

---

---

# Best Control Practices for Local Area Networks

*Produced by:  
The University of Alabama System  
Office of Internal Audit - UAB*



## **Introduction**

For most departments and offices in the UAB community, the ability to share local computing resources is vital to the efficiency and effectiveness of their operations. Increasing reliance on e-mail and desktop applications in meeting core-business requirements begs for increased attention to the control environment.

This document is a digest of control practices suggested by key members of the UAB network community and controls found or recommended by the Office of Internal Audit during reviews of several local area network (LAN) administrative functions at UAB. The material has been adapted to apply irrespective of LAN architecture and network operating system and is intended to augment official UAB policies at [www.iss.uab.edu/managsupport.htm](http://www.iss.uab.edu/managsupport.htm) and UAB Data Communications/ Networking Services (DC/NS) network guidelines at [www.tucc.uab.edu/trmpg29.htm](http://www.tucc.uab.edu/trmpg29.htm)

UAB policies address the following network-related topics: data security; copying computer software; equipment purchases, acquisition, transfer, and disposal; network connections; and copyrights. DC/NS guidelines address: LAN architecture; network operating systems; file servers; workstations; and network usage. Adherence to official policies is required. The Office of Internal Audit recommends adherence to DC/NS guidelines and implementation of the best control practices described below.

---

## **Inventory Controls**

- ❑ Maintain inventory listings with version and serial numbers for equipment and software and store a copy of the listings at an off-site storage location. (Inventory reports should be more complete than those provided by UAB Equipment Accounting - their records do not include equipment costing under \$2,000 and software costing less than \$5,000.)



- Establish procedures to ensure that equipment and software released to employees for use outside the department or off-campus is returned when the employee transfers or terminates employment.
- Oversee computer equipment and software disposal in accordance with the UAB Equipment Accountability Policy.

---

**Physical Security and  
Environmental Controls**

- Maintain servers and network hardware devices in secured areas and prevent unauthorized access.
- Place critical equipment on circuits dedicated to the building's backup emergency generator (120 volts), if available.
- Identify the location of the wiring/communication closet that feeds your network and contact the University Communication Services Help Desk/Repair at 4-7777 if the closet is left unsecured by Maintenance or Environmental Services personnel or if you have suspicions about others that make or attempt entry.
- Locate the power panels in your areas and label the circuits for your servers and other critical equipment.
- Keep server areas free of dust and other particulate matter and protected from water damage. (Servers should not be located near restrooms, beneath fire sprinklers and other sources of water.)
- Protect backup media from damage due to water, temperature extremes and the effects of magnetic fields.
- Locate fire extinguishers in or near the server area and verify inspection annually. Contact Campus Maintenance or Hospital Maintenance at <http://www.fab.uab.edu> to request an assessment of fire prevention controls at your location.
- Establish Uninterruptible Electrical Power Supply (UPS) coverage for the server, a test schedule for the UPS system, and a replacement schedule for UPS batteries.



**Logical Security and  
Data Integrity**

- Use passwords, password age requirements (60 to 90 days or less) and password length requirements (six or more characters - preferably a mixture of alpha and numeric characters) on all user accounts.
- Establish procedures to ensure that names and passwords of vendor-supplied accounts and service accounts with unlimited rights (supervisor, administrator, backup software accounts, Exchange Service Account, etc.) are changed from the vendor's default values as the system is installed and as turnover in the LAN administrative function occurs.
- Disable guest accounts not required for business operations.
- Store the supervisor/administrator ID and password in a secured place for use by backup personnel when the primary administrator is unavailable.
- Provide users with written instructions for logging on and logging off the system.
- Conduct orientation sessions with new users and provide periodic review sessions with existing employees to ensure awareness of password security controls, virus protection requirements, software licensing requirements, and the fiduciary responsibilities of using and having custody of information systems resources.
- Install virus-detection software on servers and workstations; scan hard disks, diskettes, and all files received via e-mail or through other network activity. Update the virus-scanning program and related virus signature files regularly. (Server-based virus protection requires careful consideration and planning beyond the requirements for protection of workstations.)
- Document and implement procedures for the following:
  - ◆ Establishing user accounts and access to system resources based on written management authorization.
  - ◆ Establishing access to system resources from external sources based on written management authorization.



