

# ACCD Network Assurance Task Force

In October 2003, the ACCD Information Technology Planning Council appointed a task force to examine the state of computer network security at ACCD and formulate appropriate policies and procedures to assure the continuing availability of ACCD information resources in the face of the large number of ongoing technology security threats. Initial members of the task force were:

Arne Saustrup, Operations Manager, ACCD Information Technology  
Dr. Julia Briggs, Director of Instructional Technology, SPC  
Gary Shelman, Director of Instructional Technology, PAC  
Les Germer, Coordinator of Campus Technology, SAC  
Larry Edmond, Director of Information Technology, NVC

As the Task Force moved forward, many others participated in the effort and made important contributions. They include:

Chris Delgado, Coordinator of Campus Technology, PAC  
Usha Venkat, Client Services Manager, ACCD Information Technology  
Sean Chaney, Coordinator of Campus Technology, NVC  
Dimas Reyes, Coordinator of Campus Technology, SPC

These Network Assurance Policies and Procedures are the Task Force's recommendations. The Task Force recommends rapid approval and implementation of the Policies and Procedures. In some cases, the Task Force recommends the replacement of some older, insecure equipment, and the acquisition of some additional hardware and software to improve the ACCD technology security position. It is hoped that the IT Planning Council and top ACCD Administration endorse these recommendations and fund these initiatives. The Task Force made every effort to maximize the current ACCD investments but replacement of fundamentally insecure and outmoded equipment and software is critical.

The Task Force is indebted to the authors and contributors to the Educause publication, "Computer and Network Security in Higher Education". These policies and procedures are strongly aligned with the Educause recommendations.

# **Alamo Community College District Network Assurance**

## **Policies and Procedures**

July 15, 2004

### **Purpose**

This network security document defines policies and procedures that are designed to ensure the protection of ACCD network assets. These policies and procedures will apply to all ACCD network components and workstations. They have been designed to provide "defense in depth" in order to achieve the maximum protection from the wide variety of technology security threats that currently exist. While it is not yet possible to provide total protection from all threats, strict adherence to these policies and procedures will greatly reduce our network vulnerabilities without sacrificing the flexibility and openness needed in an academic environment.

### **Network Security Challenge**

Today's computer networks exist in a dangerous world. It seems that new threats sometimes appear almost on a daily basis. Coping with this myriad array of threats requires the cooperation of the ACCD IT technical staff, the individual college Technology groups and the entire ACCD computer user community.

The goal of this document is to define policies and procedures that, if followed, will insure the continuity of the ACCD's business processes and mission in the face of the wide variety of technology security threats. The strategy used is called "defense in depth". This strategy puts prudent defenses in place to protect against threats at every layer of the network infrastructure.

### **Scope of Policy**

#### ***Charter***

This Network Assurance Policy document will be submitted for approval by the ACCD IT Planning Council. The IT Planning Council was appointed by the ACCD Chancellor. The Network Assurance Task Force of the ACCD IT Planning Council's primary responsibility is for the development, maintenance, and implementation of these Policies. These documents shall be regularly updated and appended to meet future network assurance requirements.

### ***Applicability***

The policies and procedures described in this document apply to the ACCD Enterprise Network environment, including all network facilities and equipment within the ACCD campuses, district buildings, and satellite locations, as well as all ACCD faculty, staff, and students who use this equipment.

In a limited number of unique areas, the local academic mission may be incompatible with these standards. Each area so identified will be individually analyzed and an individual security policy designed. These areas and their associated security solutions will be identified in the appendix of this document.

### ***District IT Security Responsibilities***

ACCD Information Technologies has the responsibility to ensure the integrity of the ACCD network, network attached information resources, and the data that flows within the network. The District has the right and obligation to investigate any security violations that occur within the ACCD network. This includes the right to examine any and all data that flows over network connections.

ACCD Information Technologies is generally responsible for all Enterprise information resources, including the Enterprise Network infrastructure. They are also responsible for security solutions for all ACCD District offices and designated District workstation groups.

### ***College Security Responsibilities***

The ACCD member college information technology groups have the security responsibility for all college level information resources, including college hosted shared information resources. They are responsible for security solutions for all college academic and administrative workstation environments.

