Part III
Operational Controls

Overview of Part III

This section addresses security controls that focus on controls that are, broadly speaking, implemented and executed by people. These controls are put in place to improve the security of a particular system (or group of systems). They often require technical or specialized expertise -- and can be highly interdependent with management activities as well as technical controls. The chapters, in no particular order, are:

- Personnel/User Issues
- Awareness, Training and Education
- Contingency Planning
- Computer Security Incident Handling
- Computer Support and Operations
- Physical and Environmental Protection

This section begins by addressing personnel issues. People are often cited as essential to the success of computer security -- and also, not surprisingly, as the greatest threat to security. This chapter discusses a broad range of security issues involving people, with specific emphasis on the process of granting users access to system resources. Special considerations that may arise when contractors or the public have access to the system are also presented. Two important concepts, *separation of duties* and *least privilege*, are discussed in this chapter. They show up many times throughout the Handbook, particularly in the Identification and Authentication, Logical Access Control, and Audit Trails chapters.

Closely related to the personnel chapter is the next chapter, Computer Security Awareness, Training, and Education. This chapter defines and discusses benefits and differences among awareness, training, and education. General implementation issues are also presented.

Next, the Handbook focuses on contingency planning and incident handling, two chapters which are closely related. Both help an organization maintain the availability (and integrity and confidentiality, as necessary) of their computer resources. Contingency Planning deals with those actions that can be taken to prevent and minimize damage from harmful events as well as recover from them. The various steps involved in developing a contingency plan, as well as testing its effectiveness are discussed. The Incident Handling chapter deals specifically with deliberate malicious technical threats (e.g., hackers and viruses). This chapter presents the goals of an incident handling capability both containing and repairing damage from incidents as well as preventing future damage. Characteristics of successful incident handling programs are also reviewed.

The Computer Support and Operations chapter discusses how security is integrated into the procedures and functions taken in running a system. The chapter discusses some of the many tasks within support and operations that have significant security considerations. These include: user support, software support, configuration management, backups, media controls, documentation, and maintenance.

Physical and environmental security controls are presented in the final chapter of this section. The benefits of physical security measures are discussed, followed by specific areas of consideration, including physical access controls, fire safety, supporting utilities, structural collapse, plumbing leaks, interception of data, and mobile and portable systems. The use of physical access controls to complement logical access controls is stressed in this chapter.

10 Personnel/User Issues

10.1 Introduction

Successfully securing computers ultimately comes down to security issues involving their human users, designers, implementors, and managers. A broad range of security issues is involved in how these individuals interact with computers and the access and authorities each must have to do their job. No computer system can be said to be secure without addressing these personnel and user security issues[42].

This chapter will examine issues involved in the staffing of positions which interact with computer systems; the administration of users on a system, including considerations for terminating employee access; and special considerations which may arise when contractors or the public have access to systems.

10.2 Staffing

The staffing process generally involves at least four steps and can apply equally to general users as well as application managers, system management personnel and security personnel. These four steps include: 1) defining the job, normally involving the development of a position description; 2) determining the sensitivity of the position; 3) filling the position, which involves screening applicants (often including background checks) and selecting the individual; and 4) training the individual.

10.2.1 Groundbreaking -- Position Definition

As the managerial process of defining a position occurs, security issues should be identified and dealt with -- hopefully early in the process. Once a position has been broadly defined, the responsible supervisor must determine the type of computer access needed for the position. There are two general principles which are used by management when determining access: *separation of duties* and *least privilege*.

Separation of duties refers to the division of roles and responsibilities so that a single individual cannot subvert a critical process. For example, in accounting systems, no single individual is given authority to issue checks. Rather, one person initiates a request for a payment and another authorizes that same payment. In effect, checks and balances must be designed into both the process as well as the specific, individual positions of personnel who will implement the process. Assuring that such duties are well defined is the responsibility of the cognizant management officials.

---

[42] A distinction is made between users and personnel since some users (e.g., contractors and members of the public) may not be considered personnel (i.e., employees).

Least privilege refers to the security objective of granting users *only those accesses required to perform their duties*. Data entry clerks, for example, may not have any need to run analysis reports of their database. Least privilege may still mean that some employees have significant access, if it is required for their position. However, application of this principle may limit the damage resulting from accidents, errors, or unauthorized use of system resources.

It is critical that a supervisor carefully determine the duties, responsibilities and access levels in accordance with the principles of separation of duties and least privilege prior to actually staffing a position. Knowledge of the duties and access levels that a particular position will require is necessary for determining the sensitivity of the position.

10.2.2 Determining Position Sensitivity

During this administrative phase, another security issue must be addressed: the sensitivity of the position. The responsible management official must correctly identify those position sensitivity levels so that appropriate, cost-effective screening can be completed. This position sensitivity designation directly affects resources since screening can be costly.