- ◆ Ensuring that user accounts and corresponding access rights are reviewed regularly for reauthorization by management.
- ◆ Classifying critical and sensitive files and programs and granting access accordingly.
- ◆ Reporting network intrusions (crackers) and other forms of network abuse to the UAB Campus Network Manager at [abuse@uab.edu](mailto:abuse@uab.edu).
- ◆ Reporting computer-related crimes (theft of physical property, intellectual property, proprietary and research information, etc.) to UAB Police.
- ◆ Developing and maintaining critical applications, spreadsheets, and databases created by departmental personnel or those under contract by the department. Procedures should include:
  - Acquiring advance approval by management for software development efforts and changes to existing in-house developed software.
  - Testing software changes prior to implementation.
  - Acquiring management review and sign-off on new developments and changes prior to implementation.
  - Maintaining a backup of software to ensure recovery if new changes fail.
  - Logging all changes to software and hardware.
  - Publishing system and user documentation and maintaining a copy of the system documentation at an off-site location to ensure continuity of support should the original developer become unassociated with the department.
  - Notifying affected users prior to implementation of a new system and changes to an existing system.

---

### **Backup, Recovery, and Contingency Planning**

- Make provisions for swift replacement of hard disks and other key components of the server.



- ❑ Document instructions for rebuilding all servers including special BIOS configurations, RAID controller settings, IP addresses, DNS registrations, etc.
- ❑ Create and verify daily backups, review backup logs and follow up on errors and inconsistencies. (Give careful consideration to the advantages and disadvantages of available backup strategies and their impact on restoration procedures and times.)
- ❑ Routinely rotate a current backup of system, program, and data files to a secure off-site location. (The off-site storage location should be on UAB-owned property and should be at least several blocks from the primary server – within sufficient distance to assure that a disaster at the primary server location would not impede access to the off-site location. The off-site storage location should have suitable environmental controls conducive to magnetic media. To ensure prompt restoration of a damaged system, authorized personnel should have 24x7 access to the off-site storage location.)
- ❑ Document backup, tape rotation, and other critical procedures to ensure continuity of practices during the network administrator’s absences from the office.
- ❑ Perform periodic tests to measure your ability to recover from a disaster. Use data from backup media and record the time it takes to recover.
- ❑ Develop and routinely update a written recovery/contingency plan that includes:
  - ◆ Emergency procedures to ensure the safety of staff members.
  - ◆ An assessment of the system’s vulnerabilities with estimates of downtime and recovery periods under different scenarios – including worst case.
  - ◆ A prioritized listing of services and applications with estimated recovery times and a schedule of restoration.
  - ◆ A defined chain-of-command with roles and responsibilities of the network support staff, users of network services, and administrative personnel during the downtime, recovery and reconstruction period.
  - ◆ A notification schedule and escalation procedure with names, addresses, and telephone/pager



- numbers of key departmental personnel, UAB DC/NS, vendors, and affected business partners (both internal and external to UAB).
- ◆ Provision for the periodic review and approval of the plan by management.
- Store a copy of the recovery/contingency plan at an off-site location.

---

### **Training and Miscellaneous Operational Controls**

- Establish a technical training program for the primary and backup administrator to ensure adequate support of the system and protection of information system resources.
- Document the following:
  - ◆ File/folder/directory naming conventions.
  - ◆ Hardware maintenance schedules.
  - ◆ Problem reporting and tracking procedures.

---

### **Year 2000 Compliance**

- Confirm Year 2000 preparations for all firmware and software (including software created by departmental personnel and individuals under contract by the department).
- Develop downtime and recovery procedures for mission-critical systems to ensure continuity of core business functions.
- Make necessary modifications and upgrades for non-compliant systems and test to ensure readiness.
- Retain documentation supporting Year 2000 compliance efforts.

