INFORMATION SECURITY

POLICIES and PROCEDURES

A Practitioner's Reference

Thomas R. Peltier

Boca Raton London New York Washington, D.C.

Library of Congress Cataloging-in-Publication Data

Peltier, Thomas R.
Information security policies and procedures : a practitioner's reference / Thomas R. Peltier.
p. cm.
Includes bibliographical references and index.
ISBN 0-8493-9996-3 (alk. paper)
1. Computer security. 2. Data protection. I. Title.
QA76.9.A25P428 1998
658.4'78—dc21 98-44238
CIP

Auerbach is an imprint of CRC Press LLC

No claim to original U.S. Government works

International Standard Book Number 0-8493-9996-3

Printed in the United State of America 1 2 3 4 5 6 7 8 9 0

Printed on acid-free paper

Dedication

To Lisa, my teammate and partner.

Contents

Acknowledgments

No matter who you are, when you begin to write a book, you take with you all of the experiences and acquaintances that you have generated over a lifetime. So it was with me when I began to develop the outline for this book; I began by using my notes from the training seminars that I have conducted over the past 13 years. Every class is a learning experience for me. I usually take away a number of new ideas; so, to everyone that has attended a workshop, seminar, or class, I want you to know that you are part of this process.

Over 20 years ago, I began writing policies and procedures for the organization in which I was working. This was truly on-the-job training. I had just completed my undergraduate work in education and had done well in the courses on writing fiction and poetry. It came as quite a shock to me that images and flowery language were not what was needed. Clean, clear, crisp, concise, and correct were what was needed. My boss and friend, Larry Degg, was patient when reviewing the initial procedures. He taught me that speed was not as important as getting things right.

Since I began to write policies and procedures in 1977, I have had the great good fortune to work with a number of people and organizations who have had an impact on where I am today. Chief among those are John O'Leary of the Computer Security Institute. Whenever I have a question, I know that I can turn to John and use him as either a sounding board or a source to get answers. Both John and the Institute have been exceptionally strong in their support of my activities over the years. Another group that must be mentioned is the award-winning team that I was able to put together at Detroit Edison (Lisa Bryson, Richard Coles, Cheryl Fierk, Sherry Giordano, Tim Hyland, Ken Jaworski, Mike Kadar, Naaman Mustafa, and Annette Wilson). They were able to take the raw policies and procedures and edit them (Lisa and Sherry) and put them into a finished product (Mike and Ken). This was a great group of people to work with; every day I tried to find a way to challenge them and they found the way to exceed my expectations.

Finally, how can any book on information security policies and procedures be complete without mentioning the founding fathers of this profes-

sion: William H. Murray, Donn B. Parker, and Robert Courtney, Jr. This "holy trinity" of knowledge has been an inspiration to us second-generation professionals. Among the next group are Michael J. Corby, John Blackley, Ed Devlin, Harold F. Tipton, Carl Jackson, and Charles Wood.

About the Author

Thomas R. Peltier, CISSP

Tom Peltier is in his third decade of computer technology experience as an operator, an applications programmer and systems programmer, systems analyst, and information systems security officer. Currently he is the Senior Security Consultant for the Professional Services Organization of CyberSafe Corporation, a total information security provider. Prior to this, Tom was the Corporate Information Protection Coordinator for Detroit Edison. In this assignment he implemented the development of a Corporate Information Protection Program, including the examination of control requirements during the applications development life cycle (Facilitated Business Impact Analysis, Facilitated Risk Analysis Process), the enhancement of the business continuity planning function to encompass all corporate business units, the formation and maintenance of an incident response team to manage virus and security exposure control, and the definition of nondisclosure agreements and contract employee controls for contract employees to ensure the protection of Detroit Edison proprietary assets. This program has been recognized for excellence in the field of computer and information security by winning the Computer Security Institute's Information Security Program of the Year for 1996. Tom previously was the Information Security Specialist for General Motors. In this capacity, he was responsible for the development of worldwide policies, procedures, and awareness training.

Tom has published a number of articles on various computer and information security issues, including developing policies and procedures, disaster recovery planning, copyright compliance, virus management, and security controls. He has published a book entitled *The Complete Manual of Policies and Procedures for Data Security* and was a contributing author for the *Computer Security Handbook, Third Edition* and *Data Security Management.* Tom was the technical advisor on the security films "Locking the Door," "Invasion of the Data Snatchers," "Under Wraps," "Mum's the Word," "Back in Business," "Virus: Prevention, Detection, Recovery," "Access Denied," and "The Best Defense." He is the past chairman of the Computer Security Institute (CSI) advisory council, the Chairman of the 18th

Annual CSI Conference, founder and past-president of the Southeast Michigan Computer Security Special Interest Group, and a former member of the board of directors for (ISC)2, the security professional certification organization. He was the 1993 "Lifetime Award" recipient at the 20th Annual CSI Conference. He conducts numerous seminars and workshops on various security topics and has led seminars for the CSI, Crisis Management, American Institute of Banking, American Institute of Certified Public Accountants, Institute of Internal Auditors, EDP Auditors Association, and Sungard Planning Solutions.

Chapter 1
Why Policies, Standards, and Procedures Are Needed

1 INTRODUCTION

The overall objective of an information security program is to protect the integrity, confidentiality, and availability of information. The primary threats that keep an organization from attaining this goal are unauthorized access, modification, destruction, and disclosure. These threats can be either accidental or deliberate.

An information protection program should be part of any organization's overall asset protection program. The goals and objectives that make up the information security program must be understandable by all employees.

As long as there have been Information Systems Security Officers (ISSOs), there has been a need to create and implement information security policies and procedures. The ISSO was usually brought in from one of the various groups within Information Technology and charged with the responsibility to create these documents. The background in IT often helped the ISSO in understanding technical issues, but it was sometimes a hindrance in grasping the business strategies and objectives. With this very vaguely defined charter, the ISSO would usually try to find a book on the subject and often look to attend a seminar or workshop. The information gathered from these resources often provided the "how-to," but usually failed in the "why-for."

2 LEGAL REQUIREMENTS

Are there legal and business requirements for policies and procedures? The answer to this question is a resounding — yes. Not only are there requirements, but the laws and acts define who is responsible and what they

must do to meet their obligations. The directors and officers of a corporation are required under the "Model Business Corporation Act," which has been adopted in whole or in part by a majority of states, to perform specific duties: a duty of loyalty and a duty of care.

2.1 Duty of Loyalty

By assuming office, senior management commits allegiance to the enterprise and acknowledges that interest of the enterprise must prevail over any personal or individual interest. The basic principle here is that senior management should not use its position to make a personal profit or gain other personal advantage. The duty of loyalty is evident in certain legal concepts:

- Conflict of Interest — individuals must divulge any interest in outside relationships that might conflict with the enterprise's interests.
- Duty of Fairness — when presented with a conflict of interest, the individual has an obligation to act in the best interest of all parties.
- Corporate Opportunity — when presented with "material inside information" (advanced notice on mergers, acquisitions, patents, etc.), the individual will not use this information for personal gain.
- Confidentiality — all matters involving the corporation share be kept in confidence until they are made public.

2.2 Duty of Care

In addition to owing a duty of loyalty to the enterprise, the officers and directors also assume a duty to act carefully in fulfilling the important tasks of monitoring and directing the activities of corporate management. The Model Business Corporation Act established legal standards for compliance. A director shall discharge his or her duties

- in good faith
- with the care an ordinarily prudent person in a like position would exercise under similar circumstances
- in a manner he or she reasonably believes is in the best interest of the enterprise

2.3 Federal Guidelines for Sentencing for Criminal Convictions

The Federal Sentencing Guidelines define executive responsibility for fraud, theft, and anti-trust violations, and establish a mandatory point system for federal judges to determine appropriate punishment. Since much fraud and falsifying corporate data involves access to computer-held data, liability established under the Guidelines extends to computer-related crime as well. What has caused many executives concern is that the mandatory punishment could apply even when intruders enter a computer system and perpetrate a crime.

While the Guidelines have a mandatory scoring system for punishment, they also have an incentive for proactive crime prevention. The requirement here is for management to show "due diligence" in establishing an effective compliance program. There are seven elements that capture the basic functions inherent in most compliance programs:

1. establish policies, standards, and procedures to guide the workforce
2. appoint a high-level manager to oversee compliance with the policies, standards, and procedures
3. exercise due care when granting discretionary authority to employees
4. assure compliance policies are being carried out
5. communicate the standards and procedures to all employees and others
6. enforce the policies, standards, and procedures consistently through appropriate disciplinary measures
7. implement procedures for corrections and modifications in case of violations

These guidelines reward those organizations that make a good-faith effort to prevent unethical activity; this is done by lowering potential fines if, despite the organization's best efforts, unethical or illegal activities are still committed by the organization or its employees. To be judged effective, a compliance program need not prevent all misconduct; however, it must show due diligence in seeking to prevent and detect inappropriate behavior.

2.4 The Economic Espionage Act of 1996

The Economic Espionage Act (EEA) of 1996 for the first time makes trade secret theft a federal crime, subject to penalties including fines, forfeiture, and imprisonment. The act reenforces the rules governing trade secrets in that businesses must show that they have taken reasonable measures to protect their proprietary trade secrets in order to seek relief under the EEA.

In *Counterintelligence and Law Enforcement: The Economic Espionage Act of 1996 versus Competitive Intelligence,* author Peter F. Kalitka believes that given the penalties companies face under the EEA, that business hiring outside consultants to gather competitive intelligence should establish a policy on this activity. Included in the contract language with the outside consultant should be definitions of

- What is hard-to-get information?
- How will the information be obtained?
- Do they adhere to the Society of Competitive Intelligence Professionals Code of Ethics?
- Do they have accounts with clients that may be questioned?

2.5 The Foreign Corrupt Practices Act (FCPA)

For 20 years, the FCPA was largely ignored by regulators. This was due in part to an initial amnesty program under which nearly 500 companies admitted violations. Now the federal government has dramatically increased its attention on business activities and is looking to enforce the act with vigor. To avoid liability under the FCPA, companies must implement a due diligence program that includes a set of internal controls and enforcement. A set of policies and procedures that are implemented and audited for compliance are required to meet the test of due diligence.

A way to help understand and visualize the process is to take a pseudo-Biblical approach. In this case "laws beget policy which begets standards which beget procedures, practices, and guidelines" (see Exhibit 1).

3 BUSINESS REQUIREMENTS

It is a well-accepted fact that it is important to protect the information essential to an organization, in the same way that it is important to protect the financial assets of the organization. Unlike protecting financial assets that have regulations to support their protection, the protection of information is often left to the individual employee. As with protecting financial assets, everyone knows what the solutions are to protecting information resources. However, identifying these requirements is not good enough; in order to enforce controls, it is necessary to have a formal written policy that can be used as the basis for all standards and procedures.

3.1 The Need for Controls

With requirements to access information both within the campus environment and external through remote access, the need for an organization-wide information security policy with supporting standards and procedures is more important than ever. Ten years ago, the need for nonemploy-

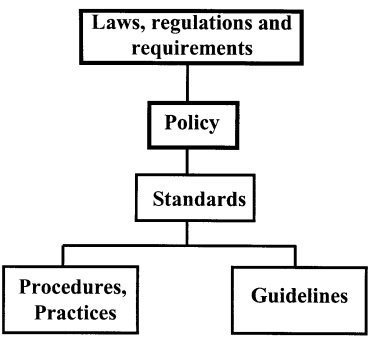

Exhibit 1. Policy chart.

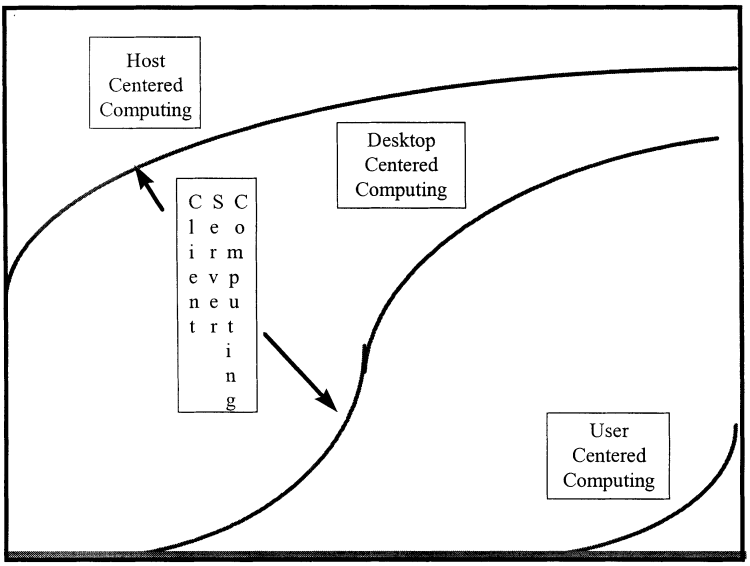

Exhibit 2. Changing environment overview.

ees to access corporate information was less than it is today. There has been a decided change in the processing environment.

3.2 The Changing Environment

In 1974, the Computer Security Institute held its first annual conference and the issues of computer and information security were brought to the forefront. Over the next ten years, the information-processing environment stayed fairly static. The world of computers was based around the mainframe. Policies and standards were developed to protect the information found on mainframe computer systems. Products such as ACF2 , RACF, TopSecret, and SAC were introduced to control access to the systems and data that they contained. Halon 1301 was touted as a safe way to protect computer rooms from fire. The Electronic Data Processing Auditors Association was founded and auditors were trained in how to conduct reviews of data processing facilities.

During the 1980s, the user community began to become disenchanted with IT due to its lack of responsiveness. A user needing a new application or an enhancement to an existing system might have to wait as long as six months before the request would be reviewed, and then another couple of months before a decision on the merits of the request were debated. Once there was approval to begin the project, it might take as long as 18 months to deliver the finished product. Often times, the finished product was not exactly what the client wanted.

By 1983 there were between six and ten million personal computers sold in the United States. Most of these early systems (Intel-based 286 processors) were found in corporations. Those departments that were dependent on IT for their new systems were now turning to their processing capabilities. A shotgun marriage of sorts was created when the information users began to install personal computers and then found that they needed to access information still maintained in the mainframe. The offspring of this attempt at desktop computing is client/server computing (CSC).

In some organizations, CSC meant that the controls, seen now as restrictive in the mainframe environment, were now taken away. Rapid Application Development (RAD) became the buzz word for cutting corners. Just when many more individuals were gaining access to corporate information, the controls that had been so hard won in the mainframe environment were being chipped away. The ability to have a centralized control function and the increase of userids and passwords have required review of the security process.

In the mainframe environment, access control could be put on at the system level. In the client/server medium, the control had to be placed at the application level. That means that every new application will require the user to have a new userid and password to gain access. Additionally, each application must maintain its own access control list. The ability to monitor and control access is greatly reduced.

The move to desktop computing has only been the beginning in this changing environment. The trend of moving the processing has now extended to the need to take the information to the user, wherever the user may be. This user-based computing has seen tremendous growth in such activities as telecommuting. Industry reports have identified telecommuting at 30 million workers with growth projected at 18 percent per year. The American Management Association forecasts 171 percent telecommuting growth now through 2000.

The Internet and e-mail usage has been a leader in this move away from the controlled mainframe environment. According to Forrester Research, Inc. (Cambridge, MA), back in 1992, only two percent of the U.S. population had access to e-mail. By 1997, the percentage had climbed to 15 percent of the total U.S. population and is expected to pass 50 percent by 2000. These, along with other remote access requirements, have moved the security requirements into a totally different arena. The need for policies, standards, and procedures is greater than ever. The security professional must adapt to these changes and the controls must meet the needs of a mobile workforce.

3.3 Good Business Practices

Although there are legal and regulatory reasons why policies, standards, and procedures should be implemented, the bottom line is that good con-

trols make good business sense. Failing to implement controls can lead to financial penalties in the form of fines and costs. Such activities can lead to loss of customer confidence, competitive advantage and, ultimately, jobs. The avoidance of public criticism, and saving the time on the investigation and subsequent disciplinary process are very effective benefits to the organization that can be obtained by implementation of proper controls.

Every organization is required to provide its services or products to its customers, either legally or contractually. To ensure that the business objectives are met in a timely and efficient manner, effective policies and standards must be in place. Protecting shareholder interests is a key component in the need to implement effective controls.

When preparing policies, standards, and procedures, tread lightly on the legal reasons (use them when needed), but learn to sell your product as any other product. To be accepted and implemented, the policies and standards will have to help managers meet their business objectives. When developing these documents, it will be necessary to understand what each business needs and then work to fulfill those requirements.

3.4 Where to Begin?

To find out what the business objectives or the mission of the organization are, one can begin to search out documents that define the organization. Many organizations have published their goals and objectives in a document similar to that depicted in Exhibit 3.

For publicly held companies, search out the stockholders Annual Report. The business objectives and commitments to providing return-on-investment are presented and endorsed by the top executives of the organization. A key section of the Annual Report is the "Responsibility for Consolidated Financial Statements." The responsibility for the integrity rests with management and normally contains a statement similar to "The Company maintains systems of internal controls supported by policies and procedures which are communicated throughout the Company."

Understanding the objectives or mission of the organization will help to ensure that the focus of the information security policies, standards, and procedures supports those objectives. Policies that hinder the completion of the business of the organization will be ignored or scrapped. When creating these documents, it will be necessary to keep this key element in mind.

Security, for security's sake, is of no value. The creation of policies, standards, and procedures must be beneficial to the organization. No policy should be created to ensure that the organization is in compliance with audit requirements. Policies, standards, and procedures are developed and implemented to ensure that the organization meets its legal and contractual obligations to its customers, clients, stockholders, and employees.

Exhibit 3. Shared beliefs.

The shareholders and customers of Company Corporation have entrusted the employees of Company Corporation with important responsibilities: to increase shareholder value by providing premier, world-class security solutions.

We have committed ourselves to fulfilling those responsibilities, recognizing that the commitment requires the personal dedication and leadership of each of us and the collective effort of all of us.

We are committed to teamwork and accountability.

We believe that unless we conduct ourselves as a team — and build team effort throughout the company — we cannot succeed. Further, we believe that a team succeeds only when all members understand the team goals, their individual roles, and how each person's performance and commitment contribute to achieving the goals. Our commitment to this concept is reflected in our willingness to accept accountability for results and to stake our personal success on those results.

We are committed to communication.

We practice open, honest, two-way communication and provide regular feedback. We believe that written communication cannot replace dialogue between people, that effective communication is a prerequisite to effect action; and that trust, respect, and understanding are necessary for effective communication. We set examples through our behavior because our actions do, in fact, speak louder than our words.

We are committed to continuous improvement and benchmarking.

Continuous improvement in our skills, methods, and results is vital to our success in the highly competitive information security sector. We measure our success and our improvement by comparing our performance with that of our competitors and other companies that are world-class performers. We recognize that just as we strive for improved performance, so do our competitors. Benchmarking, and continuous improvement, therefore, are ongoing processes that will ensure that our sights are constantly on target to become superior performers.

Our dedication to living these commitments will produce an environment in which employees are involved — involved in the goals of the company and their individual work groups — and sharing ideas and suggestions as valued contributors. In this way, we will provide value to customers, shareholders, and employees. Our goal is that every employee becomes committed to our shared beliefs.

4 SUMMARY

Every organization needs to implement policies, standards, and procedures. There are legal requirements for this:

- Model Business Corporation Act
  - Duty of loyalty
  - Duty of care
- Federal Guidelines for Sentencing
  - establish policies, standards, and procedures
  - appoint a manager responsible for compliance
  - assure compliance to policies and standards

  - enforce the policies and standards
- Economic Espionage Act
  - trade secret theft is a federal crime
  - companies must take steps to protect their trade secrets
- Foreign Corrupt Practices Act
  - companies must implement a due diligence program that includes internal controls and enforcement

Business requirements have been dictated because of the changing environment. The move away from mainframe processing to desktop processing to user-based processing has changed the security requirements.