> The Federal Personnel Manual provides instructions to federal managers on sensitivity classification of positions within the federal government.

Various levels of sensitivity are assigned to positions in the federal government. Determining the appropriate sensitivity level is based upon such factors as the type and level of harm (e.g., disclosure of private information, interruption of agency critical processing, computer fraud, and so forth) the individual can cause through use of the computer system as well as more traditional factors such as access to classified information and fiduciary responsibilities. The Office of Personnel Management's Federal Personnel Manual (Section 732-5, subchapter 7) provides detailed guidance on computer/ADP risk levels.[43] Three separate levels are defined, as shown below.

10.2.3 Filling the Position - Screening and Selection

Once a position's sensitivity has been determined, the position is ready to be staffed. In the federal government, this typically includes publication of a formal vacancy announcement. This is followed by a review of candidates to determine which meet the requirements of the position. More sensitive positions typically require *pre-employment* background screening while *post-employment* screening is often acceptable for less sensitive positions.

---

[43] There are also risk levels for other factors, such as access to national security information.

Computer/ADP Risk Levels		Adverse Impact on Computer/ADP Security
3	High Risk	Potential for exceptionally serious impact involving duties especially critical to the agency mission with broad scope and authority, and with major program responsibilities which affect a major Computer/ADP system(s)
2	Moderate Risk	Potential for moderate to serious impact involving duties of considerable importance to the agency mission with significant program responsibilities which affect large portions of a Computer/ADP system(s).
1	Low Risk	Potential for impact involving duties of limited relation to the agency mission through use of Computer/ADP system(s).

Background screening is accomplished to determine whether a particular individual is suitable to occupy a given position. For example, in positions requiring a high degree of trust, the screening process will attempt to ascertain the person's trustworthiness and the appropriateness of holding a particular position. In the federal government, the screening process is formalized through a series of background checks conducted through a central investigative office within the organization or through another organization (e.g., the Office of Personnel Management). It is again necessary to stress the importance of selecting the appropriate position sensitivity, since screening in excess of the sensitivity of the position wastes resources, while too little may cause unacceptable risks.[44]

Within the federal government, the most basic screening technique involves a check for a criminal history, checking the FBI fingerprint records, and other federal indices. More extensive background checks examine other factors such as a person's work and educational history, personal interview, possession or use of illegal substances, and interviews with current and former colleagues, neighbors, and friends. The exact type of screening that takes place depends upon the sensitivity of the position to be occupied and applicable agency implementing regulations. Screening is not conducted by the prospective employee's manager; rather, agency security and personnel officers should be consulted for agency-specific guidance.

Outside of the federal government, employee screening is accomplished in many ways. Policies vary considerably among organizations due to the sensitivity of examining an individual's background and qualifications. Organizational policies and procedures normally try to balance fears of invasiveness and slander against the need to develop confidence in the

---

[44] In the federal government, separate and unique screening procedures are not established for each position. Rather, positions are categorized by general sensitivity and assigned a corresponding level of background investigation or other checks.

integrity of employees. One technique may be to place the individual in a less sensitive position initially.

For both the federal government and private sector, finding something in a person's background does not necessarily mean that they are unsuitable for a particular job. A determination must be made based on the type of job, the type of finding or incident, and other relevant factors. In the federal government, this process is referred to as *adjudication*.

10.2.4 Employee Training and Awareness

Even after a candidate has been hired, the staffing process cannot yet be considered complete -- the employee must still be trained to do their job, including their computer security responsibilities and duties. As is discussed in the chapter on Training and Awareness, such security training can be very cost-effective in promoting security.

Some computer security experts argue that employees must receive initial computer security training before granting them any access to computer systems. Others argue that this must be a risk-based decision, perhaps only granting restricted access (or, perhaps, only access to their PC) until the required training is completed. Both approaches, however, recognize that adequately trained employees are crucial to the effective functioning of computer systems and applications. In addition, although training of new users is critical, it is important to recognize that security training and awareness activities should be on-going throughout the time that an individual is a system user. (See the Training and Awareness Chapter for a more thorough discussion.)

10.3 User Administration

This section describes the process of administering users and user accounts on systems. Effective administration of users' computer access is essential to maintaining system security. *User account management* focuses on both management of identification and authentication as well as access privileges. This is augmented by the process of *auditing* or otherwise periodically verifying the legitimacy of current accounts and access privileges. Finally, there are considerations involved in the *timely modification or removal of access* and associated issues for employees who are being reassigned, promoted, or terminated, or are retiring.

10.3.1 User Account Management

User account management encompasses the process of requesting, establishing, issuing, and closing user accounts. It also includes tracking of users and their respective access privileges and the management of these functions.

