

# CITRUS COMMUNITY COLLEGE DISTRICT GENERAL INSTITUTION

## **AP 3721 COMPUTER AND NETWORK ACCOUNT AND PASSWORD MANAGEMENT**

### **1.0 Purpose**

The purpose of this procedure is to establish a standard for the administration of computer and network accounts that facilitate access or changes to Citrus Community College District institutional data and the requirements for acceptable password selection and maintenance related to those accounts. Accounts that access electronic computing and information resources require prudent oversight. An account, at minimum, consists of a user ID and a password that grant access to some set of services and resources.

Passwords are the most frequently utilized form of authentication for accessing a computing resource. Due to the use of weak passwords, the proliferation of automated password-cracking programs, and the activity of malicious hackers and spammers, passwords are very often also the weakest link in securing data. Password use must therefore follow the procedure guidelines listed below.

This procedure establishes guidelines for issuing accounts, creating password values, and managing accounts. It provides guidance on creating and using passwords in ways that maximize security of the password and minimize misuse or theft of the password.

### **2.0 Scope**

This procedure applies to anyone accessing systems that hold or transmit district data. Systems include, but are not limited to: personal computers, laptops, district issued cell phones, and small factor computing devices (e.g., PDAs, USB memory keys, electronic organizers), as well as district electronic services, systems and servers.

This procedure also applies to those responsible for the management of user accounts or management of access to shared information, network devices or information that can be held within a database, application or shared file space. This procedure covers departmental accounts as well as those managed centrally.

## 3.0 Procedure

### 3.1 Issuing Computer and Network Accounts

The owners of district data shall make decisions regarding access to their respective data (e.g., the Dean of Admissions and Records will determine who has access to registration data, and what kind of access each user has). Account setup and modification shall require the signature of the requestor's supervisor.

Managers shall make written requests to the Technology and Computer Services (TeCS) Department for employee access to district computer resources. To maintain system security, managers shall immediately notify the TeCS Department in writing when system access is no longer required or authorized for an employee. Managers shall be responsible to provide general supervision of departmental employee adherence to the rules and procedures presented herein.

The TeCS Department shall issue a unique account to each individual authorized to access that networked computing and information resource. It is also responsible for the prompt deactivation of accounts when necessary, i.e., accounts for terminated individuals shall be removed/disabled/revoked from any computing system at the end of the individual's employment or when continued access is no longer required. Also, the accounts of transferred individuals may require removal/disabling to ensure changes in access privileges are appropriate to the change in job function or location.

When establishing accounts, standard security principles of "least required access" to perform a function must always be used, where administratively feasible. For example, a root or administrative privileged account must not be used when a non-privileged account will do. Account passwords shall not be emailed. The date when the account was issued should be recorded in an audit log.

The identity of users must be authenticated before providing them with account and password details. If an automated process is used, then the account holder should be asked to provide several information items that in totality could only be known by the account holder. In addition, it is highly recommended that stricter levels of authentication (such as face-to-face) be used for those accounts with privileged access (e.g., user accounts used for email do not require an identity validation process as thorough as for those user accounts that can be used to modify department budgets).

## 3.2 Managing Accounts

The data owner shall review all accounts at least annually to ensure that access and account privileges are commensurate with job function, need-to-know, and employment status. The TeCS Department may also conduct periodic reviews for any system connected to the district network.

All guest accounts (for those who are not official members of the district community) with access to district computing resources shall contain an expiration date of one year or the work completion date, whichever occurs first. All guest accounts must be sponsored by the appropriate authorized member of the administrative entity managing the resource.

## 3.3 Password Creation and Maintenance

All passwords (e.g., email, web, desktop computer, etc.) should be strong passwords and should follow the guidelines below. In general, a password's strength will increase with length, complexity and frequency of changes.

Greater risks require a heightened level of protection. Stronger passwords augmented with alternate security measures such as multi-factor authentication, should be used in such situations. High-risk systems include but are not limited to: systems that provide access to critical or sensitive information, controlled access to shared data, a system or application with weaker security, and administrator accounts that maintain the access of other accounts or provide access to a security infrastructure.

All passwords must meet the following guidelines, except where technically infeasible:

- Be at least eight alphanumeric characters long.
- Contain digits or punctuation characters as well as letters (e.g., 0-9, !@#\$%^&()\_~-=`{}".')
- Contain both upper and lower case characters (e.g., a-z, A-Z).
- Not be solely based on easily guessed personal information, names of family members, pets, etc.