Good business practices require that policies, standards, and procedures are implemented to protect customer confidence, competitive advantage, and employee jobs.

Chapter 2
Why Manage This Process as a Project?

1 INTRODUCTION

Although a project is usually defined as a *one-time* effort that has a definite beginning and end, and the implementation of security policies can be an *ongoing* effort, managing this process as a project will help keep the implementation team focused on the results to be achieved. Applying project management practices will also help with the assessment of those results to ensure they meet the needs of the organization.

Consideration should be given to such questions as: What is included within the area of concern or what is the scope? What should be done first? How much time will it take? Is there a deadline that will act as a constraint on how much can be accomplished? How should changing requirements be managed? How much will it cost? How relevant are the policies and procedures to the environment? Who should create them? How should they be reviewed? How should they be communicated? How can opportunities for improvement be maximized? How can the potential for resistance by staff be mitigated? When should external sources be considered for providing assistance?

Creating and implementing security policies and procedures begins with a thorough understanding of why one's organization is concerned that these policies and procedures exist. Understanding the reasons why the effort was undertaken will help one set goals and objectives when determining how the security needs of the organization will be met. Later, the results of the effort should be reviewed to ensure that they accomplished what was expected.

2 FIRST THINGS FIRST: IDENTIFY THE SPONSOR

A key factor in successfully implementing policies and procedures is to have commitment from senior-level management. The person with the means to commit resources to this effort should be identified as the project's sponsor. This sponsor will be the final person responsible for all major implementation decisions. Lack of a sponsor of sufficient seniority is

a major risk to successful implementation of policies and procedures. Work completed without this sponsor may be subject to rework if the project team proceeds in a direction not supported by management. It is important that support be explicitly obvious. Clear management support will help obtain the cooperation and contributions needed from individuals who may not be direct members of the project team.

The project manager is the individual that leads the work effort and is responsible for the day-to-day planning, management, and control of the project. The successful completion of project deliverables on time, within budget, and to the specified quality standards are included in the project manager's responsibilities.

The project manager can be recruited from any area concerned with security, such as information security or internal auditing. This individual could also be recruited from outside the organization. Superior communication, organization, and team-building skills are among the traits that this individual should possess.

It is best to have only one project manager so that the management and control of project activities can be effectively coordinated. Managing the implementation of policies and procedures requires contributions and feedback from multiple sources, and a project manager fulfills the role of the conductor by ensuring that these contributions are well integrated into the overall project.

Ensure that the project manager possesses a sufficient level of experience and skill to manage the challenges that can be encountered when policies are being implemented. Be conscious of the tendency toward resistance among staff when it comes to documenting business processes or practices that may be perceived as "needing remediation." Review any previous studies or reports that address existing security policies, procedures, or findings. A good place to start is with the internal audit staff or other groups that might perform audit or compliance-tracking functions. Determine if there are any constraints that might inhibit progress and document all assumptions that have been made. Measurable criteria should be established to assess the success of the policy and procedure implementation. If there are quality objectives, quantitative requirements, expected benefits, or cost objectives to consider, document them.

Once the sponsor and project manager have been identified, the project manager should conduct interviews with the sponsor to obtain an understanding of desired outcomes. These interviews are also an opportunity to identify other interested parties, or project stakeholders.

Initiatives to create or revise policies and procedures may be a response to any number of stimuli. Legal requirements, especially in publicly traded or financial organizations, may need to be addressed. An adverse event

that has occurred or almost occurred may prompt the effort. Sometimes, the effort is begun to guard against a situation that has occurred at another organization. A change in management can also spur a commitment to implement new or updated policies and procedures. Whatever the reason, the reason itself can be a good starting point for helping to define the overall objectives of this effort. Remember, it is extremely helpful to interview management to gain and document an understanding of their expectations. Clear, concise objectives that are documented and agreed upon by top-level management are a key success factor that should not be overlooked. Strive to obtain explicit confirmation, with a signature if possible, of the major objectives for the project to create and implement the policies and procedures to be producing.

3 DEFINING THE SCOPE OF WORK

Defining the scope of work places boundaries on what is to be accomplished. A scope statement should be developed that clearly defines what is and what is not included within the area of work to be completed. For example, one's approach to developing policies might be very different if the scope addresses issues from an enterprise perspective rather than at a more specific departmental position. Whether one is addressing an enterprise or departmental perspective, determine the high-level objectives that the policies and procedures are supposed to address and relate them to the organization's business objectives. Relating the project to the business objectives of the enterprise helps address issues associated with competing demands for limited resources. One needs to demonstrate that the activities associated with the implementation of security policies and procedures provide a positive contribution to the organization's goals.

To help define objectives, consider the types of information security challenges the organization must face. These objectives, or project requirements, lay the foundation for the plan of activities that will be developed to address those requirements. Careful consideration should be given to defining project requirements and they should always be documented. Requirements that remain floating around in someone's head are subject to ambiguity and misinterpretation. Developing a consistent understanding of the scope and requirements is extremely important to ensuring that the outcomes of the effort meet those requirements. If not sure what the organization needs are, one is not likely to develop policies to address those needs. A clear understanding of requirements will help direct effort toward achieving the project's goals. Keep requirements in mind to guide the activities and as a basis for future decisions as one defines, organizes, and implements the policies and procedures that are created.

Once requirements have been clearly defined, a high-level breakdown of project components or activities can be developed, as shown in Exhibit 1.

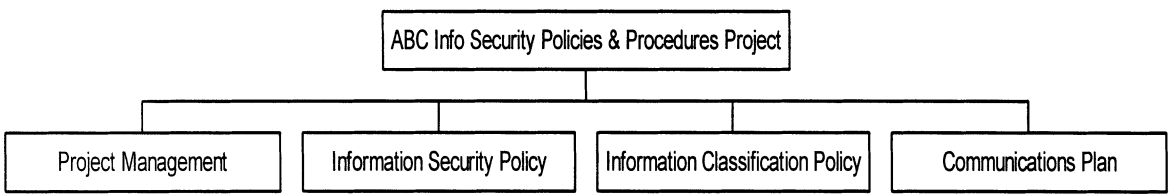

Exhibit 1. High-level work breakdown structure.

This high-level breakdown, or work breakdown structure (WBS), is a deliverable-oriented grouping of elements that help organize and define the total scope of the project. The WBS can be grouped by type of policy or procedure and should also include other supporting elements such as the communications plan. It is a good visual aid for identifying the work that the project will undertake. Work not identified in the WBS is outside the scope of the project.

After a high-level grouping of project deliverables has been defined, each high-level group should be further subdivided into more manageable components until enough detail is obtained to allow estimates of time, cost, and resource requirements to be assigned to each component. Although the sponsor and project manager can identify the high-level groups, the decomposition into subcomponents should be completed with the participation of other team members. See the Time Management section (Section 4) for more details.

Once high-level requirements are defined and agreed upon, a Project Kickoff meeting can be held to officially "begin" the project. This kickoff is a special meeting at which all stakeholders, project participants, and other interested parties are introduced to the project. It is very helpful in terms of obtaining cooperation and buy-in, if the project sponsor delivers an overview of the reasons the project was undertaken as well as key expectations.

The kickoff should also include an outline (see Exhibit 2) of the proposed approach to achieving the defined project requirements and provide an opportunity for participants to ask questions of and give feedback to the project team.

4 TIME MANAGEMENT

Based on the scope, high-level objectives, and constraints of the project, identify the appropriate lower-level steps and tasks to be accomplished. The work breakdown structure (Exhibit 3) should be reviewed and adjusted to ensure that all necessary tasks are included and that any unnecessary work has been removed. A basic project management tenet is to ensure that the project is controlled so that it includes all the work required and only the work required to bring it to successful completion. This process can be started by the project manager but should be supplemented with contributions by other project participants. Brainstorming techniques can be used when decomposing the high-level elements of the work breakdown structure into its lower-level components. After each element has been broken down, review each one and gain consensus on the validity of its subcomponents.

Each element should be decomposed to a level sufficient to later support an estimate of required time, cost, and resources to complete. The

Exhibit 2. Sample project kick-off agenda.

Security Policies and Procedures Project
Date
Time
Place

The purpose of this meeting is to begin the Security Policies and Procedures Project.

Invitees: Sponsor, project manager, project team members, other stakeholders

Desired outcomes:
1. Establish working relationships and lines of communication
2. Establish and review project scope and objectives
3. Review project approach
4. Establish responsibilities
5. Identify and document issues to be addressed
6. Identify next steps

Agenda Items	Who
1. Introduction	Project manager
2. Review agenda	Project manager
3. Project briefing: the purpose of this project	Sponsor
4. Project scope and objectives	Project manager
5. Project approach	Team
6. Responsibilities	Team
7. Issues	All
8. Next steps	Project manager

work breakdown structure is intended to organize and define the scope of the project and is not meant to demonstrate the sequence of work to be performed. Sequencing is done during the development of a schedule.

After decomposition, a list of all project activities to be performed can be developed based on the refined work breakdown structure. This list should include descriptions to ensure that the individuals assigned to complete the work understand what is to be delivered. After all activities are identified, they should be analyzed to identify interdependencies. Activities must be sequenced appropriately in order to develop a realistic schedule. Be sure to include activities that are administrative in nature, such as planning and conducting meetings and completing status reports. These activities can be grouped together, but careful consideration to this area will help prevent an over-optimistic estimate. Exhibit 4 displays a sample of a decomposed work breakdown structure.

Estimates for time to complete or effort can be developed after all activities and their interdependencies have been identified. Effort estimates will be influenced by the project manager's prior experience, ability to make judgments based on limited information, and knowledge of the subject

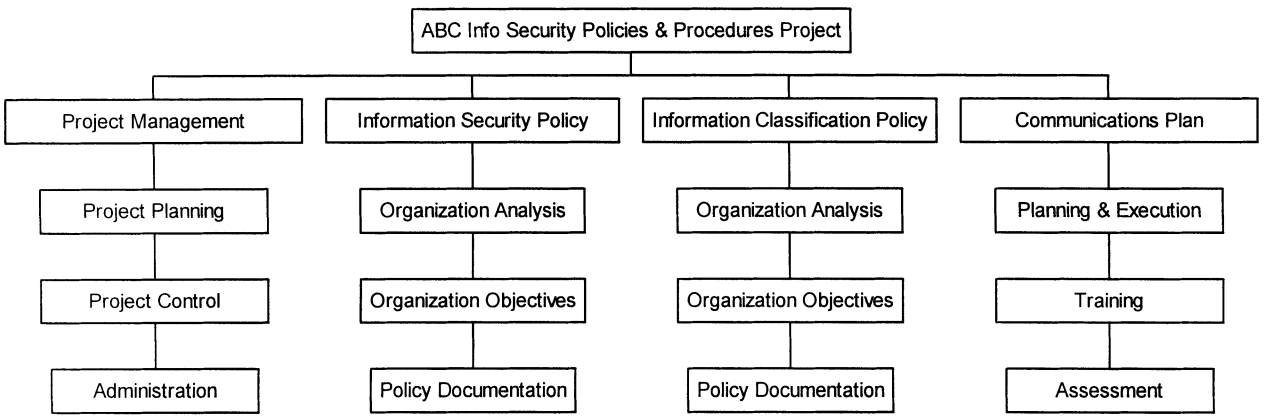

Exhibit 3. Sample work breakdown structure organized by policy type.

Exhibit 4. Sample decomposed WBS.
Policies and procedures project sample WBS.

I. Project planning, scheduling, and budgeting
   A. Project kickoff
   B. Establish project sponsor
   C. Identify benefits and costs
   D. Develop business case
   E. Establish objectives
   F. Define project scope
   G. Define project approach
   H. Define project activities
   I. Develop project schedule
   J. Prepare project budget
   K. Determine project staffing requirements
   L. Establish roles and responsibilities
   M. Conduct project status assessment
II. Training
   A. Determine training requirements
   B. Identify and acquire tools
   C. Develop training plan
   D. Manage training activities
   E. Establish budget status reporting methods
   F. Establish schedule status reporting methods
   G. Conduct project status assessment
III. Project control
   A. Monitor project progress
   B. Identify and resolve issues
   C. Manage exception situations
   D. Review and revise project plan
   E. Conduct project status assessment
IV. Project quality procedures
   A. Review enterprise documentation standards
   B. Define quality objectives
   C. Define product quality control reviews
   D. Define documentation standards for policies
   E. Define documentation standards for procedures
   F. Develop quality plan
   G. Define policy/procedure review strategies
   H. Define documentation management plan
   I. Identify/define support tools and procedures
   J. Conduct project status assessment
V. Develop policies
   A. Document definitions
   B. Identify required policies
   C. Identify procedures, standards required
   D. Determine formatting
   E. Outline content
   F. Develop and define policies
   G. Develop and define standards
   H. Develop and define guidelines
   I. Develop and define procedures
   J. Conduct project status assessment

Exhibit 4. Sample decomposed WBS. *(Continued)*
Policies and procedures project sample WBS.

VI.	Communications planning
	A. Identify audiences
	B. Determine distribution frequency requirements
	C. Determine information distribution mechanisms
	D. Develop communications plan
	E. Define performance reporting requirements
	F. Conduct project status assessment
VII.	Project Closure
	A. Complete final evaluations
	B. Initiate maintenance process
	C. Close outstanding project work
	D. Collect project feedback
	E. Compile project closure documents

matter. The estimating process should include the project team members; estimates developed by obtaining consensus from the team will probably be more accurate. Producing and reviewing estimates with the participation of the people who will do the work will also support team-building and build confidence for the estimates produced.

A bottom-up estimate for the overall project can be produced by allocating effort estimates to each lowest-level component and aggregating them up to obtain an initial estimate for the total project. Effort estimates for each WBS component, together with the identified activities to be performed and their interdependencies, will allow the project manager to develop the project schedule. Be sure to record all assumptions and issues identified.

Before beginning the estimating process, review the following questions.

- Who should be involved?
- What units of measure should be used: hours, days, weeks? The unit determined should be appropriate to the level of detail used to define the activities and ideally should be consistent across the entire project.
- How will contingencies be applied?

Two possible approaches to use are consensus-based and weighted average estimating. A consensus-based estimate involves getting a small group of people that are involved in an activity to estimate the effort required for that activity. The estimates produced will vary, based on the differing viewpoints and experiences of the people in the group. Participants are asked to produce estimates and then to explain the reasoning behind the estimates. The estimates can be discussed in reference to these explanations and, eventually, agreement can be reached for a single estimate. A weighted average estimating approach is outlined later in this section. Es-

timates can be developed using both approaches, with the results compared to refine and develop a single estimate.

To develop a weighted average estimate, have participants estimate each component of the activities list giving best-case, worst-case, and most likely estimates. This task should be completed individually; then a workshop can be conducted to consolidate and review the initial estimates. A determination of how the weighted average is calculated should be determined by the project manager or by team consensus.

The results should be reviewed with special attention paid to large variations between the best, worst, and most likely estimates and different people's estimates for the same activity. Reasons for the large variations should be determined and reconciled. Try to gain agreement among the estimators. The intention is not to arrive at the same value for the best, worst, and most likely cases, but to gain agreement on what are the best, worst, and most likely cases.

Once the estimates have been completed, they should be converted into practical estimates by allowing for nonproductive time, such as sickness and vacation. This might involve the application of a standard percentage value that is used to increase effort estimates. Be careful to avoid double-counting these items and inadvertently inflating the estimates.

As the project progresses, estimates can be revised based on the actual performance to date and due to unplanned events such as scope changes, staff changes, and newly identified activities.

The WBS and activities list (Exhibit 5) can be developed simultaneously and documented as a spreadsheet or used as input to an automated sched-

Exhibit 5. Sample table of weighted average calculations.

Category	Item	Best Case in Days (Weight — 15%)	Most Likely Case in Days (Weight — 55%)	Worst Case in Days (Weight — 30%)
Information classification	Establish the team	1	5	15
	Develop the policy	2	10	25
	Determining confidential information	5	20	80
	Identifying information to be declassified or reclassified	10	20	60

Note: Weighted average formula = (BC * .15) + (MLC * .55) + (WC * .30). This Weighted Average Table and its calculations are illustrative only and not intended to represent the actual experience of any specific project.

uling tool. An automated scheduling tool will allow the project manager to complete "what-if" scenarios such as when the work should be started if an arbitrary deadline is imposed on the project and how the schedule will be impacted if project resources are limited or expanded. The project schedule, or timeline, will serve as a basis for tracking progress against the plan.

5 COST MANAGEMENT

The work breakdown structure and sequenced activities list developed during the beginning stages of the project are used to support the development of a cost estimate. A more detailed WBS and activities list will support a more accurate estimate, but the level of detail required depends on the required degree of accuracy and the project manager's estimating experience. Keep in mind that a highly detailed WBS can be used to demonstrate the magnitude of the work involved and will provide support for the cost estimate. Each item on the activities list should include a labor and materials component. The cost of materials can be often overlooked when considering activities that appear to be labor intensive. For example, an activity identified as "training" may be estimated at 200 hours × \$60/hr. The \$1200 estimate will be too low if a graphics software package must be purchased to design the training material, printing and binding services are required, or organizational expectations are that participants will be served food and beverages during training.

See the section on Planning and Preparation for guidance on the types of activities to be included in the WBS and activities list. Also, a checklist can help minimize the risk that certain cost components will be omitted.

6 PLANNING FOR QUALITY

Planning for quality requires that processes be in place to ensure that the policies and procedures created satisfy the needs for which they were developed. These processes include activities such as inspection reviews. These reviews are conducted to critique the policies or procedures to help ensure that management expectations and requirements are met. Reviews also provide an opportunity to reduce the likelihood of errors, omissions, or misunderstandings. Results are documented and corrective action taken if necessary. Documentation standards, if any, should be reviewed to ensure that the policies and procedures developed are in compliance.

Review participants should include project team members as well as peers from other organization teams who have *not* been closely associated with the project. Management generally should *not* be included at preliminary reviews to ensure that the focus remains on the examination and tuning of the policies or procedures developed and not on the performance or status of the project itself.

7 MANAGING HUMAN RESOURCES

The primary objective of human resource management is to make the most effective use of the people involved with the project. Activities included are planning the organizational structure of the project, acquiring staff, and developing team members. The resources necessary to carry out the project and to ensure its success should be clearly defined and documented in terms of their roles and responsibilities. Reporting relationships can also be documented if necessary. Each person in the project should understand his or her responsibilities and should have the time available to carry out those responsibilities.

When determining staffing requirements, the skills required for the activities to be performed and their associated time frames should be defined. The WBS and activities list should be used during this task. Organizational policies and a description of the existing available resource pool should also be reviewed. If it is determined that resources will be acquired from outside the organization, a plan for how these resources will be brought into and removed from the project may need to be developed. Paying attention to how team members will be transitioned onto and off a project can help reduce costs by eliminating the tendency to create work to fill the time between assignments. See the section on Planning and Preparation for recommended qualities to look for in team members assigned to the development of policies and procedures.

Team development includes activities that support the ability of team members to increase their individual contributions to the project and enhance the ability of the team to function effectively. The capabilities and skills of the project team should be assessed to help establish a plan to train members in any areas of deficiency. The types of training required should be documented so that a training plan can be developed. This training is specific to the project team and is in addition to the awareness training plan that should be developed to introduce the new policies and procedures to the enterprise. The time required to develop team skills should be included in the project schedule.

