

CITRUS COMMUNITY COLLEGE DISTRICT GENERAL INSTITUTION

AP 3722 COMPUTER AND NETWORK CONNECTIVITY AND ACCESS

1.0 Purpose

Citrus Community College District must provide a secure network for student, instructional and administrative needs and services. An unsecured computer on the network allows denial of service attacks, viruses, Trojans, and other compromises to enter the district's network, thereby affecting many computers as well as the network's integrity. Damages from these compromises could include the loss of sensitive and confidential data, interruption of network services and damage to critical district internal systems. Educational institutions that have experienced severe compromises have also experienced damage to their public image. Therefore, individuals who connect computers, servers and other devices to the district network must follow specific standards and take specific actions.

This procedure defines the standards for connecting computers, servers or other devices to the district's network, and is designed to protect the district network and the ability of members of the Citrus community to use it. The procedure minimizes the potential exposure of the district to damages (including financial, loss of work, and loss of data) that could result from computers and servers that are not configured or maintained properly. The procedure also ensures that devices on the network are not taking actions that could adversely affect network performance.

2.0 Scope

This procedure applies to all members of the district community or visitors who have any device connected to the district network, including, but not limited to, desktop computers, laptops, servers, wireless computers, specialized equipment, cameras, environmental control systems, and telephone system components. The procedure also applies to anyone who has systems outside the district network that access the district network and resources. The procedure applies to district-owned computers (including those purchased with grant funds), and personally owned or leased computers that connect to the district network.

3.0 Procedures

3.1 Appropriate Connection Methods

Devices may be connected to the district network at appropriate connectivity points including voice/data jacks, through an approved wireless network access point, via a Virtual Private Network (VPN) or Secured Shell (SSH) tunnel, or through remote access mechanisms such as Digital Subscriber Line (DSL), cable modems, and traditional modems over phone lines.

Modifications or extensions to the network can frequently cause undesired effects, including loss of connectivity. These effects are not always immediate, nor are they always located at the site of modifications. As a result, extending or modifying the Citrus network must be done under supervision of the Technology and Computer Services (TeCS) Department. Exceptions will be made by TeCS for approved personnel in departments who can demonstrate competence with managing the aforementioned hardware.

The California State University 4CNET provides district connection to the World Wide Web. As a member, the district is responsible for following the 4CNET Acceptable Use Procedures.

3.2 Network Registration

Users of the district network may be required to authenticate when connecting a device. Users may also need to install an agent on their computers before they are allowed on the network. The role of such an agent would be to audit the computer for compliance with security standards as defined in this procedure.

TeCS maintains a database of unique machine identification, network address and owners for the purposes of contacting the owner of a computer when it is necessary. For example, TeCS would contact the registered owner of a computer when his or her computer has been compromised and is launching a denial of service attack or if a copyright violation notice has been issued for the internet protocol (IP) address used by that person.

3.3 Responsibility for Security

The TeCS Department has the primary responsibility for setting security on devices connected to the district network including ensuring that all devices meet the relevant security standards and managing the security of the equipment and the services that run on it.

3.4 Security Standards

These security standards apply to all devices that connect to the district network through standard district ports, through wireless services, and through home and off-campus connections.

Every computer or other device connected to the network, including a desktop computer has an associated owner (e.g. a student who has a personal computer) or caretaker (e.g. a staff member who has a computer in her office). For the sake of these procedures, owners and caretakers are both referred to as owners.

- Owners must ensure that all computers and other devices capable of running anti-virus/anti-malware software have Citrus-licensed anti-virus software (or other appropriate virus protection products) installed and running. Owners should update definition files at least once per week.
- Computer owners must install the most recent security patches on the system as soon as practical or as directed by the TeCS Department. Where machines cannot be patched, other actions may need to be taken to secure the machine appropriately.
- Owners of computers that contain sensitive district data should apply extra protections. The TeCS Department will provide consultations on request to computer owners who would like more information on further security measures. For instance, individuals who are maintaining files with Social Security information or other sensitive personal information should take extra care in managing their equipment and securing it appropriately.

3.5 Centrally-Provided Network-Based Services

The TeCS Department is responsible for providing reliable network services for the entire district. As such, individuals or departments may not run any service that disrupts or interferes with centrally provided services. These services include, but are not limited to, email, Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and Domain Registration. Exceptions will be made by the TeCS Department for approved personnel in departments who can demonstrate competence with managing the aforementioned services. Also, individuals or departments may not run any service or server that requests from an individual their district maintained password.