User account management typically begins with a request from the user's supervisor to the system manager for a system account. If a user is to have access to a particular application, this request may be sent through the application manager to the system manager. This will assure that the systems office receives formal approval from the "application manager" for the employee to be given access. The request will normally state the level of access to be granted, perhaps by function or by specifying a particular user profile. (Often when more than one employee is doing the same job, a "profile" of permitted authorizations is created.)

Systems operations staff will normally then use the account request to create an account for the new user. The access levels of the account will be consistent with those requested by the supervisor. This account will normally be assigned selected access privileges. These are sometimes built directly into applications, and other times rely upon the operating system. "Add-on" access applications are also used. These access levels and privileges are often tied to specific access levels within an application.

Example of Access Levels within an Application

Level	Function
1	Create Records
2	Edit *Group A* records
3	Edit *Group B* records
4	Edit *all* records

Next, employees will be given their account information, including the account identifier (e.g., USERID) and means of authentication (e.g., password or smart card/PIN). One issue which frequently arises at this stage is whether the USERID is to be tied to the particular *position* an employee holds (e.g., ACC5 for an accountant) or the *individual employee* (e.g., BSMITH for Brenda Smith). This may simplify administrative overhead in some cases; however, it may make auditing more difficult as one tries to trace actions of a particular individual. However, if the USERID is created and tied to a position, procedures will have to be established to change them if employees switch jobs or are otherwise reassigned.

At the time employees are given their account it is often convenient to provide initial or refresher training and awareness on computer security issues. Users should be asked to review a set of rules and regulations for system access. To indicate their understanding of these rules, many organizations require employees to sign a "computer account receipt," which may also state causes for dismissal or prosecution under the Computer Fraud and Abuse Act and other applicable state and local laws.

When user accounts are no longer required, the supervisor should inform the application manager and IRM office so that accounts can be removed in a timely manner. One useful secondary check is to work with the local organization’s personnel officer to establish a procedure for routine notification of employee departures to the systems office. Further issues are discussed in the "Termination" section below.

It is essential to realize that *access and privilege administration is a continuing process.* New users are added while old users are deleted. Permissions change: sometimes permanently, sometimes temporarily. New applications are added, upgraded and removed. Tracking this information to keep it up to date is not easy, but is necessary in order to only allow users access to those functions necessary to accomplish their assigned responsibilities -- thereby helping to maintain the principle of *least privilege*. In managing these accounts, there is a need to balance timeliness of service and record keeping. While sound record keeping practices are necessary, delays in processing requests (e.g., change requests) may lead to requests for more access than is really necessary - just to avoid delays should such access ever be required.

One example of a simple user account and password acknowledgement form is as follows:

I hereby acknowledge personal receipt of the system password(s) associated with the user IDs listed below. I understand that I am responsible for protecting the password(s), will comply with all applicable systems security standards, and will not divulge my password(s) to any person. I further understand that I must report to the Information Systems Security Officer (ISSO) any problem I encounter in the use of the password(s) or when I have reason to believe that the private nature of my password(s) has been compromised.

Detailed system security procedures, training, and guides can also be given to the employee at the time initial access is acknowledged.

Managing this process of user access is also one that, particularly for larger systems, is often decentralized. Regional offices may be will be granted the authority to create accounts and change user privileges or submit forms requesting that the centralized access control function make the necessary changes. Approval of these changes is important -- it may require the approval of the file owner and the supervisor of the employee whose access is being changed.

10.3.2 Audit and Management Reviews

From time to time, it is necessary to review an entire system. Within the area of personnel and user issues, such reviews may examine the levels of access each individual has, consistent with the concept of least privilege, whether all accounts are still active, whether management authorizations are up-to-date, whether required training has been completed, and so forth.

These reviews can be conducted on *at least* two levels[45]: 1) an application by application basis or 2) a system-wide basis. Both kinds of reviews can be conducted by, among others, "in-house" personnel, contractor personnel, or audit personnel. For example, a good practice is for application managers may wish to review all access levels of all users of the application on a monthly basis -- and sign a formal access approval list, which will provide a formal written record of the approvals. While it initially may appear that such reviews should be conducted by systems personnel, they usually are not fully effective. System personnel *can* verify that users only have those accesses which their managers have specified. However, as noted above, these may change over time. It is therefore important to involve the application manager, who is often the only individual likely to know this information.

Outside audit organizations (e.g., the Inspector General [IG] or the General Accounting Office) may also conduct audits. For example, the IG may direct a more extensive review of

---

[45] Note that this is not an either-or distinction.

permissions. This may involve discussing the need for particular access levels for specific individuals or the number of users with sensitive access. For example, how many employees should really have authorization to the check printing function? (Auditors will also review non-computer access by reviewing, for example, who should have physical access to the check printer or blank stock of checks.)

