9.3 System Administration Policies

In addition to determining user policies, certain defined policies for system administrators must be determined also. There must be a procedure for adding users, removing users, dealing with security issues, changing any system, and so on. Procedures for handling any deviation must also be taken into account.

9.3.1 New Employees

When a new employee is hired, the system administration policy must define specific steps to safeguard company security. New employees must be given access to the resources and applications their job functions require. The granting of that access must be documented (possibly in a log). It is also critical that each new employee receives a copy of the company's computer security/acceptable use policies. A document should also be signed acting as acknowledging as receipt of acknowledgment.

Before a new employee starts to work, the IT department (specifically network administration) should receive a written request from the business unit that the person will be working. That request should specify exactly what resources this user needs and when it starts. It should also have the signature of someone in the business unit with authority to approve such a request. Then, the person who manages network administration or network security should approve and sign the request. After having implemented the new user on the system with the appropriate rights, you can file a copy of the request.

9.3.2 Leaving Employees

When an employee leaves, it is critical to make sure that all logins are terminated and all access to all systems is discontinued immediately. Unfortunately, this is an area of security that many organisations do not give enough attention to. It is imperative to have all of the former employee's access shut down on his last day of work. This includes physical access to the building. If a former employee has keys and is displeased, nothing can stop him from returning to steal or vandalize computer equipment. When an employee leaves the company, you should ensure that on his last day the following actions take place:

- All logon accounts to any server, VPN, network, or other resources are disabled.
- All keys to the facility are returned.
- All accounts for e-mail, Internet access, wireless Internet, cell phones, etc., are shut off.
- Any accounts for mainframe resources are cancelled.
- The employee's workstation hard drive is searched.

The last item may seem odd. However, if an employee was gathering data to take with him (proprietary company data) or conducting any other improper activities, you need to find out right away. If you do see any evidence of such activity, you need to secure that workstation and keep the evidence in any civil or criminal proceedings.

All of this might seem a bit extreme for some people. We understand that the vast majority of exiting employees do not pose this much of a threat, however if you do not make it a habit of securing an employee's access when he departs, you could eventually be caught up in an unfortunate situation that could have been easily avoided.

9.3.3 Change Requests

The nature of IT is change. Not only end users come and go, but requirements change frequently. Business units request access to different resources, server administrators upgrade software and hardware, application developers install new software, web developers change the website, and so on. Change constantly takes palce. Therefore, it is important to have a change control process. This process does not only make the change run smoothly, but also allows the IT security personnel to examine the change for any potential security problems before it is implemented. A change control request should go through the following steps:

- An appropriate manager within the business unit signs the request, signifying approval.
- The appropriate IT unit (database administration, network administrator, e-mail administrator, and so on) verifies that the request is one they can fulfil (from both a technological and a budgetary/business perspective).
- The IT security unit verifies that this change will not cause any security problems.

- The appropriate IT unit formulates a plan to implement the change and a plan to roll back the change in the event of failure.
- The date and time for the change is scheduled, and all relevant parties are notified.

Your change control process might not be identical to this one; in fact, yours might be much more specific. However, the key to remember is that in order for your network to be secure, you simply cannot have changes happening without examining their impact before implementing them.