8 CREATING A COMMUNICATIONS PLAN

Managing security communications effectively ensures that timely and appropriate information is generated, updated, and disseminated to all who need to know. Lack of employee awareness will defeat even the most comprehensive policies and procedures. The communications process ensures that critical connections are established among all individuals of an organization. These communication links are absolutely necessary for the successful implementation of security policies and procedures. Creating a communications plan will provide a framework from which to manage the communications process.

An organization's structure will have a major effect on communications requirements. The information delivery mechanisms for an organization that houses staff in one central location can be very different from one that has employees distributed over several remote locations. Take time to determine the information needs for your organization. Consider who needs what information, when and how often should they receive it, and how will it be given to them. An analysis of the policies and procedures and the circumstances that they address will help determine how significant they are to the organization and how often they should be delivered. Analyzing the circumstances that the policies and procedures address will also help identify the intended audience.

8.1 Sample Communications Plan During Development of P & P

Exhibit 6 contains recommended types of communications that can be established during the development of policies and procedures (P & P).

Exhibit 6. Sample communication plan (during planning and preparation).

Communication Type	Audience	Frequency	Responsibility	Delivery Mechanism
Project kick-off[a]	Project sponsor Stakeholders Project team	At project start	Project manager	Meeting
Overall status report[a]	Project sponsor Stakeholders Project team	Monthly	Project manager	Document attachment via e-mail
Project review milestone assessment[a]	Project sponsor	Quarterly	Project manager	Meeting
Project team meeting[a]	Project team	Weekly	Project manager	Meeting
Project newsletter	All affected (interested) parties	Monthly	Team members	Newsletter document via general mail
Task status	Project team Project manager	Weekly	Team member	Update commitment calendar
Issue identification	Project manager	As needed	All	Issue management process
History/inquiries about project	All	As needed	Project manager	Electronic project notebook accessible via Web page
Problem identification: internal	Project manager	As needed	All	Problem management process

[a] This type of communication should be required.

Exhibit 7. Sample communications plan (after deployment).

Communication Type	Audience	Frequency	Responsibility	Delivery Mechanism
New or revised policy announcement[a]	All	As released, periodically thereafter	Sponsor	Broadcast mail Broadcast e-mail Broadcast voice-mail
New or revised procedure[a]	All affected (interested) parties	As released	Sponsor	Training
Complete policy manual[a]	All	Yearly and at new employee orientation	Sponsor	Manual[a] Intranet Web page
General security awareness	All	Quarterly	Information security team	Broadcast mail Broadcast e-mail Intranet Web page Posters
Awareness newsletter	All	Semi-annually or quarterly	Information security team	Departmental meetings Broadcast mail
Employee security awareness day	All	Yearly or semi-annually	Information security team	Promotional items Employee contests Topic discussions and demonstrations

[a] This type of communication is required.

The needs of the project and expectations of the project sponsor and stakeholders will influence how adjustments should be made.

8.2 Sample Communications Plan After Deployment

Exhibit 7 contains recommended types of communications to be established once policies and procedures have been approved and are to ready be disseminated to the organization. Responsibilities for delivery can be delegated; however, the sponsor should explicitly endorse all communications. The delivery mechanisms or frequencies should be revised to meet the needs of the organization or the urgency of the situations the policy was designed to address. For example, a new policy that states that all company communications are subject to spontaneous monitoring may require more frequent delivery in a large organization with a high contract staff ratio than in an organization with a work force that is relatively stable.

9 SUMMARY

Managing the development of security policies and procedures as a project involves the application of a variety of skills, tools, experiences,

and techniques. Project management processes help guide project activities in order to meet or exceed stakeholder needs and expectations. A primary objective of project management is to efficiently and effectively manage resources to deliver products on time and within budget while attaining a given level of quality. The intent of this chapter was to introduce a few key project management concepts that should be readily adaptable to a policies and procedures development project.

Chapter 3
Planning and Preparation

1 INTRODUCTION

Planning and preparation are an integral part of policy, standard, and procedure development, but one that is often neglected. Included in the preparation process is all of the work that must be done prior to beginning the actual development process. Covered in this chapter are discussions on reference works obtainable, milestones, task checklists, and content level.

2 OBJECTIVES OF POLICIES, STANDARDS, AND PROCEDURES

Policies, standards, and procedures are key elements in ensuring that personnel are trained to handle specific job tasks. The policy will lay out the general requirements, the standard tools required, and the procedures will provide the step-by-step process required in routine activities. They can also be used when employees are required to make decisions. Many 911 operators have a set of tabbed procedures that allow them to understand the situation and make appropriate decisions. This kind of decision tree can be used by all personnel when performing their daily functions.

Well-written procedures will never take the place of supervision, but they can take some of the more mundane tasks and move them out to the employees. These documents are basically management resources that classify and document the organization. The objectives of policies, standards, and procedures are to:

- State and clarify policy — when management is unavailable (off hours or off-site), employees have a resource to which they can refer to assist them in making the correct decision.
- Define duties, responsibilities, and authority — the policy can identify who is responsible for which activity and the procedure can provide the step-by-step process needed to complete the task at hand.
- Formalize duties — an effective set of desk procedures can assist organization in meeting two key security requirements: separation of duties and rotation of assignments.

  - Separation of duties — no single individual should have complete control of a business process or transaction from inception to completion. This control concept limits the error, opportunity, and temptation of personnel and can best be defined as segregating incompatible functions (accounts payable activities with disbursement). The activities of a process are split among several people. Mistakes made by one person tend to be caught by the next person in the chain, thereby increasing information integrity. Unauthorized activities will be limited because no one person can complete a process without the knowledge and support of someone else.
  - Rotation of assignments — individuals should alternate various essential tasks involving business activities or transactions periodically. There are always some assignments that can cause an organization to be at risk unless proper controls are in place. To ensure that desk procedures are being followed as well as provide for staff backup on essential functions, individuals should be assigned to different tasks at regular intervals.

    One of the often-heard knocks against rotation of assignments is that it reduces job efficiency. However, it has been proven that an employee's interest declines over time when doing the same job for extended periods. Additionally, employees sometimes develop shortcuts when they have been in a job too long. By rotating assignments, the organization can compare how the task was being done and where changes should be made.
- Establish standards — once a policy has been implemented, it will be necessary to find the standards that can be used to support the policy. This can range from what software is to be used, what remote access protocol is to be implemented, to who is responsible for approving what.
- Provide information to employees, customers, etc. — the ability to communicate management directions is what policies, standards, and procedures are all about. Management does not have the luxury of sitting down with each employee, customer, client, vendor, supplier, etc. and telling them what is expected, how they are to perform their assignments, and what tools are to be used. A well-crafted set of policies, standards, and procedures act as the voice for management when working with personnel.
- Educate users — some organizations have thousands of users accessing various systems and applications. The ability to provide them with the information they need to perform this task is an essential element in well-written policies, standards, and procedures. Easy-to-read, current procedures can cut the number of calls to the customer service center (Help Desk). Recently, users were calling the Help Desk because the response time on their workstations had slowed. Asked if

they had a lot of files on the system, most indicated that they had deleted the files. However, when asked if they had emptied their wastebasket, most were unaware that this function was required.

3 EMPLOYEE BENEFITS

Most organizations attempt to provide all employees with adequate levels of training. While this is the goal, often times constraints do not allow for proper formal training. Effective policies, standards, and procedures can help meet that objective. The adage heard around many offices is, "If I have the time to do it over, why don't I have the time to do it right in the first place?" By making policies, standards, and procedures available, the staff will have the tools and processes necessary to complete their assignments. They will effectively help employees do their jobs better and will provide continuity.

When an employee leaves for a promotion or takes on a new job assignment, the employee replacing them must sometimes jump right into the assignment. Having desk procedures available and current ensures that the level of disruption will be kept to a minimum. Additionally, when a number of employees are performing similar functions, the procedures can assist management in evaluating employee performance. The business unit can guarantee uniform delivery of services and eliminate guesswork.

Probably the biggest benefit to new employees is that they will begin to feel comfortable more quickly. One of the reasons that new employees have a feeling of uneasiness is that many of them were proficient in their old job, and now are faced with a new set of tasks. Where they did not need to ask questions, now they are dependent on someone else to tell them everything they know and can remember about a specific task. Many jobs have different assignments throughout the year. An employee that has to do certain things for year-end activities might not remember to tell a new employee about them. Additionally, when an employee leaves, they often do not have the time to devote to helping someone in their old job. Effective policies, standards, and procedures will help during times of transition.

4 PREPARATION ACTIVITIES

Proper planning will provide the framework on which the activities associated with the design and development of the policies, standards, and procedures documents can be based. As discussed in the project management section, the task of developing written documents must be managed as a project. Each of the phases of a normal system development life cycle can be used during the company policies, standards, and procedures. In addition to those phases and their deliverables found in an SDLC, the planning and preparation for policy and procedure document requires some extra steps.

5 CORE AND SUPPORT TEAMS

It is strongly recommended that policies, standards, and procedures be developed by teams. As with any team project, there will be a need to have an established leader. This individual will be responsible for ensuring that content meets the organization's needs and that delivery dates are met. The team responsible for the policy development is normally referred to as the *Core Group*. They are representatives from the primary stakeholders of this project. Recent Core Groups have included members from the Information Protection Group, Information Systems, Auditing, and the Policy Approval Office.

It is very important that this team be composed of individuals who have a number of years with the organization. While they may not be content experts, they are needed to provide knowledge about the culture of the organization and what pitfalls to avoid. It is their knowledge about the organization and what can cause problems that is needed as a member of the Core Group. Use their experience to help create a document that has a chance of being accepted.

Key members of the Core Group will be the writer and editor. The person that does the writing should not be the same person who does the editing. Choosing these individuals may be the single most important aspect of the preparation process.

The *Support Team* is usually made up of representatives from each of the various business units. Their responsibilities will be to review and critique the initial drafts of the policies, standards, and procedures. They will be charged with representing their business unit at each review session and to make sure that the needs of their business unit are expressed and addressed. The Support Team will also be used to gather information on what concerns their senior management has on information security and what the Development Team should be doing to arrest those concerns.

The Support Team is also charged with keeping their business unit apprised of the progress being made in the development process. They should keep their management informed and report to the Core Group management.

6 FOCUS GROUP

Once the policy has been completed, it is recommended that a focus group be established to review the document. This is an important element in ensuring that the message of the policies and procedures is understood by the intended audience. A focus group will not be used for critiquing the documents, but can be used to see if the objective of the policy has been met.

7 WHAT TO LOOK FOR IN A GOOD WRITER/EDITOR

How do we know what to look for in a good writer? To begin with, look for someone who does not require constant supervision. Writers are normally self-starters and have exceptionally good project planning and organizational skills. Any time policies, standards, and procedures need to be written, there will be a lot of background work before anything of substance can be created. Therefore, it will be necessary to ensure that a timeline of deliverables is established and that the individual(s) chosen to complete the development can meet those dates.

A major portion of the implementation and acceptance process is dealing with people. Not just people — but management. The writer must have the ability to work effectively and pleasantly with personnel from all levels of the organization. It is not uncommon for a writer to interview an entry-level clerk and then have a meeting with the vice president of some business unit. The ability to write is only a small portion of the writer's job requirements. A writer must be able to work well with individuals within the organization.

The ability to check one's ego is an essential element of this individual's make-up. The ability to conduct an effective interview is another key attribute of the writer. Not only does the writer need to ask good questions, but he must be able to listen to the answers and follow up when necessary. A good interviewer not only listens to the words, but also watches the body language on the interviewee. Often times, more is learned from watching than from the words that are being said. Many times the words will state one thing, but the body gestures will give a totally different message. So, not only ask and listen, but watch and understand.

Finally, these individuals will need good writing and editing skills. Not everyone can be a writer and even fewer make good editors. The writer must be able to identify the target audience and prepare material to meet the audience's needs. Too many write at their knowledge and comprehension level and this can often lead to confusion and misunderstanding. Studies financed by the Veterans Administration indicated that the average informed consent statement is written at a graduate school level and fewer than a third of VA patients have had any college. To be effective, writers must always know the audience for which they are writing.

8 DEVELOPMENT RESPONSIBILITIES

Key responsibilities for the writer or editor include establishing the development plan. As discussed in the project management chapter (Chapter 2), there are a number of tasks and milestones to be established. It is the responsibility of this group to do the research and gather materials that can be used for policy, standards, and procedure development. The research material must be analyzed to determine if it can be used based on the needs and culture of the organization.

Understanding the culture or mental model of the organization is an essential element in creating a set of policies, standards, and procedures that will be accepted and implemented by the organization. As was discussed in Chapter 1, *Why Policies, Standards, and Procedures Are Needed,* there is a business need for these documents. When developing them, the organization mission or business objectives should be posted in the office or cubicle where the writing and editing are being done. Never lose sight of the business reasons that this project is being undertaken.

The project leader and the writer or editor (often the same individual) will have to establish the Development Team. These individuals will be responsible for providing input to the process and subject experts. Procedures will be developed by subject experts. The writers and editors will have to interview prospective candidates (subject writers), establish a scope statement for their specific assignments, and establish delivery dates. (The establishment of due dates is a mutual activity and as much concession to the subject writers other responsibilities must be made as possible.)

Additional responsibilities for the Project Team leader will be to establish the layout of the document page. In order for a policy to be a policy, it must look like a policy. Individuals involved in the development process are often thrown for a loop when the document they have spent so many hours creating is summarily dismissed because it does not look like a policy. In business, "form over substance" will win almost every time. Research the layout of existing policy statements and adopt the generally accepted presentation. This includes the page format (the masthead, page number and date location, and policy number).

9 OTHER CONSIDERATIONS

Taking on the task of writing and implementing policies, standards, and procedures can be a long-term activity, depending on how large or detailed the project needs to be. The involvement of personnel and the number of staff hours required to head up such a project may force the organization to look outside for writers and editors. Another factor in choosing these individuals is how quickly does the organization need to have the documents in place. All too often, organizations are faced with responding to an audit concern before they are willing to expend any resources on creating policies, standards, and procedures. The size and scope of the project, the possibility of a time constraint, and the skill set required may force organizations to look to contractors to fill this need.

10 KEY FACTORS IN ESTABLISHING THE DEVELOPMENT COST

The total cost of developing a quality document will vary from organization to organization. However, regardless of the industry, agency, or business, the components that make up the document development are basically consistent.

10.1 Research, Collect, and Organize the Information

It will be necessary to ferret out all existing policies, procedures, letters (Chairmen, President, Comptroller, General Letters, Business Unit Vice President, etc.) relating to the subject. It will be necessary to obtain copies of all laws, regulations, and requirements under which the organization is expected to function. These documents will have to be read to determine if they are still in effect. A good place to begin to create a list of such documents is with the Audit Staff. Over the years, they have been writing Audit Exceptions to either existing organization policy or good business practices (normally used when no organization policy exists). Once these documents have been located and read, it will be necessary to organize the material to meet the needs of the current project.

10.2 Conduct Interviews

Reading history is only the beginning process. To be effective, it will be necessary to interview senior management, department heads, first line supervisors, and users on how they use the resources and what would happen if the resource was lost, stolen, modified, or destroyed. The interview process should be used to get an understanding of where the organization is and how much control will be accepted.

Included in this process will be interviews with the Audit Staff. It is important to know and understand where they feel are the biggest areas of concern. The Legal Staff must also be included in this activity. They should be able to identify legal concerns (either laws, regulations, or potential litigation exposures). The Human Resources Staff can provide information on how personnel information should be handled.

10.3 Write the Initial Draft and Prepare Illustrations

Once the research and reading is finished, the interviews are complete, and the physical layout of the document has been determined, it will be necessary to begin to write the policies, standards, and procedures (usually in that order). How long will it take to write a policy? Well, that depends on many factors. Once all of the research has been completed, a good writer should be able to create an initial draft of a policy within 8 to 16 hours. The more experience the writer has in these areas, the better the results and the faster he or she can generally work. What causes the most problems is the desire to have the document perfect before anyone sees it. While this is a very human characteristic, it defeats the role of the proofreader and editor (their roles are discussed in Section 10.4).

It is during this time that any illustrations will be created. These could be graphs, charts, forms, flowcharts, or other visual aids. Typically, policies and standards do not contain illustrations. It is the procedure that often uses these to help explain the process being described.

10.4 Proofread and Edit

Running the spell checker is not the same as proofreading a document. It is recommended that different people assume the role of proofreader and editor. The advantage of a "fresh" set of eyes to examine the document can work wonders in creating a document that can be understood, accepted, and implemented.

The proofreader will review the document to ensure that spelling, grammar, and syntax are correct. This is an essential step in the review process. Eventually, the documents will be sent out to the review team (Review Panels will be discussed in Chapter 10) and if the document is not correct, the reviewers will spend their time correcting the punctuation and spelling and not comment on the content.

The individual responsible for editing will prepare the material for publication. Included in these responsibilities is to ensure that the message of the work makes sense. It is recommended that two editors be used — one who understands the technical side of the message and one who is a representative of the target audience. The objective of the policy, standard, and procedure is to take the message to a specific audience.

10.5 Choosing the Medium

Some organizations still require the printed document. If this is the case, then it will be necessary to include time for printing, collating, binding, shipping, and logging all numbered copies. The use of a physical medium is an added expense. Today, many organizations are using the intranet to post policies, standards, and procedures using HTML files or some other hypertext facility. The beauty of this revolution in publishing is that everyone has access to the most current copy of the document, and when an update is made it only needs to be made once.

10.6 Maintenance

Writing and publishing the documents is only the beginning of the process. It will be necessary to conduct a periodic review of the documents to determine if they are still relevant. The review should occur at least every 12 to 18 months.

11 REFERENCE WORKS

When preparing to develop policies, standards, and procedures, it will be advantageous to have access to a set of standard reference materials. These include but are not limited to a dictionary and thesaurus. While most word processor packages have a thesaurus, the spell checker is not a replacement for the dictionary. The dictionary will be used to understand the meaning of the word. Grammar texts can also be of use; however, the

grammar function of most word processor tools set is an excellent (although pedantic) way of ensuring proper grammar.

An important reference tool is the Office Administrator's Handbook. This document provides insight into how documents are constructed within an organization. The document can provide the way certain levels of management are referred to in print and how the organization itself is identified in print.

Financial reports, annual stockholder reports, audit findings, and other company documents will provide the reference material needed to ensure that newly created policies, standards, and procedures meet the needs of the organization and of management's fiduciary responsibilities.

12 MILESTONES AND TIMELINES

When writing policies, standards, and procedures, it will be prudent to establish milestones to help plan the activities, to budget resources, to control the phases or the project, and to set deliverables, as shown in Exhibit 1. These milestones, once tested for the implementation of one set of documents, can be used as a template for future document projects.

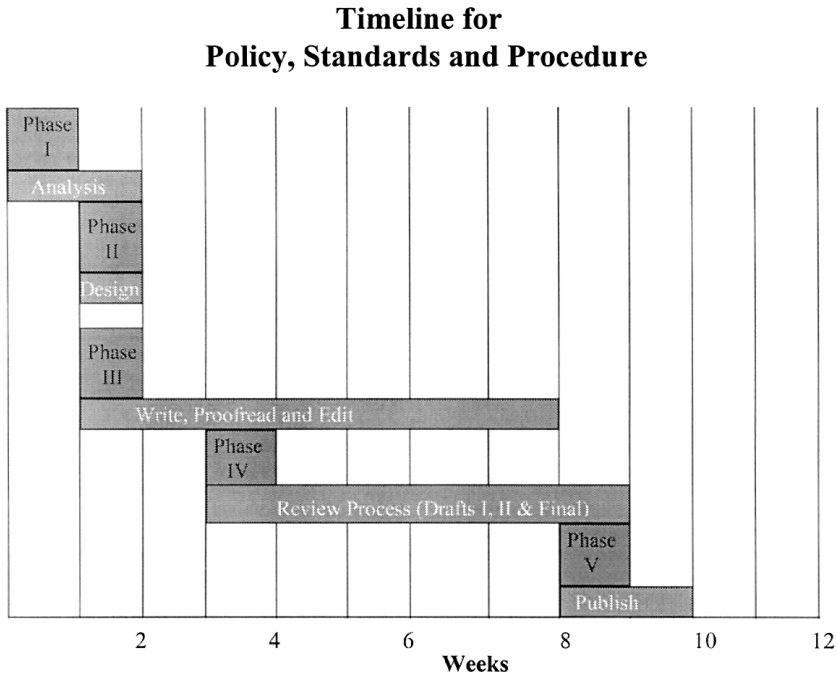

Exhibit 1. Development timeline.