### ***User Responsibilities***

ACCD users are responsible for the physical security of the equipment and/or workstation allocated for their use. Users shall not give network or email userid or passwords to anyone else. They are urged to use the email password assigned by the IT department. This password consists of eight random alphanumeric characters and cannot be easily guessed. If users suspect their password(s) have been compromised, they shall contact Support Central immediately to have them changed. Users may be held accountable for any security violations that occur using the equipment in their custody.

All ACCD technology users are expected to comply with the applicable ACCD Administrative Policy and Student Code of Conduct.

### ***Breaches Of Policy***

Any breach of the policies and procedures outlined in this document by any ACCD employee or student, in which the breach results in the damage and/or destruction of district computer equipment or data, or which causes denial of

network services to other ACCD network users, will be considered a serious matter. The offending employee or student shall be reported immediately to his or her immediate supervisor or academic authority.

### ***Cooperation/Coordination***

Network assurance is the responsibility of the entire ACCD and the ACCD College Technology Staff. In an environment the size, complexity, and geographical distribution of the ACCD, security must be a part of everyones focus. Network assurance and defense in depth can only be accomplished by full participation, collaboration, and cooperation at every level.

The college Technology Departments will be the primary coordinators and liaisons with ACCD IT for all security and network assurance issues.

## **Standards**

### ***Physical Security***

Proper physical security measures shall be taken at every level of the network, including the ACCD Central Computer Center, Campus server facilities, Campus MDFs and IDFs, and all labs and offices. Telecommunications IDFs are dedicated facilities and will not be used to house workstations or servers.

### ***IP Network***

- ACCD Information Technologies will be responsible for administration and security of all ACCD DNS servers.
- ACCD Information Technologies will administer all ACCD IP address space. The ACCD IT DHCP server network will be the standard mechanism for IP address assignments throughout ACCD. All networked workstations will be configured to automatically obtain IP address, gateway, DNS and all other IP information via DHCP.
- IP addresses and other IP information will not be hard coded on workstations or printers.
- Reserved addresses for servers and other shared resources will be available from ACCD IT upon request, with reasonable justification.
- ACCD IT is responsible for all IP network routing and traffic flow.
- ACCD IT is responsible for all network routers, switches and network hardware. All college network equipment expansions and purchases shall be coordinated through and engineered by ACCD IT. All future network

linkages shall be via Ethernet switches. No additional Ethernet hubs shall be purchased or deployed.

### ***Wireless Network***

There is general agreement 802.11x wireless technology presents a huge technology security threat if not carefully configured, deployed, and monitored. ACCD IT and the College IT Groups have collaborated on a wireless network security solution to be implemented and enforced throughout the entire ACCD.

- All deployments of wireless networking components of any kind and at any location must be coordinated through the College IT group and ACCD IT. Any rogue wireless components will be immediately disconnected and removed from the ACCD location when discovered. ACCD DPS will be contacted if necessary. In the case of college campus deployments, the installation shall be coordinated between ACCD IT and the College IT group.
- By prior agreement, a secure wireless Virtual LAN (VLAN) has been created spanning all ACCD locations. All wireless Access Points (APs) must be connected to this and only this VLAN.
- Mobile wireless classroom carts shall have the AP access encrypted with a unique WEP key. The classroom cart laptop computers shall also have this same encryption code to ensure that only that cart's laptops can access that cart's AP.
- Wireless clients connecting to the secure wireless VLAN will then access the Internet and the ACCD network after being authenticated by the BlueSocket Wireless Gateway.

### ***Workstations***

- Microsoft Active Directory has been implemented district-wide, and all network domains will be merged into this structure. All workstations will be required to logon to the Active Directory structure.
- The Systems Management Server will be used as the "push" mechanism within the Active Directory. The SMS management client will be installed on all workstations. All workstations will connect to this server for remote control, hardware inventory, software inventory, software updates, and remote installation services. SMS will be used to keep all network attached Microsoft OS workstations updated with security patches.