10.3.3 Detecting Unauthorized / Illegal Activities

Auditing is one essential tool to detect unauthorized and illegal activities. Analysis of audit trails can yield significant insight into unauthorized activities. (See the chapter on Audit.) Other mechanisms also exist. For example, fraudulent activities may require the regular physical presence of the perpetrator(s). In such cases, the fraud may be detected during the employee’s absence. Mandatory vacations, for critical systems and applications personnel can help detect such activity (however, this is not a guarantee, particularly if problems are saved for the employee to handle upon their return). It is useful to avoid creating an excessive dependence upon any single individual, since the system will have to function during the vacation period. Rotation of jobs among employees can be useful too. Periodic re-screening of personnel may also provide possible indications of illegal activity (e.g., living a lifestyle in excess of known income level).

10.3.4 Temporary Assignments and In-house Transfers

One significant aspect of managing a system involves keeping user privileges up-to-date. Privileges are typically changed under two types of circumstances: 1) change in job role, either temporarily (e.g., while covering for an employee on sick leave) or permanently (e.g., after an in-house transfer) and 2) termination. (Termination considerations are discussed in 10.4.5 below.)

Users often are required to perform duties outside their normal scope during the absence of others requiring additional access privileges. Although necessary, such extra access privileges should be granted sparingly and carefully monitored, consistent with the need to maintain separation of duties for internal control purposes. Also, they should be removed in a timely manner when no longer required.

In addition to temporary changes in access privileges, permanent changes are usually necessary when employees change positions within an organization. In this case, the process of granting account privileges (detailed in the section on "User Account Management") will occur again. At this time, however, is it also important that access privileges of the prior position be promptly removed. Many instances of "privilege creep" have occurred with employees continuing to maintain their access rights for all previously held positions within an organization. This is inconsistent with the principle of least privilege and must be avoided.

10.3.5 Termination

Termination of user's system access generally can be characterized as either "friendly" or "unfriendly." Friendly termination may occur when an employee is voluntarily transferred, resigns to accept a better position, or retires. Unfriendly termination may include situations when the user is being fired for cause, "RIFed," or being involuntarily transferred. Fortunately, the former situation is more common, but security issues must be faced in both situations.

10.3.5.1 Friendly Termination

Friendly termination refers to the removal of an employee from the organization when there is no reason to believe that the termination is other than mutually acceptable. Since terminations can be expected regularly, this is usually accomplished by implementing a standard set of procedures for outgoing or transferring employees. These are part of the standard employee "out-processing," and are put in place, for example, to ensure that system accounts are removed in a timely manner. In this case, the personnel office may send a memo to the head of the computer processing office notifying them of the employee's scheduled date of departure. But other issues must be examined by the agency as well.

The continued availability of data, for example, must often be assured. In both the manual and electronic world, this may involve documenting procedures or filing schemes. For example, how are documents stored on the hard disk and how are they backed up? Are employees instructed whether or not to "clean up" their PC before leaving? If cryptography is used to protect data, how will the availability of cryptographic keys to management personnel be assured? Who will collect access tokens? Are employees asked to document how they accomplish their tasks? What procedures are in place to make sure this is accomplished?

Confidentiality of data can be an issue as well. For example, do employees know what information they are allowed to share with their immediate organizational colleagues? Does this differ from the information they may share with the public? These and other agency specific issues should be addressed throughout an agency to assure continued access to data and to provide continued appropriate protection for its confidentiality and integrity during personnel transitions. The agency's training and awareness program should address such issues, as appropriate.

10.3.5.2 Unfriendly Termination

Unfriendly termination describes the situation when the removal of the employee takes place under involuntary or adverse conditions. This may include termination for cause, RIF reduction, involuntary transfer, resignation for "personality conflicts," situations with pending grievances, and so forth. The tension in such terminations may multiply and complicate security issues which must be faced. Additionally, all of the issues involved in friendly terminations are still present, but addressing them may be considerably harder.

The greatest threat from unfriendly terminations is likely to come from those with the capability to change code or modify the system or applications. For example, systems personnel are ideally positioned to wreak considerable havoc on systems operations. Without appropriate safeguards, personnel with such access can place logic bombs (e.g., a hidden program to erase a disk) in code which will not even execute until after the employee's departure. Backup copies can be destroyed. There are even examples where code has been "held hostage." But other employees, such as general users, can also cause damage. Errors can be input purposefully. Documentation can be misfiled. Other "random" errors can be made. Correcting these situations can be resource intensive.

Given the potential for adverse consequences, security specialists routinely recommend that system access be terminated as quickly as possible in such situations. If an employee is to be fired, system access should be removed at the same time (or just before) the employee is notified of their dismissal. When an employee notifies an agency of a resignation and it can be reasonably expected that it is on unfriendly terms, system access should be immediately