02.02 Discipline and Dismissal Procedure for Nonfaculty Employees
  - 33 Employment, Standards of Conduct
- Texas A&M University-Corpus Christi Rule
  - 12.01.99.C3 Faculty Dismissals, Administrative Leave, Non-Reappointments and Terminal Appointments
  - 13.02.99.C1 Student Disciplinary Proceedings

Contact for Interpretation: Assistant Vice President for Technology

Office of Responsibility: Executive Vice President, Finance & Administration