To help prevent identity theft, personal or fiscally useful information such as Social Security or credit card numbers must never be used as a user ID or a password. All passwords are to be treated as sensitive information and should never be written down or stored online unless adequately secured. Do not use the password storage feature offered on Windows or other operating systems as this feature creates a password file that is vulnerable to hackers.

The following guidelines describe password usage.

- Passwords should not be inserted into email messages or other forms of electronic communication.
- Passwords that could be used to access sensitive information must be encrypted in transit.
- It is recommended that passwords be changed at least every six months and some district systems will enforce a password change.
- Individual passwords should not be shared with anyone, including administrative assistants or Technology and Computer Services (TeCS) Department staff. Necessary exceptions must have a primary responsible contact person. Shared passwords used to protect network devices, shared folders or files require a designated individual to be responsible for the maintenance of those passwords, and that person will ensure that only appropriately authorized employees have access to the passwords.
- If a password is suspected to have been compromised, it should be changed immediately and the incident reported to the TeCS Department.
- The TeCS Department or its delegates, with the cooperation and support from the appropriate system administrator, may perform password cracking or guessing on a periodic or random basis. If a password is guessed or cracked during one of these scans, the password owner will be required to change it immediately.

#### 3.4 Desktop Administrator Passwords

In addition to the password guidelines listed above in this procedure, the following apply to desktop administrator passwords, except where technically and/or administratively infeasible:

- These passwords must be changed at least every six months.
- Where technically and administratively feasible, attempts to guess a password should be automatically limited to ten incorrect guesses. Access should then be locked for a minimum of ten minutes, unless a local system administrator intercedes.
- Failed attempts should be logged, unless such action results in the display of a failed password. It is recommended that these logs be retained for a minimum of 30 days. Administrators should regularly inspect these logs and any irregularities or compromises should be immediately reported to the TeCS Department.

### 3.5 Server Administrator Passwords

In addition to the general password guidelines listed in this procedure, the following apply to server administrator passwords, except where technically and/or administratively infeasible:

- Passwords for servers must be changed as personnel changes occur.
- If an account or password is suspected to have been compromised, the incident must be reported to the TeCS Department and potentially affected passwords must be changed immediately.
- Attempts to guess a password should be limited to ten incorrect guesses. Access should then be locked for a minimum of ten minutes, unless a local system administrator intercedes.
- Uniform responses should be provided for failed attempts, producing simple error messages such as "access denied." A standard response minimizes clues that could result from hacker attacks.
- Failed attempts should be logged, unless such action results in the display of the failed password. It is recommended that these logs be retained for a minimum of 30 days. Administrators should regularly inspect these logs and any irregularities such as suspected attacks should be reported to the TeCS Department.

### 3.6 Guest Passwords

Guest users who do not have accounts on district computers may have accounts, including email accounts, assigned to them for use in conducting district business.

### 3.7 Departmental Accounts

For access to sensitive information managed by a department, account management should comply with the standards outlined above. In addition, naming conventions must not cause contention with centrally managed email addresses or usernames. Should the potential for contention arise, the applicable system(s) shall not be connected to the district network until a mutually satisfactory arrangement is reached.

Managers shall have the right to impose additional departmental rules or procedures. In the event of conflict, the rules and procedures presented herein shall take precedence over departmental rules and procedures.

### 3.8 Shared Accounts

Use of shared accounts is not allowed except when necessary to support the functionality of a process, system, device (such as servers, switchers or routers) or application (e.g., management of file shares). Such exceptions will require documentation which justifies the need for a shared account; a copy of the documentation will be shared with the TeCS Department.

Each shared account must have a designated owner who is responsible for the management of access to that account. The owner is also responsible for the above mentioned documentation, which should include a list of individuals who have access to the shared account. The documentation must be available upon request for an audit or a security assessment.

### 3.9 Application and System Standards

Applications developed at district or purchased from a vendor should contain the following security precautions:

- Where technically or administratively feasible, shared ID authentication should not be permitted.
- Authentication should occur external to an application, i.e., applications should NOT implement their own authentication mechanism. Instead, external authentication services should be relied upon, provided by the host operating system, the web server, or the servlet container. [In general, applications programmers are not necessarily familiar with the techniques associated with security protocols, and may inadvertently create security holes. Security services available from these external environments are much more likely to provide a high level of security.]
- Passwords must not be stored in clear text or in any easily reversible form.
- Role-based access controls should be used whenever feasible, in order to support changes in staff or assigned duties.
- Systems should allow for lock-outs after a set number of failed attempts (ten is the recommended number). Access should then be locked for a minimum of ten minutes, unless a local system administrator intercedes. Lock-outs should be logged unless the log information includes password information.