13 RESPONSIBILITIES

Different groups within the organization will have different responsibilities with regard to the development and implementation of policies, standards, and procedures. *Senior Management* has the responsibility to sponsor, fund, and support the development project. They establish the organization's overall program goals, objectives, and priorities in order to support the enterprise business objectives or mission statement. Ultimately, the head of the organization (e.g., the CEO, Chairman, President, Director, etc.) is responsible for ensuring that adequate resources are applied to the program and that it is successful. They are also charged with setting the example from which all employees can follow.

13.1 Corporate Information Officer (CIO)

The CIO and support staff are responsible for directing the enterprise's day-to-day management of the information security program. The CIO is also responsible for coordinating all security-related interactions among the business units, departments, and service providers, both internal and external to the enterprise.

13.2 Application, System, and Information Functional Owners

These are the business unit management charged with the responsibility to provide appropriate security of the organization's information assets, including management, operational, and technical controls that support the overall policy directives and standards. They are responsible for monitoring these controls and ensuring that employees are in compliance with established controls.

13.3 Users

Users are responsible for following organization policies, standards, and procedures, for reporting security problems, and for attending regular security awareness, education, and training sessions.

14 DEVELOPMENT CHECKLIST

A checklist is an example of items that should be considered when working on a project. Checklists can be misleading in that some people believe that whatever is on the checklist must be all that there is to do. A checklist is a starting point, to be added to or subtracted from. Once a development and implementation cycle is complete, one will have a better idea of the chronology of what events must take place.

1. Research and gather policies, procedures, letters, and documents.
2. Analyze the material and determine which ones are still applicable.
3. Identify and prioritize the policies that must be updated or created.

4. Identify the team members for the Core and Support Teams.
5. Create a Scope Statement and a Statement of Work.
6. Create a working Table of Contents.
7. Establish a schedule, and post a project timeline.
8. Identify the policy and procedure approval process.
9. Form a Critique Panel.
10. Determine the physical characteristics of the document (page layout, etc.).
11. Determine the medium for the completed document (if hardcopy, there will be additional steps and materials to be ordered).
12. Write the initial policy (first draft).
13. Proofread and correct first draft.
14. Submit first draft to the Critique Panel.
15. Prepare a communication plan.
16. Review and reconcile comments from the Critique Panel.
17. Prepare second draft based on critiques.
18. Proofread and edit second draft.
19. Repeat steps 14 and 15.
20. Prepare Final Draft based on critiques.
21. Obtain approvals.
22. Prepare cover or transmittal letter.
23. Publish approved policies, standards, and procedures.
24. Create and conduct employee awareness presentations.
25. Establish a calendar to review policies, standards, and procedures on a regular basis.

15 SUMMARY

This chapter determined that the objectives of policies, standards, and procedures were:

- to state and clarify enterprise policy
- to define the duties and responsibilities and authority process
- to formalize duties
  - separation of duties
  - rotation of assignments

The benefits to employees for having well-written policies, standards, and procedures include:

Preparation activities:

- Core Group
- Support Team
- Focus Group
- Writer and editor attributes and development responsibilities

Key factors in establishing the development cost include:

- researching, collecting, and organizing information
- conducting interviews
- writing the initial draft and preparing illustrations
- proofreading and editing
- choosing the medium

Reference works were discussed and how they can help the development process.

Employee responsibilities examined include those of:

- Senior management
- CIO
- Application, System, and Information Owners
- Users

Finally, this chapter reviewed those elements that might make up a development checklist.

Chapter 4
Developing Policies

1 POLICY IS THE CORNERSTONE

The cornerstone of an effective information security architecture is a well-written policy statement. This is the source from which all other directives, standards, procedures, guidelines, and other supporting documents will spring. As with any foundation, it is important to establish a strong footing. As will be discussed, a policy performs two roles: one internal and one external.

A policy is senior management's directives to create an information security program, establish its goals, measures, and target and assign responsibilities. Management is faced with many choices in directing the protection of information resources. Some choices are easy and are based on cost and benefit analysis or return on investment. But others involve granting concessions, questions of enterprise strategic direction versus implementing information security controls. Once these decisions have been made, policy will have been created *de facto*. The task at hand is to take these decisions, common practices, or folklore and fashion them into published policy that can be used as the basis for protecting information resources and guiding employee behavior.

2 WHY IMPLEMENT AN INFORMATION SECURITY POLICY?

In the absence of an established policy, the organization's current and past activities become the *de facto* policy. Since there is no formal policy to be defended, the organization may be in greater danger of a breach of security, loss of competitive advantage, customer confidence, or government interference. By implementing policies, the organization takes control of its destiny. In the absence of established policies, the internal and external audit staffs and the courts can step in and set policy. Most organizations would prefer to establish their own policies instead of having some third party impose policy.

The goal of an information security policy is to maintain the integrity, confidentiality, and availability of information resources. The basic threats that can prevent an organization from reaching this goal are unauthorized

access, modification, disclosure, or destruction — whether deliberate or accidental — of the information or the systems and applications that process the information.

It is a well-accepted fact that it is important to protect the information resources essential to an organization, in the same manner that it is important to drive on the correct side of the road. Unlike the driving scenario, which has regulations and laws to support it, the protection of information is all too often left to the individual. As with the driving problem, everyone knows what solutions are available for protecting information. Identifying these requirements is not enough; in order to enforce controls, it is necessary to have a formal policy. This will form the basis for all necessary controls.

3 SOME MAJOR POINTS FOR ESTABLISHING POLICIES

When developing the policy, there is as much danger in saying too much as there is in saying too little. The policy should provide the direction required by the organization while maintaining business unit management discretion in the actual implementation of the policy. The more intricate and detailed the policy, the more frequent the update requirements and the more complicated the training process for employees.

While it is important to keep to the facts and keep the document brief, it is also important to include a clear discussion on the proprietary rights of the organization. The employees deserve to know what is expected of them and how they will be apprised with respect to their obligations. By establishing well-written policies, the enterprise can expect that management will (if properly trained) take approximately the same course of action in similar circumstances.

4 WHAT IS A POLICY?

Policy means different things to different people. For our purposes, the term "policy" is defined as a high-level statement of enterprise beliefs, goals, and objectives and the general means for their attainment for a specified subject area. A policy is brief (which is highly recommended) and set at a high level (see Exhibit 2).

Because policy is written at a broad level, organizations must also develop standards, guidelines, and procedures that offer employees, managers, and others a clearer method for implementing the policy and meeting the organization's business objectives or mission.

A policy is not a specific and detailed description of the problem and each step that is needed to implement the policy. A policy on requiring access control for remote users has exceeded its scope if there is a discussion about passwords, password length, password history, etc.

Exhibit 1. Sample e-mail policy.

The Company maintains a voice-mail system and an electronic-mail (e-mail) system to assist in the conduct of business within the Company. These systems, including the equipment and the data stored in the system, are and remain at all times the property of the Company. As such, all messages created, sent, received, or stored in the system are and remain the property of the Company.

Messages should be limited to the conduct of business at the Company. Voice-mail and electronic-mail may not be used for the conduct of personal business.

The Company reserves the right to retrieve and review any message composed, sent, or received. Messages may be reviewed by someone other than the intended recipient.

Messages may not contain content that may reasonably be considered offensive or disruptive to any employee. Offensive content would include, but would not be limited to, sexual comments or images, racial slurs, gender-specific comments, or any comments that would offend someone on the basis of his or her age, sexual orientation, religious or political beliefs, national origin, or disability.

Employees learning of any misuse of the voice-mail or electronic-mail system or violations of this policy shall notify the Director of Human Resources immediately.

5 DEFINITIONS

5.1 Policy

A policy is a high-level statement of enterprise beliefs, goals, and objectives and the general means for their attainment for a specified subject area. Exhibit 1 is an example of a company e-mail policy.

5.2 Standard

Standards are mandatory activities, actions, rules, or regulations designed to provide policies with the support structure and specific direction they require to be meaningful and effective. They are often expensive to administer and, therefore, should be used judiciously.

6 COMPUTER VIRUS PROTECTION

Policy: Information custodians are responsible for providing a safe and secure processing environment in which information can be maintained with integrity.

Standard: Custodians of information processing systems must ensure that the system is free from destructive software elements (such as viruses) that would impair the normal and expected operation of the system.

6.1 Guidelines

Guidelines are more general statements designed to achieve the policy's objectives by providing a framework within which to implement procedures. Where standards are mandatory, guidelines are recommendations.

Policy: Information custodians are responsible for providing a safe and secure processing environment in which information can be maintained with integrity.

Standard: Custodians of information processing systems must ensure that the system is free from destructive software elements (such as viruses) that would impair the normal and expected operation of the system.

Guidelines:

- Where available, a virus prevention, detection and recovery package should be installed.
- Employees having access to computer systems should attend a training session on the virus threat to understand the damage a virus infection can inflict and understand their personal responsibility for protecting their own systems.

6.2 Procedures

Procedures spell out the specifics of how the policy and the supporting standards and guidelines will actually be implemented in an operating environment.

Policy: Information custodians are responsible for providing a safe and secure processing environment in which information can be maintained with integrity.

Standard: Custodians of information processing systems must ensure that the system is free from destructive software elements (such as viruses) that would impair the normal and expected operation of the system.

Guidelines:

- Where available, a virus prevention, detection and recovery package should be installed.
- Employees having access to computer systems should attend a training session on the virus threat to understand the damage a virus infection can inflict and understand their personal responsibility for protecting their own systems.

Procedure:

- Viruses often are transmitted through public domain software. Software that is public domain (i.e., nonlicensed software also called "shareware" or "freeware") or the employee's personal property shall not be permitted on company equipment without the explicit authorization of organization management and after being certified as being virus free.

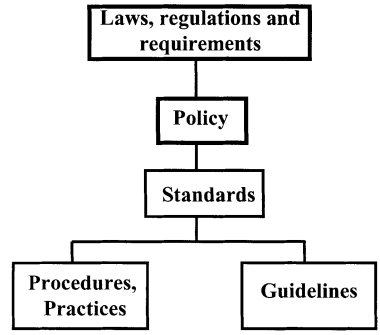

Exhibit 2. Policy chart.

- Employees are to turn off and lock up desktop systems at the end of the workday to prevent unauthorized access and possible virus contamination.
- Employees are to use the "write protection" tabs on diskettes whenever possible.
- Employees are to report any type of unauthorized access, theft, and virus infection to the Information Protection group or the Help Desk upon discovery.

Some organizations issue overall information security documents, regulations, handbooks, or other such manuals. These can be a mix of policies, standards, guidelines, and procedures, since they address a closely linked subject. While these documents can serve as an important tool for employee use of systems and overall security, it is often helpful to distinguish between policy and the implementation pieces. The key reason for this identification is to assist in promoting management flexibility and cost-effectiveness by allowing alternative approaches to the implementation process.

Many organizations seem to get along with informal policies. These exist much like folklore and customs, passed on to one employee after another by word-of-mouth. So why then is there actually a need to write and publish a policy? Information is a unique enough asset to warrant a written statement. For many employees, there is a great deal of confusion about information, how to handle it, what its classification is, and who is its owner.

As discussed in Chapter 1, there may be legal or regulatory reasons why an information security policy must be published. Most important, only a written policy can be convincing in courts of law, customer contracts, vendor relations, acquisitions, and public relations.

7 POLICY KEY ELEMENTS

To meet the needs of an organization, a good policy should:

- Be easy to understand. As discussed in Chapter 1, it is important that the material presented meet the requirements of the intended audience. All too often policies, standards, and procedures are written by subject experts and given to a general-use audience. The material is often written at a college level when the average reading and comprehension level in the workplace is that of a sixth grader (a 12-year-old).
- Be applicable. When creating policy, the writer may research other organizations and copy that document verbatim. What really must be done is to ensure that whatever is written meets the needs of your specific organization.
- Be do-able. Can the organization and its employees still meet business objectives if the policy is implemented? I have seen many organizations that have written the ultimate security policy, only to find out that it was so restrictive that the mission of the organization was placed at risk.
- Be enforceable. Do not write a self-defeating policy such as "Use of the company-provided telephone is for business calls only." For most organizations, this may in fact be the policy, but almost every phone in the facility is used daily for personal calls. What might make a better policy is one that says "Company-provided telephones are to be used for management-approved functions only." This opens up some latitude and still meets the business need.
- Be phased in. It may be necessary to allow the organization to read and digest the policy before it takes effect. Many organizations publish a policy and then require the business units to submit a compliance plan within a specific number of days after publication. This provides the business unit managers a period of time to review the policy, determine where their organization might be deficient, and then submit a timetable for compliance. These compliance letters are normally kept on file and are made available to the audit staff.
- Be proactive. State what has to be done: do not get into the rut of making pronouncements — "Thou shalt not!!!!" Try to state what can be done and what is expected of the employees.
- Avoid absolutes. Never say never. Be diplomatic and understand the politically correct way to say things. When discussing sanctions for noncompliance, some organization have stated that "employees violating this policy will be subject to disciplinary sanctions up to and including dismissal without warning," when the policy could have something like, "Employees found in noncompliance with this policy will be deemed in violation of the Employee Standards of Conduct." The Standards of Conduct state that employees will suffer disciplinary sanctions up to and including dismissal. Use the kindlier, gentler approach.

- Meet business objectives. Security professionals must learn that the controls must help the organization to an acceptable level of risk. One hundred percent security is zero percent productivity. Whenever controls or policy impact the business objectives or mission or the organization, then the controls and policy will lose. Work to understand that the policy exists to support the business, not the other around.

The information security policy should cover all forms of information. In 1965 there was an announcement about the move to the "paperless office." The advent of the third-generation computer had many believing that all information would be stored electronically and that paper would become obsolete. Computer-held information only accounts for at best 20 percent of an organization's information. The paper document is still supreme. Make certain that any policy regarding information security and protection includes all forms of information from inception to destruction.

8 POLICY FORMAT

The actual format (layout) of a policy will depend on what policies look like within a specific organization. It is very important that any policy developed look like published policies from the organization. Some members of the review panel will be unable to read and critique the new policy if it does not look like a policy.

Policies are generally brief (in comparison to procedures and practices), usually not much more than a page or two of material.

> Information is an asset and the property of the organization. All employees are responsible for protecting that asset from unauthorized access, modification, disclosure, or destruction.

When creating policies, it is helpful to understand that there are generally three types of policies that will be used during the development of a security document. The three basic types of policy are:

1. Program policy — this is used to create an organization's overall information security vision.
2. Topic-specific policies — these address specific topics of concern. There will normally be a topic-specific policy for each section of an Information Security Document.
3. Application-specific policies — these focus on decisions taken by management to protect particular applications or systems.

8.1 Program Policy

Senior management is responsible for issuing a Program Policy to establish the organization's information security policy and its basic construction. This high-level policy defines the intent of the information security

program and its scope within the organization. It also assigns responsibilities for implementation and compliance with the policy.

The components of a Program Policy should include the following items.

8.1.1 Intent. The intent portion of the policy normally defines the goals of the program. When discussing information, most program policies concentrate on protecting the confidentiality, integrity, availability, and authenticity of the information resources. Additionally, it will attempt to establish that information is an item of value to the enterprise and, as such, must be protected from unauthorized access, modification, disclosure, or destruction — whether accidental or deliberate.

8.1.2 Scope. The scope establishes which resources of the organization are covered by the policy. For purposes herein, this could include all electronically stored, processed, transmitted, printed, faxed, or discussed information, whether accessed by or created by regular, full-time employees, contract personnel, consultants, customers, suppliers, vendors, or others.

8.1.3 Responsibilities. Typically, this section of the policy will identify three or more specific roles and their responsibilities. The first role to be discussed is that of management and they are typically charged with implementing and supporting the program. Employees are responsible for adhering to the policy and reporting any suspected problems to their management. The policy could also establish an office responsible for day-to-day administration of the policy.

8.1.4 Compliance. The policy will generally discuss two issues regarding compliance:

- Who is responsible for ensuring compliance to the policy objectives. Normally, two specific groups are identified:
  - First line supervision and its role in monitoring employee activities
  - The Internal Audit Staff and its responsibility to conduct formal reviews
- What happens when the policy is violated? When developing and implementing the policy, keep in mind that violations of the policy can be unintentional. The violation could be a result of lack of training and awareness. Therefore, it will be necessary to establish a review process for each violation case-by-case as opposed to creating mandatory sanctions. Allow management to have some leeway when reviewing problems.

8.2 Topic-Specific Policy

In each section of the procedure document, the material will begin with the organization's policy statement. Unlike the Program Policy, the Topic-

Specific Policy narrows the focus to one issue at a time. Creating a procedure document to support the policy statement will be discussed. It will be in this document or, in some cases, in stand-alone policies where this approach will be used.

The basic components of a Topic-Specific Policy include the following items.

8.2.1 Thesis Statement. To establish a policy on a specific topic, the writer must interview management and determine what are the relevant issues to be addressed. As in the Intent section of the Program Policy, the goals and objectives of the policy should be identified.

8.2.2 Relevance. The Topic-Specific Policy also needs to establish to whom the policy applies. In addition to whom, the policy will want to clarify where, how, and when the policy is applicable. Is the policy only enforced when employees are in the work-site campus or will it extend to offsite activities?

8.2.3 Responsibilities. The establishment of roles and responsibilities is usually included in the Topic-Specific Policy. Whenever identifying an individual in a policy or procedure, it is always best to identify the position or job title rather than an individual by name. Job functions are normally more permanent than people.

8.2.4 Compliance. Here it might be appropriate to describe in some detail the behavior that is unacceptable and the consequences of that behavior. The responsibility for monitoring compliance should also be identified.

8.2.5 Additional Information. For a Topic-Specific Policy, an identification of individuals (by job title) and departments that the user can contact for additional information should be made available. Where to obtain copies of associated procedures should also be included.

8.3 Application-Specific Policy

Program-Level and Topic-Specific Policies both address policy on a broad level; they usually encompass the entire enterprise. The Application-Specific Policy focuses on one specific system or application. As the construction of an organization security architecture takes shape, the final element will be the translation of Program and Topic-Specific Policies down to the application and system level.

Many security issue decisions apply only at the application or system level. Some examples include:

- Who has the authority to read or modify application data?
- Under what circumstances can data be read or modified?

- How is remote access to be controlled?

To develop a comprehensive set of system security policies, use a process that determines security rules (policy) from business and mission objectives.

- Define the business objectives. Then establish which security tools will support those objectives.
- Establish the rules for operating the application or system. Define who has access to what resources and when.
- Determine if automated security tools can help administer the policy.

9 POLICY CONTENT

The written policy should clear up confusion, not generate new problems. When preparing a document for a specific audience, remember that the writer will not have the luxury of sitting down with each reader and explaining what each item means and how it impacts the users daily assignments. Know the audience for whom the policies are being developed. Remember the reading and comprehension level of the average employee. When writing the policy, remember the 6 Ws of Journalism 101:

1. What — what is to be protected (the Intent)?
2. Who — who is responsible (Responsibilities)?
3. Where — where within the organization does the policy reach (Scope)?
4. How — How will compliance be monitored (Compliance)?
5. When — when does the policy take effect?
6. Why — why was the policy developed?

