



ADMINISTRATIVE PROCEDURE

Procedure Number 27-3

Effective Date 3-1-98

C. Dubelben

County Administrator

Subject: Internet and Computer Network Security Procedure

Departments Responsible: Information Services
Departments with Internet and Computer Network Access

I. PURPOSE

This administrative procedure sets forth security guidelines regarding the configuration of computer networks which have Internet and Pima County Backbone Network access.

II. DEFINITIONS

- A. Backbone Network: A high-speed connection between computer networks.
- B. Firewall: A combination of hardware and software which separates one computer network from another for security reasons.
- F. Internet: The global network that connects millions of computers, and allows users to send and receive e-mail, log in to remote computers (telnet), browse databases of information (gopher, World Wide Web, WAIS), and send and receive programs (ftp) contained on network computers.
- H. Internet Services: Any of a number of applications which are primarily intended for use over the Internet. This includes email, browse, log in, and file transfer applications.
- E. Perimeter Network: A network which exists between an organization's Internet connection and a firewall. Also known as a De-Militarized Zone or DMZ.
- E. Pima County Backbone Network: The fiber optic backbone network which runs between Pima County buildings and connects departments.
- K. Server: A computer which provides a specific kind of service to another group of computers.

III. PROCEDURE

- A. All Pima County Internet connected data traffic must pass through the Information Systems Department (ISD) Firewall.
- B. All external connections which are not to Pima County agencies and use Internet protocols must be to a government agency network which is either protected behind a firewall or does not have an Internet connection. Otherwise, the data traffic must pass through the ISD Firewall.
- C. The ISD Firewall configuration default will be to deny all requests from external Internet sources into the internal Pima County network.
- D. Departmental servers which provide unsecured services to external Internet users will be located on the ISD Perimeter Network between the ISD Firewall and the Internet.
- E. Pima County staff or other authorized users will only be allowed to access the internal Pima County network via the Internet if they utilize secured authentication or encryption services located on the ISD Firewall.
- F. ISD shall manage the electronic devices on the Pima County Backbone Network.
- G. Any firewall used to comply with these standards must use software or hardware which is certified by the National Computer Security Association. The responsible Pima County department must provide documentation to ISD which contains the software and hardware used, rules applied, network configuration, and a security contact.
- H. Any exception to the Pima County Internet and Computer Network Security Procedure must be requested in writing and approved by the ISD Director or designee.

IV. RESPONSIBILITIES

- A. IT IS THE RESPONSIBILITY OF EACH DEPARTMENT HEAD OR DESIGNEE TO COORDINATE ANY ACCESS FROM THE INTERNET OR NON-COUNTY COMPUTER NETWORK WITH THE INFORMATION SERVICES DEPARTMENT.
- B. THE INFORMATION SERVICES DEPARTMENT WILL PROVIDE AND MANAGE PIMA COUNTY COMPUTER NETWORK SECURITY FOR INTERNET AND NON-COUNTY COMPUTER NETWORK ACCESS.