- The use of a managed Symantec anti-virus server is required. This server provides for the centralized management of anti-virus updates and services. Each college will maintain a campus server, and ACCD IT will maintain the central District server.
- All workstations will have a consistent naming convention. This convention will have the format Building-Room-ACCD Tag.
- All workstations will be given network access consistent with the user's academic mission.
- Users will not be allowed to enable local workstations to act as DNS, DHCP, WINS, NNTP, WWW, NTP, FTP, TFTP, RAS, or Terminal Services servers.
- Workstations may be left on 24/7 and users will be required to log off at the end of the day. This will facilitate security and patch management operations, however, this will be at the discretion of the local Campus IT Group.

### ***Printers***

- All printers (where applicable) will be network enabled and shared through centralized print servers.
- Printers will not be shared from a local workstation.
- Users will be allowed to attach local non-shared printers to their workstations.

### ***Servers***

- All servers will be regularly scanned for security vulnerabilities.
- Managed Symantec real-time anti-virus services will be enabled on all servers.
- A Server Security Patch plan will be developed to keep all servers patched and up-to-date.
- There will be one campus managed web server, one campus managed anti-virus server, one campus managed email/collaborative solutions server, one campus managed database storage solution, and one campus managed system management platform.

- Read/write access to specific WWW server folders must be requested with an ACCD Web Page Agreement form with the appropriate department chair or administrative signature.
- Servers that send and receive private and confidential data such as userids and passwords will have a Verisign Secure Server certificate installed to provide encryption of this data.

### ***Networks***

- Network access controls will be implemented to eliminate unneeded traffic paths and types throughout the network.
- The IP Monitor system will be used to share network status information throughout the district.
- A network based internal intrusion detection and suppression system will be deployed to protect district servers and gateways.
- All network IP addresses will be automatically assigned by ACCD DHCP servers. Reserved or static IP addresses for servers or for other special devices will be assigned upon Erequest only. Hard coded IP address information will not be done without documented approval.
- Servers and/or other network resources that require public Internet access or public DNS lookup will be enabled upon Erequest only. Appropriate administrative approval will be required prior to enabling these services. All such requests from the colleges shall be requested through that college's IT group.
- All employees will be issued a unique userid and password for network access. This id and password must not be shared. Use of generic userids will be phased out wherever possible. Special Guest Userids may be issued on a temporary basis under managed conditions.

### ***Email***

- The PureMessage spam and virus filter will be used to filter all incoming and outgoing email traffic.
- Anti-virus agents will be kept up-to-date. All internal virus infections will be reported to college or ACCD IT immediately so that appropriate action can be taken.

- The number of various email client programs in use throughout the district should be reduced to simplify management and support of the email environment.
- Students should be encouraged to use ACCD College ePortal email ids to facilitate better tracking of email problems, and to eliminate valid student email being filtered due to matching spam heuristics.
- Users are required to change email passwords on a regular basis and to utilize strong passwords. Use of the "Remember Password" feature is discouraged.
- Any internal ACCD user sending junk commercial email (spam) will be reported to his or her immediate supervisor for appropriate action.

### ***Internet***

- Firewall protection will be provided to protect internal PCs and workstations from the Internet. This will include protection for IDEA and wireless network PCs.
- Internet access to ACCD servers will only be allowed on the required TCP/IP ports.
- Intrusion detection systems will be deployed on all Internet gateways.

### ***Communications***

- All the Information Technologies Groups will be integrated through the use of the Nextel radio system.
- A district-wide Technology Crisis Response Team has been created that includes members from each college and other major district campus locations
- A district wide Crisis Response Plan will be developed that will include a communications plan, district responsibilities, college responsibilities, and shared responsibilities.
- All ACCD IT groups will share information on known security threats.

### ***Users***

- Users will be responsible for the physical security of their workstations and/or other computer equipment. They will also be responsible for the security and integrity of the data on this equipment.
- Users will not be allowed to share files or directories from their local workstations.
- A formal user security responsibility policy/statement will be developed and implemented.
- A clear computer acceptable use policy will be developed and implemented.

## **Security Crisis Response Information**

### ***Crisis Response Team Members***

The Crisis Response Team information is currently being collected and will be appended at this point.

### ***Crisis Response Notification Plan***

The Crisis Response Notification Plan is currently under development and will be appended at this point.

## **Exceptions To Network Assurance Standards**

The only current exception is the SAC CIS Department Network. An exception plan has been developed and is pending approval. This exception plan will be appended at this point.