A number of actual information security policy statements are examined below. As each one is examined, please use the above six items as a checklist to determine the completeness of each policy. Items 1 through 4 have more weight than items 5 and 6. All six are important, bust some are more important than others.

9.1 Example No. 1: A Utility Company

Information is a valuable corporate asset. Business continuity is heavily dependent on the integrity and continued availability of certain critical information and the means by which that information is gathered, stored, processed, communicated, and reported. As such, steps will be taken to protect information assets from unauthorized use, modification, disclosure, or destruction, whether accidental or intentional.

The protection of these assets is a basic management responsibility. Senior management is responsible for:

- identifying and protecting computer-related information assets within their assigned area of management control
- ensuring that these assets are used for management-approved purposes only; ensuring that all employees understand their obligation to protect these assets
- implementing security practices and procedures that are consistent with the Company Information Asset Security Manual and the value of the asset
- noting variance from established security practice and initiating corrective action

Example No. 1 addresses the checklist as follows:

1. What — what is to be protected (the Intent) — "Information is a valuable corporate asset … As such, steps will be taken to protect information …"
2. Who — who is responsible (Responsibilities) — "The protection of these assets is a basic management responsibility."
3. Where — where within the organization does the policy reach (Scope) — "Ensuring that all employees understand their obligation to protect these assets."
4. How — how will compliance be monitored (Compliance) — "Noting variance from established security practice and initiating corrective action."
5. When — when does the policy take effect?
6. Why — why was the policy developed?

This is a fairly well-written policy. If there is any major critique item, it might be that the topic at times gets lost. As with any good writing technique, it is important to begin with a strong topic sentence. This policy starts out well — "Information is a valuable corporate asset." — but it just kind of lets it hang out there. Additionally, the policy limits the scope by identifying a Senior Manager responsibility as "identify computer-related information assets." To make the sentence stronger, continue the sentence with "… and all employees are responsible for protecting it."

9.2 Example No. 2: Medical Service Organization

The Medical Service Association shall provide an appropriate level of security to:

- maintain the reliability, integrity, and availability of its assets
- prevent and detect misuse
- protect information assets against unauthorized modification, disclosure, or destruction (whether accidental or intentional)
- satisfy legal and contractual requirements for security

- provide enforcement and recovery guidelines (including insurance coverage) for instances when a compromise of security is detected
- protect and provide a secure and safe work environment for its employees

Expenditures for security generally shall not exceed the value of the asset being protected.

Management Analysis Department's Security Unit shall be the central authority for developing, monitoring, and enforcing associationwide policies, procedures, and guidelines.

Management of each department shall be responsible for:

- ensuring adherence to all Association security policies, procedures, and guidelines
- continually assessing the department's specific security risk
- developing and maintaining a disaster recovery plan that both defines and protects department assets from unauthorized access and ensures their recovery from any misuse or destruction by human or natural means
- providing adequate security training of department personnel based on the Association Security Training Plan

All new product or system development shall include adequate security internal control, and disaster recovery elements.

Any use of Association assets for other than their intended purpose is considered a misuse and is a violation of this policy.

Violations or suspected violations of any Association policy or procedure must be reported immediately to department management and the Association Security Officer or his appointed representative(s). Violators may be subject to immediate disciplinary action up to and including termination of employment and criminal prosecution, if appropriate.

Example No. 2 addresses the checklist as follows:

1. What — what is to be protected (the Intent) — Eventually the policy establishes that " the Association shall provide an appropriate level of security … of its assets … and protect information assets …"
2. Who — who is responsible (Responsibilities) — The policy does establish that "Management of each department shall be responsible for: …" and then list a number of items.
3. Where — where within the organization does the policy reach (Scope) — The policy does not seem to establish if this is Association-wide, or exactly where is the scope of the policy.
4. How — how will compliance be monitored (Compliance) — The policy does establish that "Management … is responsible for … ensur-

ing adherence to all Association security policies, procedures, and guidelines."
5. When — when does the policy take effect?
6. Why — why was the policy developed?

This policy meets most of the checklist guidelines, but it misses some others and then adds pieces of information, such as the discussion on expenditures, that probably belong somewhere else. Again, a strong topic sentence is missing. If one has the attention of a reader, the place to get them hooked is the first sentence. Sell the policy in the opening sentence. The policy does make a strong statement about what can occur if noncompliance is found.

9.3 Example No. 3: Power Company

Policy Statement

It is the policy of the Power and Light Company to protect all company information from disclosures that would violate company commitments to others or would compromise the company's competitive stance.

Employee Responsibilities

Employee responsibilities are defined in Company Procedure AUT 15. Violations of these responsibilities are subject to appropriate disciplinary action up to and including discharge, legal action, or having the matter referred to law enforcement agencies.

Example No. 3 addresses the checklist as follows:

1. What — what is to be protected (the Intent) — The policy statement establishes that "company information … that would violate company commitments … or compromise … competitive stance …" must be protected.
2. Who — who is responsible (Responsibilities) — The policy does establish "Employee responsibilities."
3. Where — where within the organization does the policy reach (Scope)?
4. How — how will compliance be monitored (Compliance)?
5. When — when does the policy take effect?
6. Why — why was the policy developed?

While this policy does meet one of the main requirements of a policy, that it be brief, it appears to be too brief. Some very important elements are left out, especially what role management will play in this policy and how compliance will be monitored. The policy also seems to exclude information about personnel.

The opening sentence discusses the "policy" of the company. The document was drafted as a policy statement. It is not necessary to add the word "policy" to the text. Let the words establish what the policy is.

9.4 Example No. 4: Manufacturing Company (International)

Basic Policies

The Company relies heavily on various kinds of information resources in its daily operations. These resources include data-processing systems, electronic-mail, voice-mail, telephones, copiers, facsimile machines, and other information-generation and -exchange methods. It is very important for users to recognize that these resources are made available to them to help the company meet short- and long-term goals, objectives, and competitive challenges. Any improper use of any resource **is not** acceptable and **will not** be permitted.

The company policies listed here form the basis for the IRPP:

1. Data and information about the operation of the company and its employees are collected and retained only to satisfy legitimate business purposes or as required by law.
2. Protecting company information is every employee's responsibility. Company people share a common interest in ensuring information is not intentionally, accidentally, or improperly disclosed, lost, or misused.
3. Positive steps must be taken to prevent improper disclosure of company information and unauthorized access to company information resources.
4. Data, information, and processing resources are company assets that may be used only for management-approved company business purposes and not for personal or any other kinds of use of gain.
5. Like any company asset, the company reserves the right to inspect information resources and their use at any time.
6. Company records and information are available to individuals only on a need-to-know basis. Access or attempted access to information and the use of information resources outside one's authority are prohibited.
7. Established corporate and unit procedures are to be used for budgeting, approval, and acquisition of information-processing facilities, equipment, software, and support services.
8. Protective measures must be provided to control access to and protect the integrity of all information systems that process information.
9. Appropriate safeguards must be built into information-processing facilities. These safeguards should minimize the extent of loss of information or processing support that could result from such haz-

ards as fire, water, or other natural disasters while at the same time maintaining operational effectiveness. Business recovery plans must provide for a continuation of vital business functions if loss failure should occur.
10. Independent reviews to ensure that program objectives are being met are an integral part of this effort. These reviews may be conducted by Corporate Auditing, a unit's internal audit staff, or external auditors.
11. Deliberate unauthorized acts against company or customer automated information system(s) or facilities, including but not limited to misuse, misappropriation, destruction of information or system resources, the deliberate and unauthorized disclosure of information or the use of unauthorized software/hardware, will result in disciplinary action as deemed by management.

Example No. 4 addresses the checklist as follows:

1. What — what is to be protected (the Intent) — Items 4, 5, and 8 can be used and modified to form the text of what is to be protected.
2. Who — who is responsible (Responsibilities) — Item 2 seems to address this issue.
3. Where — where within the organization does the policy reach (Scope)?
4. How — how will compliance be monitored (Compliance) — Item 10 addresses formal review.
5. When — when does the policy take effect?
6. Why — why was the policy developed — Most of the "policy" seems to be addressing this element.

Basically this is a good policy; it can be improved upon by moving the big-ticket items to the top. Whenever a policy is developed, start right out with what the topic to be discussed is all about. Lead with this information in the first sentence.

9.5 Example No. 5: Insurance Company

Business information is an essential asset of The Company. This is true of all business information within The Company regardless of how it is created, distributed, or stored and whether it is typed, handwritten, printed, filmed, computer generated, or spoken.

All employees are responsible for protecting corporate information from unauthorized access, modification, duplication, destruction, or disclosure — whether accidental or intentional. This responsibility is essential to Company business. When information is not well protected, Company can be harmed in various ways such as significant loss to market share and a damaged reputation.

Details of each employee's responsibilities for protecting Company information are documented in the Information Protection Policies and Standards manual. Management is responsible for ensuring that all employees understand and adhere to these policies and standards. Management is also responsible for noting variances from established security practices and for initiating corrective actions.

Internal auditors will perform periodic reviews to ensure ongoing compliance with Company information protection policy. Violations of this policy will be addressed as prescribed in the Human Resource Policy Guide for Management.

Example No. 5 addresses the checklist as follows:

1. What — what is to be protected (the Intent) — Paragraph number 1 addresses this issue.
2. Who — who is responsible (Responsibilities) — Paragraph number 2 addresses employee responsibilities and paragraph 3, sentence 2 establishes management role.
3. Where — where within the organization does the policy reach (Scope) — Paragraph number 1 addresses the scope of the policy.
4. How — how will compliance be monitored (Compliance) — Paragraph number 3 refers employees to a company document that provides more detail on the responsibilities. Paragraph number 4 establishes the formal review process.
5. When — when does the policy take effect?
6. Why — why was the policy developed — Paragraph number 1, sentence number 1 and paragraph 2, sentence 3 are used to meet this guideline.

This policy is good. It is clear, crisp, and concise.

10 ADDITIONAL HINTS

To have even the slightest hope of being successful, the policy must receive some level of visibility. Visibility takes a number of forms. The first, and probably most important form, will be management support. The issue of information security is not contained within the Information Systems organization. It is an enterprisewide concern and, thus, any policy relating to the protection and security of organization information must come from the highest possible level within the enterprise. In Chapter 11 on Selling the Document, strategies used to gain management and employee support are discussed. For now, one should begin to formulate a plan on how to get senior management support.

As discussed in Chapter 2, one needs a communication plan to take the message policy and all of its ramifications to the employees. This plan should include an employee awareness program. The program should in-

clude all existing and incoming (new hires) employees. If the organization desires to have contract personnel be compliant with the policies, then this must first be negotiated through the language of the contract. It is permissible to include contract personnel in the list of those that must comply with the policy; however, the actual compliance piece must be included in the language of the purchase order and the contract.

11 PITFALLS TO AVOID

Effective policy statement is not an oxymoron. If properly drafted, a policy statement can actually improve productivity rather than add to organizational overhead. The following is a ten-step approach to help improve the likelihood of having a successful policy implementation process.

1. Review existing policies — before writing a new policy, review what already exists. It is easier to update an existing policy than it is to gain acceptance to a totally new concept.
2. Make the organization's business objectives or mission an active part of the policy — there is a reason that policies are created, and that is to support the activities of the enterprise. To help gain acceptance, use the language in your organization's "Shared Beliefs" or "Corporate Vision" in the policy statement.
3. Make policies look like policies — take the time to ensure that whatever is created looks like existing policies. All too often, the message gets lost because the format is unfamiliar. Save the development team some grief and research the policy format of the organization.
4. Watch out for grammar and spelling — the worst thing that one can do is to send out a draft document that has not been edited for spelling and grammar. Show the user community that proper care has been taken, by looking out for the "little" things; the chances of success will be increased.
5. Streamline the language — most advanced writing courses have the students explore all of the elements of language. Painting pictures through the use of prose; while this might be effective in a class in writing fiction, it will not help in a policy document.
6. Security is not attainable — be realistic in policy implementation. The most secure computer system is one that is turned off, locked away, and unplugged. A computer in this condition is secure, but productivity is probably going to be impacted. Seek out an acceptable level of security.
7. Remember the audience — whenever writing, remember who the intended audience is. The majority of the readers will not be technical or security professionals. Ensure that the words are understandable.
8. Sell the policy prior to introduction — to be discussed later; but for now, remember that senior management must be fully aware of the

policy and understand how it applies to their organization before it is submitted to them for approval.

9. Keep the message brief — long-winded or complicated policies often lead to trouble. Keep the policy as simple as possible. This will allow for a limited variation on interpretation and, by being brief, there will be a better chance that someone will actually read the policy.
10. Take the message to the people — be prepared to develop employee awareness programs for the implementation of the policy.

12 SUMMARY

The policy is the cornerstone of an organization's information security architecture. A policy is important to establish both internally and externally what an organization's position on a particular topic might be.

This chapter defined what a policy is and what it is not. Also included were definitions for:

- policy
- standard
- guideline
- procedure

Next, there was an examination of the key elements of a policy:

- be easy to understand
- be applicable
- be do-able
- be enforceable
- be phased in
- be proactive
- avoid absolutes
- meet business objectives

This chapter also provided a review of what the policy format might be and then discussed the three basic types of policy:

1. Program Policy
2. Topic-Specific Policy
3. Application-Specific Policy

The chapter also looked at the policy content and a checklist based on the elements found in a journalism class:

- What — the intent of the policy
- Who — employee responsibilities and obligations
- Where — the scope of the policy
- How — compliance

- When — when the policy takes effect
- Why — the selling of the policy

Finally, five actual policy statements were examined and critiqued, based on the checklist and some helpful hints and pitfalls to avoid.

Chapter 5
Information Classification

1 INTRODUCTION

The next four chapters are devoted to addressing specific topics and what the policies for those topics might look like. Included in the text is a formal discussion on each of the topics and examples of existing policy statements. The chapter critiques these policies and establishes the framework for the development of such policies for any organization. The first topic discussed will be information classification. From there, Chapter 6 examines the need for an e-mail policy and then an Internet policy along with the supporting awareness program needed for Internet compliance. Finally, a basic list of corporate-level policies that every organization should have is established, along with the slight modification required to support an information security program.

2 OVERVIEW

Information is an asset and the property of the organization. All employees are to protect information from unauthorized access, modification, disclosure, and destruction. Before employees can be expected to protect information, they must first understand what they have. An information classification policy and methodology will provide them with the help they need.

There are four essential aspects of information classification: (1) information classification from a legal standpoint, (2) responsibility for care and control of information, (3) integrity of the information, and (4) the criticality of the information and systems processing the information. Examples of how the classification process fits into the application and system development life cycle will be presented to assist you in the development of your own information classification process.

3 WHY CLASSIFY INFORMATION?

Organizations classify information in order to establish the appropriate levels of protection for those resources. Because resources are limited, it

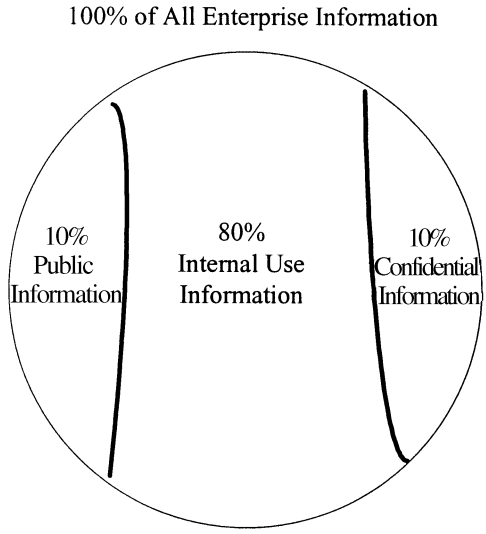

Exhibit 1. Information classification breakdown.

will be necessary to prioritize and identify what really needs protection. One of the reasons to classify information is to ensure that scarce resources be allocated where they will do the most good. All information is created equal, but not all information is of equal value (see Exhibit 1).

The old concept in computer security was that everything is closed until it is opened. However, after nearly 20 years of working with companies in establishing information classification systems, this author has found that nearly 90 percent of all enterprise information needs to be accessed by employees or available through public forums. Because resources are limited, the concept that all information is open until it requires closing is perhaps a better way of protecting information.

Most organizations do not have information that is all of the same value. Therefore, it is necessary to at least develop an initial high-level attempt at classification. This should be done, if for no other reason than to ensure that budgeted resources are not misused in protecting or not protecting information assets. Before employees can protect information assets, they must first have a mechanism in place that allows them to establish the value of the information. An information classification system and a scoring methodology that relies on common sense and a knowledge of the corporate culture and market sensitivity can be a significant advantage for most organizations.

Exhibit 2. Fortune 500 managers rate information importance.

Deloitte & Touche	Rate 1–3	Ernst & Young
1	Availability	2
3	Confidentiality	3
2	Integrity	1

Note: 1 = most important, 2 = next, 3 = least.

4 WHAT IS INFORMATION CLASSIFICATION?

An information classification process is a business decision process. When developing an organization's system, it will be necessary to limit the role of the security professionals and the computer technicians. The project to develop an information classification system is one in which the business side of the enterprise must take an active role (see Exhibit 2).

In a recent pair of surveys, the Big Four Accounting firms of Ernst & Young and Deloitte & Touche interviewed Fortune 500 managers and asked them to rank in importance to them information availability, confidentiality, and integrity. As can be seen from the results in Exhibit 2, the managers felt that information needed to be available when they needed to have access to it. Implementing access control packages that rendered access difficult or overly restrictive is a detriment to the business process. Additionally, other managers felt that the information must reflect the real world. That is, controls should be in place to ensure that the information was correct. Preventing or controlling access to information that was incorrect was of little value to the enterprise.

5 ESTABLISH A TEAM

Because the establishment of an information classification system and policy is a business function, it will be necessary to create a team for this project. It is recommended that there be two teams: Core Group, made up of three to five members, and a Support Team. The Support Team should consist of members from each of the major user departments or groups. The Core Group will be responsible for actually drafting the information classification policy. This will be accomplished after interviewing each of the user departments and determining their needs.

The Support Team will be used for two vital elements in this process. They will review and critique the information classification policy and they will assist in the sale of the policy to their management. To be effective, the policy will have to be accepted by all management. To be accepted, it will be necessary to sell this product to each of the managers based on their in-

dividual needs and business objectives. Using the Support Team members, one will be able to determine what each manager is expecting. Once the draft policy has been reviewed by the Support Team (probably twice) and their comments addressed, it is strongly recommended to set up a meeting with key management personnel.

These meetings should be in the individual manager's office and should have one or two representatives from the Core Group and a Support Team member from the policy development team. The objective of this session is to quickly explain what the policy is about and how it will assist them in meeting their mission, and then to answer any questions they might have. By having input from personnel from that manager's organization will assist in the acceptance of the information classification policy.

6 DEVELOPING THE POLICY

The first cut at the development process is to examine information from two perspectives:

Sensitivity — the need for confidentiality, integrity, and controlled usage
Availability — information that is there when it is needed

It may be necessary to examine examples of different kinds of information found within the organization. Each of the Support Team members should be prepared to discuss examples of the kinds of information used within their organization. It will be necessary to have information examples from all of the organizations: human resources, engineering, financial, budget, legal, information systems, and administrative records.

As a team, examine each of the examples of corporate information and apply them to a scoring table like the one pictured in Exhibit 3. Using the information gained from this process, the team should be able to establish classification categories and criteria for confidentiality, integrity, and availability that:

- are based on the impact to the business or mission
- can be clearly and consistently interpreted by managers and employees
- will result in different protective actions for each category

Exhibit 3. Priority matrix.

