

### Definition

The role of the system administrator is to install, maintain, and support the shared hardware and software resources of an organization. Areas of responsibility typically include:

- Setup and configuration of servers
- System administration: setting up and maintaining accounts, access control, and the user interface
- Installation of shared software and hardware
- System documentation
- Troubleshooting / Problem determination
- Problem management
- System performance analysis
- Change management
- Operations management
- Execution of back-up and recovery procedures
- System monitoring and maintenance of system logs
- User support

### Standards

A number of standards have been recommended by the Governor's Task Force on Information Resource Management for providing guidance when acquiring technology (see Policies). These standards will be updated on an ongoing basis and the most recent version can be obtained from the Governor's Task Force Web site, available at <http://www.irm.state.ny.us>. A section of the recommended standards For Network Services is listed below:

### Best Practices

The System Administrator must keep abreast of organizational needs and objectives as well as developments in technology and suggest possible enhancements or changes that could improve productivity and performance. The system administrator must ensure that the networked environment is reliable and serves the needs of the organization. Recommended practices include:

- Make technical decisions which support organizational needs; let the users make the final decision regarding software choices whenever possible - the System Administrator should act as a consultant in this decision-making process.
- Know your users and anticipate their needs. Focus on learning technologies which can support those needs.
- Look at long-term objectives when building the system.
- Understand all components of the system.
- Test all components of the system. In particular, test the back-up and recovery plan. Do not assume that any software or recovery plan will work unless it has been periodically tested.
- Know what the most critical components of the system are and monitor these components. Develop a recovery/contingency plan in case problems occur with these components and test this plan frequently.
- Document all components of the system so that another staff member could troubleshoot when the System Administrator is not available.

### Policies

On January 9, 1997, the Governor's Task Force on Information Resource Management issued 'Technology Policy 97-1 Information Security Policy,' which states: "the individual responsible for systems security should not be a system administrator whose primary responsibilities are for maintaining and upgrading operating systems. Separating systems administration from security duties improves the security climate."

On July 19, 1996, and again on January 3, 1997, the Governor's Task Force on Information Resource Management issued 'Technology Policy 96-16 - Technology Standards,' and Technology Policy 96-16A --

Electronic Document Management Systems - Standards, which provides general guidance to agencies for future technology acquisitions. Recommended standards are identified for Data Management Systems, Data Interchange, Network Services, Advanced Telephony, and Document Imaging.