

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

---

**21.01.06.C2.03 Account Management**

*Approved June 11, 2007*

*Supplements University Rule 21.01.06.C2*

1. GENERAL

University information resources are strategic assets which, being property of the State of Texas, must be managed as valuable state resources. Access to university information resources is normally controlled by a logon ID associated with an authorized account. Proper administration of these logon IDs is very important to ensure the security of confidential information and normal business operation of university managed and administered information resources.

2. APPLICABILITY

This university procedure applies to university information resources that store or process mission critical and/or confidential information.

The purpose of the implementation of this university procedure is to provide a set of measures that will mitigate information security risks associated with account 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 for this university procedure includes, but is not limited to, all information resources data/owners, management personnel, and system administrators.

3. DEFINITIONS

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

4. PROCEDURES

4.1. All accounts created must have an associated request and approval that is appropriate for the university system or service.

## **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 accounts must be uniquely identifiable using the assigned user name.
- 4.4. All default passwords for accounts must be constructed in accordance with the University Procedure 21.01.06.C2.15 Password.
- 4.5. All accounts must have a password expiration that complies with University Procedure 21.01.06.C2.15 Password.
- 4.6. All new user accounts that have not been accessed within 30 days of creation shall be disabled.
- 4.7. Faculty and staff terminating employment with the university may request that that their email and we account access be continued for a period of time. Written requests shall be considered on an individual basis and must be approved by both the former employee's immediate supervisor and the system administrator.
- 4.8. System Administrators or other designated staff:
  - (1) are responsible for removing the accounts of individuals that change roles within the university or are separated from their relationship with university;
  - (2) must have a documented process to modify a user account to accommodate situations such as name changes, accounting changes, and permission changes;
  - (3) must have a documented process for periodically reviewing existing accounts for validity;
  - (4) are subject to independent audit review;
  - (5) must provide a list of accounts for the systems they administer when requested by authorized university management, and
  - (6) must cooperate with authorized university management investigating security incidents.

#### **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

## **UNIVERSITY PROCEDURES**

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

---

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 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