	Impact to the Organization		
	Low	**Medium**	**High**
Probability			
Low	1	4	7
Medium	2	5	8
High	3	6	9

If the difference between two types of information is not important to the organization from a confidentiality or availability standpoint, then do not include it. Make the language and the categories as simple as possible. When developing a category system, try the categories out on different groups of managers and solicit their input. It might be beneficial to conduct two or three brainstorming sessions to test out the category possibilities.

7 RESIST THE URGE TO ADD CATEGORIES

Keep the number of information classification categories to a minimum. If two possible categories do not require substantially different treatment, then combine them. The more categories available, the greater the chance for confusion among managers and employees. Normally, three or four categories should be sufficient to meet the organization's needs.

Additionally, avoid the impulse to classify everything the same. To simplify the classification process, some organizations have flirted with having everything classified as confidential. The problem with this concept is that confidential information requires special handling. This would violate the concept of placing controls only where they are actually needed, and would require the organization to waste limited resources protecting assets that do not really require that level of control.

Another pitfall to avoid is to take the information classification categories developed by another enterprise and adopt them verbatim as one's own. Use the information created by other organizations to assist in the creation of the organization's unique set of categories and definitions.

8 WHAT CONSTITUTES CONFIDENTIAL INFORMATION

There are a number of ways to look at information that may be classified as confidential. A number of statements relating to confidential information are examined below. The first is a general statement about sensitive information.

For a general definition on what might constitute confidential information, it may be sufficient to define such information as:

> Information if disclosed could violate the privacy of individuals, reduce the company's competitive advantage, or could cause damage to the organization.

The *Economic Espionage Act of 1996* (EEA) defines "trade secret" information to include "all forms and types of financial, business, scientific, technical, economic, or engineering information" regardless of "how stored, compiled, or memorialized." The EEA has a two-edged sword; while it is illegal for someone to steal trade secret information, the Act requires that the owner must take reasonable measures to keep the information se-

cret, and it must be shown that the information derives value from being kept secret.

There are a number of other information classification types that have been available over the years. Take just a minute to review copyright, patent, and trademarks.

Copyright — at regular intervals, employees will be creating new work in the form of application programs, transactions, systems, Web sites, etc. To protect the organization from loss of created material, enterprise policies on copyright ownership must be implemented and all employees must be reminded of these policies on a regular basis.

Unlike other forms of intellectual property protection, the basis for copyright occurs at the creation of an original work. Although copyrights are granted by government copyright offices, every original work has an inherent right to a copyright and is protected by that right even if the work is not published or registered.

All original works of authorship created by employees for a company are the property of the company and are protected by the copyright law. The copyright also applies to consultants doing work for an organization while under a purchase order or other contractual agreement. Unless there is an agreement to the contrary, any work created by a contractor under contract to an organization is owned by the organization, not the contractor.

The types of work that qualify for copyright protection include:

- all types of written works
- computer databases and software programs (including source code, object code, and micro code)
- output (including customized screens and printouts)
- photographs, charts, blueprints, technical drawings, and flowcharts
- sound recordings

A copyright does not protect:

- ideas, inventions, processes, and three-dimensional designs (these are covered by *Patent Law*)
- brands, products, or slogans (covered by *Trademark Law*)

For confidential information (see Exhibit 4), if the organization takes adequate steps (operates in good faith) to keep confidential information secret both internally and externally, then if there is a breach, the organization can seek relief through the courts. For trade secret and competitive advantage information, there may be criminal penalties for individuals as well as organizations, as well as civil penalties.

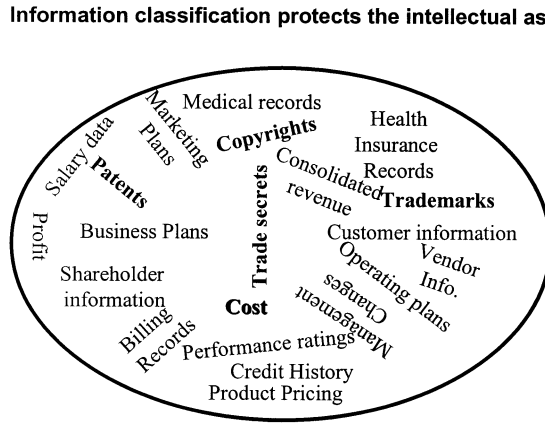

Exhibit 4. Typical organization confidential information.

9 CLASSIFICATION EXAMPLES

This section examines attributes and examples of different classification categories. Examples of organization information classification definitions are also presented.

9.1 Example No. 1

Information Classification

Policy: Security classifications should be used to indicate the need and priorities for security protection.

Objective: To ensure that information assets receive an appropriate level of protection.

Statement: Information has varying degrees of sensitivity and criticality. Some items may require an additional level of security protection or special handling. A security classification system should be used to define an appropriate set of security protection levels, and to communicate the need for special handling measures to users.

Critique of Example No. 1: This is an actual classification policy (very high level) for the executive branch of a national government. There is little here to help the average user. This is an example of a program or general policy statement; however, a Topic-Specific Policy Statement may have been more beneficial. Perhaps the next two examples will provide more information.

9.2 Example No. 2

Classification Requirements

Classified data is information developed by the organization with some effort and some expense or investment that provides the organization with a competitive advantage in its relevant industry and that the organization wishes to protect from disclosure.

While defining information protection is a difficult task, four elements serve as the basis for a classification scheme:

1. The information must be of some value to the organization and its competitors so that it provides some demonstrable competitive advantage.
2. The information must be the result of some minimal expense or investment by the organization.
3. The information is somewhat unique in that it is not generally known in the industry or to the public or may not be readily ascertained.
4. The information must be maintained as a relative secret, both within and outside the organization, with reasonable precautions against disclosure of the information. Access to such information could only result from disregarding established standards or from using illegal means.

Top Secret (Secret, Highly Confidential)

Attributes:

- It provides the organization with a very significant competitive edge.
- It is of such a nature that unauthorized disclosure would cause severe damage to the organization.
- It shows specific business strategies and major directions.
- It is essential to the technical or financial success of a product.

Examples:

- specific operating plans, marketing strategies
- specific descriptions of unique parts or materials, technology intent statements, new technologies and research
- specific business strategies and major directions

Confidential (Sensitive, Personal, Privileged)

Attributes:

- It provides the organization with a significant competitive edge.
- It is of such a nature that unauthorized disclosure would cause damage to the organization.
- It shows operational direction over extended period of time.

- It is extremely important to the technical or financial success of a product.

Examples:

- consolidated revenue, cost, profit, or other financial results
- operating plans, marketing strategies
- descriptions of unique parts or materials, technology intent statements, new technological studies and research
- market requirements, technologies, product plans, revenues

Restricted (Internal Use)

Attributes:

- all business-related information requiring baseline security protection, but failing to meet the specified criteria for higher classification
- information that is intended for use by employees when conducting company business

Examples:

- business information
- organization policies, standards, procedures
- internal organization announcements

Public (Unclassified)

Attributes:

- information that, due to its content and context, requires no special protection
- information that has been made available to the public distribution through authorized company channels

Examples:

- online public information, Web site information
- internal correspondences, memoranda and documentation which do not merit special controls
- public corporate announcements

Critique of Example No. 2: The policy seems to stress competitive advantage information in its opening paragraphs. It does not appear to address personal information about employees or customers. It does provide for these topics as categories under Confidential, but it never really mentions them by name. This appears to be a policy that is somewhat limited in scope. Additionally, it does not establish the scope of the information (is it computer generated only or exactly what information is being addressed?). The employee responsibilities are missing. What is management's responsibility with respect to information classification and what is

expected of the employees? Finally, what are the consequences of noncompliance?

9.3 Example No. 3

Information Classification

Introduction

Information, wherever it is handled or stored (e.g., in computers, file cabinets, desktops, fax machines, voice-mail) needs to be protected from unauthorized access, modification, disclosure, and destruction. All information is *not* created equal. Consequently, segmentation or classification of information into categories is necessary to help identify a framework for evaluating the information's relative value and the appropriate controls required to preserve its value to the company.

Three basic classifications of information have been established. Organizations may define additional subclassifications as necessary to complete their framework for evaluating and preserving information under their control.

When information does require protection, the protection must be consistent. Often, strict access controls are applied to data stored in the mainframe computers but not applied to office workstations. Whether in a mainframe, client/server, workstation, file cabinet, desk drawer, waste basket, or in the mail, information should be subject to appropriate and consistent protection.

The definitions and responsibilities described below represent the minimum level of detail necessary for all organizations across the company. Each organization can decide that additional detail is necessary to adequately implement information classification within their organization.

Corporate

Policy: All information must be classified by the owner into one of three classifications: Confidential, Internal Use, or Public. (From: Company Policy on Information Management)

Confidential

Definition: Information that, if disclosed, could:
- violate the privacy of individuals
- reduce the company's competitive advantage
- cause damage to the company

Examples: Some examples of **Confidential** information are:
- personnel records (including name, address, phone number, salary, performance rating, Social Security number,

date of birth, marital status, career path, number of dependents, etc.)
- customer information (including name, address, phone number, energy consumption, credit history, Social Security number, etc.)
- shareholder information (including name, address, phone number, number of shares held, Social Security number, etc.)
- vendor information (name, address, product pricing specific to the company, etc.)
- health insurance records (including medical, prescription, and psychological records)
- specific operating plans, marketing plans, or strategies
- consolidated revenue, cost, profit, or other financial results that are not public record
- descriptions of unique parts or materials, technology intent statements, or new technologies and research that are not public record
- specific business strategies and directions
- major changes in the company's management structure
- information that requires special skill or training to interpret and employ correctly, such as design or specification files

If any of these items can be found freely and openly in public records, the company's obligation to protect from disclosure is waived.

Internal Use

Definition: Classify information as **Internal Use** when the information is intended for use by employees when conducting company business.

Examples: Some examples of **Internal Use** information are:
- operational business information and reports
- noncompany information that is subject to a nondisclosure agreement with another company
- company phone book
- corporate policies, standards, and procedures
- internal company announcements

Public

Definition: Classify information as **Public** if the information has been made available for public distribution through authorized company channels. **Public** information is not sensitive in context or content, and requires no special protection.

Examples: The following are examples of **Public** information:

- Corporate Annual Report
- information specifically generated for public consumption, such as public service bulletins, marketing brochures, and advertisements

Critique of Example No. 3: Example Nos. 2 and 3 are very similar; Example 3 does address the role of the owner, but it fails to define what an owner is. The issue of noncompliance is not addressed and the scope of the policy is vague.

9.4 Example No. 4

Information Management

1. General
   A. Corporate information includes electronically generated, printed, filmed, typed, or stored.
   B. Information is a corporate asset and is the property of the Corporation.
2. Information Retention
   A. Each organization shall retain information necessary to the conduct of business.
   B. Each organizational unit shall establish and administer a records management schedule in compliance with applicable laws and regulations, and professional standards and practices, and be compatible with Corporate goals and expectations.
3. Information Protection
   A. Information must be protected according to its sensitivity, criticality, and value, regardless of the media on which it is stored, the manual or automated systems that process it, or the methods by which it is distributed.
   B. Employees are responsible for protecting corporate information from unauthorized access, modification, destruction, or disclosure, whether accidental or intentional. To facilitate the protection of corporate information, employee responsibilities have been established at three levels: **Owner, Custodian,** and **User.**
      1. **Owner:** Company management of the organizational unit where the information is created, or management of the organizational unit that is the primary user of the information. **Owners** are responsible to:
         a. identify the classification level of all corporate information within their organizational unit
         b. define appropriate safeguards to ensure the confidentiality, integrity, and availability of the information resource

c. monitor safeguards to ensure they are properly implemented
d. authorize access to those who have a business need for the information
e. remove access from those who no longer have a business need for the information

2. **Custodian:** Employees designated by the owner to be responsible for maintaining the safeguards established by the owner.
   a. **User:** Employees authorized by the owner to access information and use the safeguards established by the owner.

C. Each vice president shall appoint an Organization Information Protection Coordinator who will administer an information protection program that appropriately classifies and protects corporate information under the vice president's control and makes employees aware of the importance of information and methods for its protection.

4. Information Classification

To ensure the proper protection of corporate information, the owner shall use a formal review process to classify information into one of the following classifications:

A. **Public:** Information that has been made available for public distribution through authorized company channels. (Refer to Communication Policy for more information.)
B. **Confidential:** Information that, if disclosed, could violate the privacy of individuals, reduce the company's competitive advantage, or cause significant damage to the company.
C. **Internal Use:** Information that is intended for use by all employees when conducting company business. Most information used in the company would be classified Internal Use.

Critique of Example No. 4: The Intent of the policy is stated that "Information is a corporate asset and is the property of Corporation." The scope of the policy is "Corporate information includes electronically generated, printed, filmed, typed, or stored." The responsibilities are well established. The issue of compliance is the only policy element that appears to be lacking.

10 DECLASSIFICATION OR RECLASSIFICATION OF INFORMATION

Classified information normally declines in sensitivity with the passage of time. Downgrading should be as automatic as possible. If the information owner knows the date that the information should be reclassified, then it might be labeled as: *Confidential until (date).* There should be an established review process for all information classified as confidential, and reclassified when it no longer meets the criteria established for such information.

Part of an effective information classification program is to destroy documents when they are no longer required. Placing restrictions on copying classified documents will ensure that the documents and datasets are controlled and logged as to the number of copies created and to whom those copies were assigned. To assist in this process, it may be convenient to create an information handling matrix.

11 INFORMATION HANDLING PROCEDURES MATRIX

11.1 Printed Information

See Exhibit 5.

Exhibit 5. Printed information.

Confidential	Internal Use	Public
Labeling of documents		
Document should identify **owner** and be marked **CONFIDENTIAL** on cover or title page	No special requirements	Document may be marked **PUBLIC** on cover or title page
Duplication of documents		
Information **owner** to determine permissions	Duplication for business purposes only	No special requirements
Mailing of documents		
No classification marking on external envelope; **CONFIDENTIAL** marking on cover sheet; confirmation of receipt at discretion of information **owner**	Mailing requirements determined by information **owner**	No special requirements
Disposal of documents		
Owner observed physical destruction beyond ability to recover	Controlled physical destruction	No special requirements
Storage of documents		
Locked up when not in use	Master copy secured against destruction	Master copy secured against destruction
Read access to documents		
Owner establishes **user** access rules; generally highly restricted	**Owner** establishes **user** access rules; generally widely available	No special requirements; generally available within and outside company
Review of document classification level		
Information **owner** to establish specific review date (not to exceed 1 year)	Information **owner** to review at least annually	No special requirements

11.2 Electronically Stored (Computer-Based) Information

See Exhibit 6.

Exhibit 6. Electronically stored (computer-based) information.

Confidential	Internal Use	Public
Storage on fixed media (access controlled)		
No encryption required	No encryption required	No encryption required
Storage on fixed media (not access controlled)		
Encrypted	No encryption required	No encryption required
Storage on removable media		
Encrypted	No encryption required	No encryption required
Read access to information (includes duplication)		
Information **owner** to authorize individual **users**	Information **owner** to define permissions on **user,** group, or function basis	No special requirements
Update access to information		
Information owner to authorize individual **users**	Information **owner** to define permissions on **user,** group, or function basis	Information **owners** to define permissions
Delete access to information		
Information **owner** to authorize individual **users; user** confirmation required	Information **owner** to define permissions on **user,** group, or function basis; **user** confirmation required	Information **owner** to define permissions
Print hard copy report of information		
Output to be routed to a predefined, monitored printer	Information **owner** to define permissions	No special requirements
Internal labeling of information at the application or screen/display level		
Notification of **CONFIDENTIAL** to appear at top of display	No special requirements	Notification of **PUBLIC** may optionally appear at top of display
External labeling of exchangeable media		
Media must identify **owner** and be marked **CONFIDENTIAL**	Marking at discretion of **owner**	No special requirements
Disposal of electronic media (diskettes, tapes, hard disks, etc.)		
Owner observed physical destruction beyond ability to recover	Physical destruction	No special requirements
Disposal of information		
Delete by fully writing over information	Delete files through normal platform delete command, option, or facility	No special requirements

Exhibit 6. Electronically stored (computer-based) information. *(Continued)*

Confidential	Internal Use	Public
Review of classified information for reclassification		
Information **owner** to establish specific review date (not to exceed 1 year)	Information **owner** to review annually	Information **owner** to review annually

11.3 Electronically Transmitted (Computer-Based) Information

See Exhibit 7.

Exhibit 7. Electronically transmitted (computer-based) information.

Confidential	Internal Use	Public
By fax		
Attended at receiving fax	Information owner to define requirements	No special requirements
By WAN		
Confirmation of receipt required; encryption optional	No special requirements; encryption optional	No special requirements
By LAN		
Confirmation of receipt required; encryption optional	No special requirements; encryption optional	No special requirements
By inter-office mail		
No external labeling on envelope; normal labeling on document	No special requirements	No special requirements
By voice-mail		
Confirmation of receipt required (sender); remove message after receipt (recipient)	No special requirements	No special requirements
By electronic messaging (e-mail)		
Confirmation of receipt required; encryption optional	No special requirements	No special requirements
By wireless or cellular phone		
Do not transmit	No special requirements	No special requirements

12 INFORMATION CLASSIFICATION METHODOLOGY

The final element in an effective information classification process is to provide management and employees with a method with which to evaluate

information and provide them with an indication of where the information should be classified. To accomplish this, it may be necessary to create an information classification worksheet (see Exhibit 8). These worksheets can be used by the business units to determine what classification of information they have within their organization.

To complete this worksheet, the employee would fill in the information requested at the top of the sheet:

- Organization — the department designated as the information owner
- Group — the reporting group of the individual performing the information classification process
- Review performed by/Phone — the name and phone number of the individual performing the review
- Date — the date of the review
- Information Name/Description — an identifier and description of the information being reviewed

In the section for Information Name/Description, it will be necessary to enter the information type. For example:

Employee Records
- employee performance review records
- timecards
- employee discipline documents
- pay records
- medical records

Group Administrative Records
- monthly status reports
- yearly status reports
- yearly business objectives

Business Process Records
- purchasing contracts
- quarterly financial reports
- project management tasks, schedules
- reference manuals
- contract negotiations

Operations Information
- business partner information
- asset allocation
- trading activities
- production formulas
- production cost information
- customer lists

Distribution Records
- distribution models

Organization: _____ Group: _____

Review Performed By / Phone: _____ Date: _____

	INFORMATION NAME / DESCRIPTION	STORAGE MEDIUM	CLASSIFICATIONS (select one) CONFIDENTIAL If disclosed, could violate the privacy of individuals, reduce the company's competitive advantage, or could cause damage to the company.	RESTRICTED Intended for use by a subset of employees when conducting company business. (Usually regulatory requirement.)	INTERNAL USE Intended for use by all employees when conducting company business.	PUBLIC Made available for public distribution through authorized company channels.
EMPLOYEE RECORDS						
1						
2						
3						
4						
5						
6						
GROUP ADMINISTRATIVE RECORDS						
1						
2						
3						
4						
5						
6						
7						
BUSINESS PROCESS RECORDS						
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						

Exhibit 8. Sample information classification worksheet.

- inventory records

- parts supplies

Using the definitions, the person(s) performing the review would place a check in the appropriate column; only one check for each item being reviewed. This process would allow the user department to identify all of the various types of information found in their department and then be able to determine under which classification they probably fall.

13 AUTHORIZATION FOR ACCESS

To establish a clear line of authority, some key concepts will have to be established. As discussed above, there are typically three categories of employee responsibilities. Depending on the specific information being accessed, an individual may fall into more than one category. For example, an employee with a desktop workstation becomes the owner, custodian, and user. To better help understand the concepts, the responsibilities of each category are listed below.