3.6 Protection of the Network

The TeCS Department uses multiple methods to protect the Citrus network including monitoring for external intruders, scanning hosts on the network for suspicious anomalies and blocking harmful traffic. All network traffic passing in or out of Citrus's network is monitored by an intrusion detection system for signs of compromises. By connecting a computer or device to the network, users are acknowledging that the network traffic to and from their computer may be scanned.

The TeCS Department routinely scans the Citrus network, looking for vulnerabilities. At times, more extensive testing may be necessary to detect and confirm the existence of vulnerabilities. By connecting to the network, users agree to have their computer or device scanned for possible vulnerabilities.

The TeCS Department reserves the right to take necessary steps to contain security exposures to the district and or improper network traffic. TeCS will take action to contain devices that exhibit the behaviors indicated below, and allow normal traffic and central services to resume. Such behaviors include but are not limited to:

- Imposing an exceptional load on a district service.
- Exhibiting a pattern of network traffic that disrupts centrally provided services.
- Exhibiting a pattern of malicious network traffic associated with scanning or attacking others.
- Exhibiting behavior consistent with host compromise.

The TeCS Department reserves the right to restrict certain types of traffic coming into and across the Citrus network. The TeCS Department will restrict traffic that is known to cause damage to the network or hosts on it. The TeCS Department also may control other types of traffic that consume too much network capacity, such as file-sharing traffic.

By connecting to the network, users acknowledge that a computer or device that exhibits any of the behaviors listed above is in violation of these procedures and will be removed from the network until it meets compliancy standards.

3.7 Enforcement

Access to district computing facilities may be wholly or partially restricted by the district without prior notice and without the consent of the user when there is reason to believe that violations of policy or law have taken place, or, in exceptional cases, when required to meet time-dependent, critical operational needs. Such restriction is subject to established district procedures or, in the absence of such procedures, to the approval of the Superintendent/President or Chief Information Service Officer, or appropriate designee.

Individuals may report suspected violations of these guidelines to the alleged abuser's manager, supervisor, instructor, and/or dean as appropriate. The District also provides anonymous reporting options. Disciplinary action may be taken in accordance with one or more of the following: district policies, California law, and/or the laws of the United States.

Minor infractions of these guidelines or those that appear accidental in nature are typically handled internally by the TeCS Department in an informal manner. In some situations it may be necessary, however, to suspend account or computer access to prevent ongoing misuse while the situation is under investigation.

More serious infractions, such as unauthorized use, attempts to steal passwords or data, unauthorized use or copying of licensed software, violations of district policies, or repeated violations of minor infractions may result in the temporary or permanent loss of access to computing facilities.

Offenses that are clearly in violation of local, state, or federal laws will result in the immediate loss of access to computing resources and will be reported to the appropriate law enforcement authorities. In addition, disciplinary action, up to and including dismissal, may be applicable under other district policies, guidelines, or collective bargaining agreements.

Users do not own accounts on district computers, but accounts including email accounts are assigned to individuals for use in conducting district business. Under the Electronic Communications Privacy Act of 1986 users are entitled to privacy regarding information contained on these accounts. This act, however, allows system administrators or other district employees to access user files in the normal course of their employment when necessary to protect the integrity of computer systems or the rights or property of the district. For example, system administrators may examine or make copies of files that are suspected of misuse or that have been corrupted or damaged. User files may be subject to search by law enforcement agencies under court order if such files contain information that may be used as evidence in a court of law. In addition, records maintained by the district on district computer facilities are considered "educational records" under the Family Educational Rights and Privacy Act of 1974.

3.8 Technology and Computer Services Department Rights and Responsibilities

In the normal course of systems administration, the TeCS Department may need to examine files, electronic mail, and printer output in order to gather sufficient information to diagnose and correct system problems or perform technical maintenance. In the course of this work, the staff may, without notice to the manager and employee, inspect, copy, remove, or otherwise modify any data, file, or system resources which has the potential to adversely affect the system. In addition, the TeCS Department reserves the right to restrict system access of any user who violates the rules/procedures presented in this document. Although the TeCS Department has the right to examine any system files without notice to the manager and employee, they also have a responsibility to maintain users' privacy to the maximum extent possible.

Board Approved 05/04/10