13.1 Owners

Minimally, the information owner is responsible for:

- judging the value of the information resource and assigning the proper classification level
- periodically reviewing the classification level to determine if the status should be changed
- assessing and defining appropriate controls to assure that information created is properly safeguarded from unauthorized access, modification, disclosure, and destruction
- communicating access and safeguard requirements to the information custodian and users
- providing access to those individuals with a demonstrated business need for access
- assessing the risk of loss of the information and assuring that adequate safeguards are in place to mitigate the risk to information integrity, confidentiality, and availability
- monitoring safeguard requirements to ensure that information is being adequately protected
- assuring a business continuity plan has been implemented and tested to protect information availability

13.2 Custodians

At a minimum, the custodian is responsible for:

- providing proper safeguards for processing equipment, information storage, backup, and recovery

- providing a secure processing environment that can adequately protect the integrity, confidentiality, and availability of information.
- administering access requests to information properly authorized by the owner.

13.3 User

The user must:

- use the information only for the purpose intended
- maintain the integrity, confidentiality, and availability of information accessed

Being granted access to information does not imply or confer authority to grant other users access to that information. This is true whether the information is electronically held, printed, hardcopy, manually prepared, copied, or transmitted.

14 SUMMARY

Information classification drives the protection control requirements and this allows information to be protected to a level commensurate with its value to the organization. The costs of overprotection are eliminated and exceptions are minimized. With a policy and methodology, specifications are clear and accountability is established.

There are costs associated with implementing a classification system. The most identifiable costs include labeling classified information, implementing and monitoring controls and safeguards, and proper handling of confidential information.

Information, wherever it is handled or stored, needs to be protected from unauthorized access, modification, disclosure, and destruction. All information is not created equal. Consequently, segmentation or classification of information into categories is necessary to help identify a framework for evaluating the information's relative value. By establishing this relative value, it will be possible to establish cost-effective controls that will preserve the information asset for the organization.

Chapter 6
Developing an Electronic Communications Policy

1 INTRODUCTION

The use of electronic communications (e-mail) in business is spreading rapidly, and in many organizations the e-mail system is now the place for office gossip and other conversations unrelated to work. Although some of the information exchanged on e-mail is personal or frivolous, the system also frequently carries vital organization information. The "information mix" raises many moral and business issues that must be addressed. This chapter provides the reader with the tools to develop effective e-mail policies and controls for an enterprise, and examines the legal and privacy issues that must be considered.

2 DEFINITION

Electronic mail, often referred to as e-mail, is a paperless form of communication. Regardless of whether the system used is based on local area networks (LANs), mainframe computers, or some third-party commercial value-added network, e-mail allows messages to be sent from one computer to another, much like postal mail is sent from one location to another. However, the privacy protection afforded postal mail far outstrips that currently afforded e-mail.

In 1990, the Electronic Messaging Association (EMA) estimated that 20 million people were using e-mail. In June 1997, the German magazine *Stern* projected that e-mail usage would continue to grow, and that by the year 2000, 200 million users would be using e-mail systems worldwide. At the MIS Open Systems Security '95 Conference in March 1995, Barbara Fraser of the Internet Computer Emergency Team at Carnegie Mellon University,

indicated that more e-mail messages had been sent in the past 15 minutes than were sent in all of 1993.

3 CURRENT CONTROVERSY

A poll in 1994 by the Louis Harris Organization found that 84 percent of Americans said they were concerned about privacy, and 51 percent were very concerned — an all-time high. In a 1991 Lou Harris Poll, nearly 80 percent of Americans said they regard privacy as a fundamental right. More than 70 percent believed they had lost control over their personal information.

Most employees regard the expectation of privacy as a fundamental right. Legislation over workplace privacy issues is expected to increase as greater numbers of employers, both public and private, engage in testing, monitoring, and surveillance of employees.

The courts have ruled that a "reasonable expectation of privacy" requires two key elements:

1. that the individual exhibit an actual (subjective) expectation of privacy
2. that this expectation be one that society is prepared to regard as reasonable

4 WHAT TO DO

Before attempting to address e-mail privacy issues, it may be beneficial to review existing organization policies with respect to such privacy for office space, employee desks, file cabinets, briefcases, internal and external mail, and phone conversations. Even if there is no written policy, all organizations are strongly urged to implement such a policy. Then look to the current culture within each department or the enterprise as a whole. As an example, are spare sets of keys kept in the office administrator's desk? Are these keys used to retrieve documents from desks, file cabinets, and offices? If so, then the organization may already have an unwritten policy regarding the expectation of employee workplace privacy. It is important to identify the level of privacy expectation in employees before starting to establish a new level of control in the electronic environment.

5 EMPLOYEE PRIVACY ISSUES

Traditionally, employees have received little privacy protection on the job. It is argued that employers' interests should be favored because work is done on the employers' premises. Employers own the communications equipment used at work and it is the company's business that is being conducted on this equipment.

Employers have a strong interest in monitoring employee activity for the purposes of ensuring the quality and quantity of the work product, and

for protecting against theft and fraud. In March 1989, Alana Shoars was fired as the e-mail administrator for Epson America, Inc. located in Torrance, CA. Epson claimed that Shoars was terminated for "gross misconduct and insubordination;" however, she believed that the firing was the consequence of her questioning why a supervisor was printing out employee e-mail messages. She filed a wrongful discharge and invasion of privacy action against Epson. This lawsuit left unanswered many legal and ethical issues about e-mail. One issue made clear by this suit is that many, if not most, employees have a strong expectation of privacy in the use of e-mail.

As e-mail systems are currently structured, it is not possible to guarantee complete privacy with regard to the messages sent and received. Each organization will have to balance the proprietary rights of the organization against the privacy rights of the employees. In "Bosses with X-Ray Eyes," *MacWorld,* July 1993, a survey of managers of businesses in the United States indicated that the searching of e-mail files is one of the most frequently used forms of monitoring. Although many employers feel that monitoring e-mail will help improve employee productivity, it may in fact have just the opposite effect. In a 1993 study presented by Michael Crawford in *Canadian Business,* it was found that electronic monitoring can increase employee "tension, anxiety, depression, anger, and fatigue." In an era when a majority of employees feel unempowered, disenfranchised, and disgruntled, the monitoring of employee e-mail can be an additional source of stress in the workplace.

6 BALANCING THE ISSUES

The issues that need to be considered in protecting e-mail messages include:

- the privacy rights of the employees
- the need of the employer to protect system security and to manage company resources
- the rights of third parties to get access to company files

Take a few minutes to examine each of these issues. Each is important to understand when attempting to develop a policy or control mechanism that will be for the prudent balancing of controls and communications.

6.1 The Privacy Rights of Employees

There is a need for employers to balance the needs of the company with the needs of the employees to be able to communicate with one another without the fear that someone is watching their every word. One of the strengths of e-mail is that it allows all employees to communicate throughout the organization. Where an employee may not have an opportunity to

meet and speak with certain executives, the e-mail system provides a way of breaking down the communication barriers.

A report from the State of California indicated that more than 60 percent of all e-mail messages are of a nonbusiness nature. (Office of Information Technology, Department of Finance, State of California, "Security and Risk Management Guidelines Update," *Calculated Risk: Risk Management, Public Access and Privacy,* Apr-May-Jun 1992, p. 4). As controls are developed and policies finalized, it is important to know and understand that employees at all levels of the enterprise will be using e-mail for other than business-related correspondence — both internal and external to the organization.

If your organization is determined to restrict the nonbusiness use of e-mail communications, then be prepared to develop a policy that will be widely ignored by all employees at all levels of the organization. The primary concern is that such a policy will restrict the use of the system and then will inhibit employees from using the system to develop and express actual business documents.

6.2 The Need of the Employer to Protect System Security and Manage Company Resources

With the massive growth of e-mail usage and the connection to the worldwide Internet, information that could be controlled within an organization may now be made available to anyone with access to the Internet. There are a number of legitimate reasons to monitor e-mail messages, and the need to do this must be addressed by every organization. The first step in this process should be a formal risk analysis of e-mail system usage. Using a facilitated approach, an organization can review the impacts of e-mail usage based on information integrity, confidentiality, and system availability.

7 DO A RISK ANALYSIS PRIOR TO WRITING

Prior to conducting a risk analysis, it will be necessary to establish the scope of the review. A key question that must be addressed is: what is the purpose for which the e-mail system can be used and who will be using the system? It is possible that the corporate e-mail system may be used by employees, contractors, consultants, customers, clients, suppliers, regulatory agencies, and other third parties.

Looking at the various aspects of what can be said via e-mail messages, there are specific areas that will cause a great deal of concern. The e-mail system is a microcosm of current society. All other concerns and taboos addressed through other venues will become part of the corporate concern in employee use of the e-mail system. Among those topics that must be addressed and controlled by any organization using an e-mail system are the following.

7.1 Sexual Harassment

Most organizations already have policies in place that address this issue. However, the very nature of the e-mail system may lend itself to problems in this area. Because there is no personal contact, employees may say things electronically that they would never say face-to-face.

7.2 Race, Age, or Other Forms of Discrimination

As stated above, most organizations already have policies in place and have regular training sessions on this topic. However, in a recent *Detroit Free Press* article, two companies that were in litigation because of alleged discrimination lost their cases because of e-mail messages uncovered in the discovery process. In both instances, *private* communications between supervisors contained language that was used by the plaintiff's attorney to support his client's claims. In each case, the messages could have been just an off-hand remark made between two colleagues. These off-hand remarks cost each company financially and public image-wise.

7.3 Libel and Slander

With the ability to send e-mail messages anywhere in the world, it is important to make certain that the contents reflect the true position of the corporation. If an organization is connected to an external e-mail source such as the Internet, then the ability of employees using company equipment to put statements out in the public forum may cause legal problems for the organization.

7.4 Insider Trading

Some employees cannot pass up the temptation to access and send financial information to friends and relatives.

7.5 Trade Secrets/Competitive Advantage Information

The business credo of the 1990s has been "Know what your customer wants and know what your competition is doing." With the ability to send attachments along with e-mail messages, organizations are finding out that there is little or no control over information that has cost them time, money, and resources to create.

7.6 The Rights of Third Parties to Get Access to Company Files

With all of this electronic access, many government and regulatory agencies require electronic access. This access allows for the timely communication of conditions and status with those organizations requiring regular reports. Additionally, law enforcement and shareholders may want access to the organization's e-mail system.

8 OTHER E-MAIL ISSUES

Each of the problems discussed previously can be impacted by some of the very basic characteristics of any e-mail system. There is an inherent illusion of privacy between the sender and the receiver. Therefore, many employees say things to each other that they would never say in a public meeting or forum. Because all messages eventually are stored in some form of electronic media, anyone with some technical skill and access to the proper equipment can access messages.

Once a message is sent, all control of distribution is lost. If the financial department is working on financial statements and sends a copy along for review, there is no ability to ensure that the information will remain only with the intended recipient. Additionally, each new recipient can forward the information to whomever they desire. Another problem related to this message distribution is the use of distribution lists or global sending commands. Too often, messages meant to be shared by only a select few are accidentally sent to many more users.

As Oliver North can attest, e-mail messages seem to have a life of their own. Even after messages have been "deleted," they can reappear in recipient mailboxes, backup tapes, or mirrored disks. A message is almost never gone. Even if the space on the media has been written over, there is a chance that experts can retrieve at least a portion of the original message.

9 E-MAIL POLICY DEVELOPMENT

The key to successful handling of the issues is to consider them carefully and to reach a balanced judgment based on a formal risk analysis process that addresses the business needs of the company and the privacy concerns of the employees. Any e-mail policy must be compatible with those already established regarding workplace privacy. Of particular interest are those policies regarding computer files, phone usage, employee work space, and employee personal property.

An appropriate company policy will differ from one organization to another. There will be many of the same elements in all policies, but the culture and business needs of each enterprise will dictate the overall contents. Included in these differences will be an examination of the proprietary needs of the company, the reasonable expectation of privacy by the employees, and the balancing of these interests.

Today, many organizations have decided that e-mail and other forms of electronic communication should be incorporated into the existing policies on all forms of corporate communications. For most organizations, e-mail policies are not viewed as an information systems problem or responsibility, but a corporate responsibility. Over the past two years, there has been a movement to incorporate these controls into the general corporate

policy manual. Some organizations have made compliance to electronic communication policies an issue contained in the "Employee Standards of Conduct."

When developing an e-mail policy, a key question that must be answered prior to policy development is: "What is it that the organization is trying to control?" Is the policy trying to control the employees? Or will it stress access to the system? Or will the policy focus on the information that may be transmitted via e-mail? Typically, the answer is a combination of these three elements with a strong emphasis on the information.

9.1 Formulate a Policy-Development Team

To formulate an e-mail policy, most organizations will find it beneficial to assemble a working group of company personnel who will represent different interests and responsibilities. An example of a typical team might include representatives from Information Systems, Information Protection, Auditing, Human Resources, Corporate Investigation, Policies and Procedures, Labor Relations (for union-represented shops), and some user groups. Auxiliary team membership would include someone from the Legal Staff and Corporate Communications.

9.2 Setting the Scope

There will be three key stakeholders in the e-mail policy development. Each of these will have a view of how the policy should be developed and enforced. Typically, those three views are:

1. *The organization*. How will the policy affect the organization's need to manage the system resources? As the system is opened up for electronic messaging, there will be an overhead associated with usage. A key component to any workplace is the protection of the employees. An e-mail policy will want to ensure that the security of employees is not jeopardized. There will be a need to ensure that unlawful actions by employees are prevented as much as possible, and that appropriate actions are taken with employees that do break the law.

   Even with the stress of often-times negative control features, the organization will want to foster an environment in which the employees are productive and morale is not compromised. This is the balancing act under discussion: the need to make certain that the e-mail system is used by the employees and that they feel secure that when they use the system as it was intended, there will be no repercussions.
2. *The employee*. How will the policy affect the need for a well-functioning, congenial, and secure workplace. How much monitoring will be necessary and who will be doing the monitoring? Fear of the unknown will cause paralysis within the employee community. Keep the control to a minimum and explain through employee awareness

sessions what the controls are about and what will be the consequences of violation of corporate policy.

3. *Third parties.* How will the policy affect those who have a need or duty to disclose e-mail messages to other parties? The normal course of business will not require that employee personal messages be disclosed to third parties. However, there could be some legal reason when employee personal messages might be requested by outsiders. Law enforcement during an investigation of a crime or some civil litigation or regulatory proceedings may cause all forms of e-mail to be disclosed.

10 SEVEN PRINCIPLES FOR E-MAIL SECURITY

The Information and Privacy Commission, Ontario (Canada), created the Privacy Protection Principles for Electronic Mail Systems. A brief examination of these principles follows.

1. *The privacy of e-mail users should be respected and protected.* Employees will only use the e-mail system if they feel that what they transmit will be kept confidential. A West Coast company informed employees that they were going to begin monitoring e-mail activity. Shortly after the announcement, e-mail usage dropped 35 percent.
2. *Every enterprise should create an explicit policy that addresses the key elements of e-mail policies.* The policy should include input from other departments and should address three key issues:
   a. the purposes for which e-mail can be used
   b. what third-party access to e-mail may be allowed
   c. consequences for a breach of the e-mail policy
3. *Each organization should make its e-mail policy known to users and inform them of their rights and obligations regarding the confidentiality of messages on the system.* Simply including information relating to e-mail use in the corporate policy document may not be adequate. Employees (and other users) must be directly informed of the policy, and this must be done on at least an annual basis.
4. *Users should receive proper training regarding e-mail security and privacy issues surrounding its use.* Most employees assume that their communications are private. This is not necessarily true. In many circumstances, the privacy of e-mail can be breached.
   a. employers, supervisors, or system staff can access personal communications
   b. messages can be stored in an automatic backup
   c. deleting the message from one's personal file will not destroy all of the copies sent or stored elsewhere
   d. e-mail messages can be readily forwarded to others without the author's permission or knowledge

e. e-mail can be networked to other organizations, making information more vulnerable
f. third parties can access the e-mail recipient's files
g. hackers can break into e-mail systems
h. e-mail can be remotely monitored without any indication that the monitoring is being conducted
i. use of e-mail at remote sites can create records over which the organization has little control
j. not all e-mail systems automatically encrypt files and messages

5. *E-mail systems should not be used for the purposes of collecting, using, or disclosing personal information, without adequate safeguards to protect privacy.*
6. *Providers of e-mail systems should explore technical means to protect privacy.* Sample measures include:
   a. access control through a secure single sign-on process or some other remote access authentication process
   b. encryption measures to protect the contents of messages and files (where appropriate)
   c. automatic log-off process for users who have not interacted with the system in a specified period of time
   d. the subject of a message can be concealed
7. *Each organization should develop appropriate security procedures to protect e-mail messages.* Security breaches can occur when it is possible to access computers easily, in particular when some messages have been archived on personal files that have no security safeguards. Passwords should be changed as regularly as the requirements for mainframe password change. The number of personnel with system administrator capabilities should be minimized and their activities monitored by third parties. Employees should be aware of any backup files and the length of time for which such backups are retained.

11 POLICY DEVELOPMENT POINTS

The typical policy statement is brief. That is, the information is contained in only one or two pages of text. The key to an effective policy is to have the words express exactly what the organization wants the employees to understand. This is perhaps the most difficult part of writing. Remember, one does not have the luxury of sitting down with each user and explaining what each passage means. To create an effective policy, one needs to have a number of people review and critique the document for its "read-ability."

Keep the text simple. Remember, this is a policy document for persons with little time to examine and grasp what is being asked of them. Do not

attempt to write a doctoral dissertation; keep the message plain and to the point. Explain what is required and what is expected of each employee. If there are consequences for actions, this is the place where those consequences should be discussed.

12 E-MAIL POLICY EXAMPLES

Some specific examples of policies addressing the various elements are presented below. Keep in mind the three elements needed for an effective e-mail policy:

- the purposes for which e-mail can be used
- what third-party access to e-mail may be allowed
- consequences for a breach of the e-mail policy

12.1 Policy No. 1: Sample Electronic Data Systems Policy

The Company maintains a voice-mail system and an electronic-mail (e-mail) system to assist in the conduct of business within the Company. These systems, including the equipment and the data stored in the system, are and remain at all times the property of the Company. As such, all messages created, sent, received, or stored in the system are and remain the property of the Company.

Messages should be limited to the conduct of business at the Company. Voice-mail and electronic-mail may not be used for the conduct of personal business.

The Company reserves the right to retrieve and review any message composed, sent, or received. Please note that even when a message is deleted or erased, it is still possible to recreate the message; therefore, ultimate privacy of messages cannot be ensured to anyone. While voice-mail and electronic-mail may accommodate the use of passwords for security, confidentiality cannot be guaranteed. Messages may be reviewed by someone other than the intended recipient. Moreover, all passwords must be made known to the Company. The reason for this is simple: your system may need to be accessed by the Company when you are absent.

Messages may not contain content that may reasonably be considered offensive or disruptive to any employee. Offensive content would include, but would not be limited to, sexual comments, or images, racial slurs, gender-specific comments, or any comments that would offend someone on the basis of his or her age, sexual orientation, religious or political beliefs, national origin, or disability.

Employees learning of any misuse of the voice-mail or electronic-mail system or violations of this policy shall notify the Director of Human Resources immediately.

12.2 Policy No. 2: Subject: Electronic-Mail (e-mail)

1. Policy/Purpose. Electronic-mail is a Secretary of State resource and is provided as a business communications tool. All Agency electronic mail is a public record (ORS 192) and is subject to inspection and disclosure and scheduled retention and disposition. Employees should have no expectation of privacy in their use of electronic-mail.
2. Responsibilities.
   a. Secretary of State: Implement, maintain, and communicate to all employees an agency policy on electronic-mail (e-mail) use.
   b. Division Directors: Develop division procedures as appropriate to implement the agency e-mail policy. These procedures should: specify whether e-mail documents should be filed electronically or as paper; establish appropriate use of e-mail within the Secretary's policy; establish procedures, where applicable, for providing public access to electronic files and establish fees charged for requests; and monitor compliance with agency policy and division procedures.
   c. Information Systems Section: Support and maintain the e-mail system; provide routine backup and off-site storage of e-mail files for disaster recovery purposes
   d. All employees: Comply with agency policy and divisional procedures
3. Privacy/Public Access.
   a. The Secretary of State reserves the right to monitor e-mail messages and to access employee e-mail.
   b. No employee shall read e-mail received by another employee when there is no business purpose for doing so.
   c. No employee shall send e-mail under another employee's name without authorization.
   d. No employee shall change any portion of a previously sent e-mail message without authorization.
4. Appropriate Use.
   a. E-mail shall be used for business matters directly related to the business activities of the Secretary of State and as a means to further the agency mission by providing services that are efficient, complete, accurate, and timely.
   b. E-mail shall not be used for personal gain, outside business activities, political activity, fundraising, or charitable activity not sponsored by the state of Oregon or the Secretary of State.
   c. E-mail shall not be used to promote discrimination on the basis of race, color, national origin, age, marital status, sex, political affiliation, religion, disability, or sexual preference; promote sexual harassment; or to promote personal, political, or religious business or beliefs.

5. Filing and Retention.
   a. The Secretary of State's Policy is to provide for efficient retention of e-mail communications. E-mail communications are considered public records and retention and disposition of public records is authorized by retention schedules issued by the Archives Division.
   b. Divisions may retain e-mail in hardcopy, electronically, or by a combination of these two means. Divisions are responsible for developing filing systems which include e-mail and are responsible for instructing employees on appropriate use of these systems.
   c. When appropriate, e-mail messages may be filed with program records and assume the same retention as the records they are filed with. When e-mail records do not relate obviously or directly to a program, they may be filed as correspondence. When they are filed as correspondence, the retention contained in OAR 166, Division 300 may be used.
   d. Some e-mail systems enable users to enclose or attach records to messages. These enclosed or attached records need to be filed according to their function and content, and they will assume the retention of the records they are filed with.

   Employees found to have violated any provision of this policy shall be subject to appropriate disciplinary action.

12.3 Policy No. 3: Company E-Mail Policy

Company e-mail service is provided to support the educational mission of the Company institutions. Access to and use of e-mail is a privilege, not a right, and should be treated as such. All students and staff are responsible for seeing that these e-mail services are used in an effective, efficient, ethical, and lawful manner.

Computing services, including e-mail, may not be used for illegal activities or unauthorized purposes, including, but not limited to:

- harassment
- destruction of or damage to equipment, software, or data
- unauthorized copying of copyrighted materials
- the disruption or unauthorized monitoring of electronic communications for private business or personal gain or profit

As an e-mail user, you are responsible for using the system resources wisely.

General Standards and Guidelines. E-mail users are asked to take care in subscribing to list-serves, transmitting large messages and attachments, and sending multiple copies.

Privacy of e-mail messages cannot be guaranteed. Maintenance of the e-mail system may require access to user's files.

Sanctions for Violations. If you use the system in ways that are judged excessive, wasteful, or unauthorized, you may be subject to loss of access and appropriate disciplinary procedures.

All e-mail users will have to acknowledge acceptance of these guidelines before their account is activated.

By clicking "I agree" below, I agree to release to Company my name, social security number, and date of birth to create and maintain my account. I also agree to abide by the above listed e-mail policies.

Please check "I disagree" if you disagree with any of the above.

[I agree | I disagree]

Some organizations have developed a standard of conduct for electronic communications, the following is a example of such a statement.

12.4 Standards of Conduct for Electronic Communications

The Company's policies regarding Employee Standards of Conduct, Conflict of Interest, Equal Employment Opportunity and Diversity in the Workplace, and Communication and Information Protection also apply to electronic messages (e-mail), telephone messages (voice-mail), and other internal and external electronic communications, including, but not limited to, computer bulletin boards, Newsgroups, and the Internet.

Transmitted messages are to be created, handled, distributed, and stored with the same care as any other business document. This includes complying with information-access prohibitions, accessing information only for legitimate business purposes, and protecting information from access by unauthorized persons.

Users should be aware that these systems, and the information stored within them, are the property of the Company and are to be used only for Company-approved activities. The Company maintains the right to monitor the operation of these systems.

Since confidentiality is not assured, these systems are to be used only for transmitting information considered "Public" or for "Internal Use." (The definitions for "Public," "Internal Use," and "Confidential" may be found in the Company Policy on Information Protection.) "Confidential" information should not be communicated using these electronic systems. The Company's prohibition of derogatory and offensive comments also applies to messages communicated through these systems. Special care should be given to ensure that the style and tone of messages are appropriate.

Every effort should be made to send messages only to those who "need to know." The Company Policy on Communication details the approvals re-

quired before distributing information externally or internally through the use of company mailing lists.

Employees are responsible for using these systems appropriately. Inappropriate use could result in disciplinary action.

13 SUMMARY

Protecting e-mail privacy through the implementation of an organizationwide policy will enhance the work environment and promote effective communication within the organization. While these general principles lay out a framework for e-mail privacy protection, the difficult decisions involving the balance between employee privacy and employer proprietary interests will need to be made based on the needs of the organization.

Chapter 7
Typical Organization Policies

1 INTRODUCTION

Every organization needs to implement a basic sets of policies. These will normally be found as a document prepared by the organization and can be used by the information security professional to reinforce the messages needed to ensure information resources are properly protected. Included for the reader are samples of these important enterprisewide policies and, where applicable, the changes needed for information security.

2 SHARED BELIEFS

The shareholders and customers of Company Corporation have entrusted the employees of Company Corporation with important responsibilities: to increase shareholder value by providing premier, world-class security solutions.

We have committed ourselves to fulfilling those responsibilities, recognizing that the commitment requires the personal dedication and leadership of each of us and the collective effort of all of us.

We are committed to teamwork and accountability.

We believe that unless we conduct ourselves as a team — and build team effort throughout the company — we cannot succeed. Further, we believe that a team succeeds only when all members understand the team goals, their individual roles, and how each person's performance and commitment contribute to achieving the goals. Our commitment to this concept is reflected in our willingness to accept accountability for results and to stake our personal success on those results.

We are committed to communication.

We practice open, honest, two-way communication and provide regular feedback. We believe that written communication cannot replace dialogue between people, that effective communication is a prerequisite to effect action; and that trust, respect, and understanding are necessary for effective

communication. We set examples through our behavior because our actions do in fact speak louder than our words.

We are committed to continuous improvement and benchmarking.

Continuous improvement in our skills, methods, and results is vital to our success in the highly competitive information security sector. We measure our success and our improvement by comparing our performance with that of our competitors and other companies that are world-class performers. We recognize that just as we strive for improved performance, so do our competitors. Benchmarking and continuous improvement, therefore, are ongoing processes that will ensure that our sights are constantly on target to become superior performers.

Our dedication to living these commitments will produce an environment in which employees are involved — involved in the goals of the company and their individual work groups — and sharing ideas and suggestions as valued contributors. In this way, we will provide value to customers, shareholders, and employees. Our goal is that every employee becomes committed to our shared beliefs.

Use the key phrases or terms identified in this kind of document in the text of the information security policies. Such important concepts as "teamwork," "accountability," communication," "continuous improvement," and "benchmarking" will add creditability to the information security policies.

3 STANDARDS OF CONDUCT

Standards of Conduct

A. Company employees are expected to adhere to the following standards of conduct:
   1. Employees shall act in an ethical manner, and shall avoid actions that have the *appearance* of being unethical.
   2. Employees shall abide by applicable laws, regulations, and professional standards.
   3. Employees shall avoid conflict of interest situations. (See Conflict of Interest policy for more information.)
   4. Employees shall meet individual performance expectations.
   5. Employees shall abide by company and organizational policies and practices.
   6. Employees shall accurately and honestly record and report corporate information. Employees shall also maintain the confidentiality of corporate information. (See Information Protection policy.)
   7. Employees shall treat co-workers and others with dignity and respect.

Application of Standards of Conduct and Reporting Violations

1. Employees are expected to use intelligence, common sense, and good judgment in applying these standards of conduct.
2. When in doubt, employees shall direct questions relating to the standards of conduct to their supervisors.
3. Employees who observe conduct that does not appear consistent with these standards of conduct should discuss the matter with their supervisor. The supervisor shall report fraudulent activity to the General Auditor. However, employees who feel uncomfortable reporting to their supervisors, or who are not satisfied with the action taken, rather than letting the matter drop, should seek the counsel of the General Auditor.
4. Any employee who feels that they have been the subject of a violation of the standards of conduct should immediately report the matter to their supervisor or to the Vice President of Human Resources.
5. All complaints shall be investigated in as discreet a fashion as possible.
6. Once the investigation is complete, action will be taken where appropriate.
7. Supervision shall provide appropriate feedback to those who report misconduct.
8. Company will not retaliate against employees who report suspected misconduct.
9. Company management has the responsibility to manage corporate information, personnel, and physical properties relevant to their business operations, as well as the right to monitor the actual utilization of all corporate assets.
10. If an employee becomes involved in a legal matter arising out of employment with Company, the Company shall provide or select legal counsel and indemnify that employee, if, in the opinion of the General Counsel, the employee was acting in good faith, within the scope of the job responsibilities, and legal counsel or indemnification is not otherwise available to the employee.

Unacceptable Conduct

A. Employees who violate these standards of conduct are subject to disciplinary action up to and including discharge. In some cases, employees may also be subject to criminal charges.
B. Supervisors shall follow appropriate disciplinary procedures, up to and including discharge, for employees whose work performance or behavior does not meet the standards of conduct. Some examples of unacceptable conduct are shown below. This list is not all-inclusive.
    1. Work performance
        a. Failure to meet job requirements

b. Violation of safety rules
c. Unacceptable work performance

2. Attendance and tardiness
   a. Absence without notice or permission less than X consecutive work days
   b. Failure to call as required
   c. Tardiness or excessive absence
3. Conduct — General
   a. Alcohol or substance abuse
   b. Conflict of interest
   c. Dishonesty
   d. Failure to maintain acceptable appearance, any hygiene standards
   e. Gambling or operating a lottery
   f. Possession of unauthorized weapons or cameras on company property
   g. Sleeping on the job
   h. Unauthorized use or possession of company property
   i. Insubordination
   j. Violation of a copyright or software licensing agreement, including the introduction of noncompany approved software or code into any company system
4. Conduct — Harassment
   a. Harassment, including sexual harassment; verbal abuse; threatening others. Harassment can take many forms in words or actions that are either implied or clear and direct. It is not limited by position, or sex, or race.
   b. Sexual harassment refers to behavior of a sexual nature that is unwelcome and offensive and is a form of misconduct that undermines the integrity of the employment relationship. Sexual harassment means unwelcome sexual advances, requests for sexual favors, and other verbal or physical conduct or communication of a sexual nature when:
      i. Submission to such conduct or communication is made a term or condition, either explicitly or implicitly to obtain employment
      ii. Submission to, or rejection of, such conduct or communication by an individual is used as a factor in decisions affecting such individual's employment
      iii. Such conduct or communication has the purpose or effect of substantially interfering with an individual's employment or creating an intimidating, hostile, or offensive work environment
   c. Employees who commit any of the following will normally be subject to immediate discharge. This list is not all-inclusive. An

employee may be discharged for serious offenses or for any reason management deems appropriate.

i. Absence without notice for X consecutive workdays
ii. Defrauding company records
iii. Falsifying company records
iv. Physical assault
v. Possessing, selling, distributing, dispensing, manufacturing, or using illegal drugs while on company premises or business
vi. Theft of company, employee, customer, or supplier confidential or proprietary information, resources, or other property
vii. Willfully destroying company, employee, customer, or supplier proprietary information resources, or other property

The key sections here can be found in the Application of Standard, item 9. This item discusses that the organization has the right to monitor employee activities. Unacceptable Conduct, item B.3.j., makes it unacceptable for employees to violate copyright laws and to introduce unauthorized code (software or viruses) into the systems. Make certain that your organization's standards of conduct are modified to meet the needs for protecting information assets.

4 CONFLICT OF INTEREST

I. Guidelines

A. Company employees are expected to adhere to the highest standards of conduct. To ensure adherence to these standards, employees must have a special sensitivity to the ethical and conflict-of-interest situations or relationships, as well as the inappropriateness of personal involvement in them. While not always covered by law, these situations can harm the company or its reputation if handled improperly.
B. A conflict of interest occurs when an employee's personal interests conflict with the company's interests. Conflicts of interest may also involve relationships between members of the employee's immediate family and the company. Such situations are frequently "gray" areas of decision for the employee. In conflict-of-interest situations, employees are expected to act in the best interests of the company.
C. The following guidelines for ethical behavior in conflict-of-interest situations are established for all employees:
    1. When actual or potential conflict-of-interest situations arise, or where there is an *appearance* of such conflict, employees shall remove themselves from involvement in the matter. In no case should employees become involved to the extent where they are or could be influenced to make decisions that are not in the company's best interest.

2. Employees shall not solicit or accept personal gain, privileges, or other benefits through involvement in any matters on behalf of the company.
3. Employees shall direct their efforts to company business while at work, and shall use company resources only for management-approved activities. Resources include, but are not limited to, equipment, supplies, corporate information, and company-paid time.

II. Application of Guidelines

A. Whenever faced with an actual or potential business-related conflict-of-interest situation, employees shall seek guidance from their supervisors.
B. When conflict-of-interest questions cannot be resolved within the organizational unit, employees may request advice from the General Auditor.
C. When requested, employees shall also disclose actual and potential conflict of interest situations to the General Auditor who shall review each situation and advise the organizational unit of any recommended action the employee should take.

III. Common Conflict of Interest Situations

A. The specific situations described in this section are common, but are not all-inclusive of business-related conflict-of-interest situations that may arise for Company Corporation employees.
   1. Gifts, etc.: Giving gifts, providing meals and entertainment, and offering site tours and product samples are common business practices. Because the intent of these practices is to build relationships and influence business decisions, such practices can result in conflicts of interest. Company expenses incurred in any of the following situations are subject to organizational approval.
      a. Gifts: Gifts generally benefit the employee, but not the Company. In dealing with suppliers, customers, or others outside the Company, employees shall not accept or give money or gifts, except an occasional, unsolicited, nonmonetary item of a token nature, such as an advertising novelty of nominal value.
      b. Meals and entertainment: In dealing with suppliers, customers, or others outside the Company, employees shall not accept or provide meals or entertainment, except when there is a business purpose. The provider of the meal or entertainment should be present at the occasion. Frequent or repeated acceptance of meals and entertainment may be an indicator of the employee's personal gain, and could raise questions about the

legitimacy of the business purpose for such occasions. When there is a business purpose for frequent meals or entertainment, the Company encourages reciprocation.

c. Travel: When there is a business purpose for travel, the Company should pay travel expenses. Employees should not accept air transportation offered by suppliers or others outside the Company when convenient commercial transportation is available. Generally, the Company should pay for lodging expenses.

d. Product samples: If Company wants a sample product or service of more than nominal value, Company should pay for it.

2. Outside work: Employees who have another job outside of Company shall not represent themselves as performing work for Company when doing such jobs. Furthermore, they may not use Company resources in performing the other job.
3. Interest in outside business organizations: Employees shall avoid significant financial or management interest in any business that does or seeks to do business with Company if such involvement could cause employees to make business decisions that are not in Company's best interest.
4. Use of confidential or proprietary information: Employees entrusted with such information shall restrict access and use to authorized individuals inside and outside the Company who have a clear business need to know this information.
5. Insider trading: No employee who has material nonpublic ("insider") information relating to the Company may use that information in buying and selling securities of Company, either directly or indirectly. Furthermore, employees may not engage in other actions to take personal advantage of that information or pass it on to others. Even the appearance of an improper transaction must be avoided to preserve the Company's reputation for adhering to the highest standards of conduct.

Item III.A.4 discusses that the use of confidential or proprietary information must be controlled to those with an identified business need for access. Wherever possible, have the corporate policies support the information security policy.

5 COMMUNICATION

I. General

A. Company is committed to building good relationships by effectively communicating with employees, customers, (shareholders), and the general public. Employees are encouraged to seek guidance from their management regarding interaction with these groups.

B. All Company communications shall be: (1) truthful, credible, and consistent with the Company's performance and actions; and (2) in accordance with applicable legal and regulatory requirements.

II. Internal Communication

A. A two-way flow of information is encouraged and expected. Ideas and information should flow between and among employees and organizations at all levels to enhance understanding.
   1. Each employee is expected to keep management informed about issues that concern or may impact Company employees and customers. Every supervisor is expected to maintain an open environment that encourages employees to provide them with an upward and free flow of information.
   2. Timely information should flow in a cascading manner, from management to every level within the Company, so each employee is informed about the Company's plans and results, as well as issues that affect them as individuals. Every supervisor is expected to use regular meetings, written communications, and any other appropriate means to ensure that there is a continual flow of information and ideas to and from all employees.

B. Companywide publications and news groups are provided to help keep employees informed about policies and events of concern to the Company. However, these vehicles are not intended to replace face-to-face dialogue, which is critical between all levels of employees.

C. All levels of management should use established vehicles to convey information of companywide interest.

III. External Communication

A. Company is open, honest, and willing to help media and others seeking information about the Company. However, each employee shall take care not to disclose information that violates the privacy of employees and customers. Each employee shall also take care not to disclose information that is proprietary or could be of strategic or competitive business value to others.

B. Company management shall determine which employees have authority to sign correspondence or other external communications or issue public statements on behalf of the Company. Formal communications to audiences on behalf of the company, such as speeches, technical papers, and brochures, shall be reviewed by Public Relations.

C. All communication with the media, such as newspapers, radio, television, news groups, and magazines, shall be approved by Public Relations. Only Public Relations may release written communications to the media.

Of all the corporate policies, this one may be most beneficial to the information security process. It discusses what kinds of things are appropriate in communications (regardless of the medium) coming from employees and the organization, and who is authorized to approve distribution of information outside the organization. Use this policy to support all electronic communication policies. It may be necessary to have some of the following supporting documents and policies.

6 ELECTRONIC COMMUNICATION SYSTEMS (ECS) (E-MAIL, cc:MAIL, VOICE-MAIL, VIDEO-MAIL, OTHER)

Policy

The use of electronic communication systems (ECS) is increasing in the workplace. Therefore, the Company has established certain standards for use with such mediums. The ECS and all information and communications transmitted by, received from, or stored in these systems are the property of the Company and are to be used by employees only for management-authorized purposes.

Provisions

1. As property of the Company, employees are not to have a reasonable expectation of privacy or a personal privacy right in ECS and related systems.
2. To ensure that the use of ECS is consistent with this policy, the Company may, at its discretion, from time to time, monitor the use of such systems without prior notice. Such monitoring may include, but is not limited to, printing and reading all communications entering and leaving the ECS.
3. ECS are to be used for management-approved activities only.
4. No ECS message is to be created or sent which may constitute intimidating, hostile, or offensive material on the basis of race, color, creed, religion, national origin, age, sex, marital status, lawful alien status, nonjob-related physical or mental disability, veteran status, sexual orientation, or other basis prohibited by law. The Company's policy against sexual or other harassment applies fully to ECS, including same-sex harassment.
5. In accordance with the Company's No Solicitation, No Distribution, or Posting Policy, the use of ECS for solicitation of any kind, unless company sponsored, is expressly forbidden.
6. All passwords and related security codes are the property of the Company
7. The sharing of passwords with unauthorized personnel violates this policy.

8. Noncompliance with any portion of the above may result in disciplinary action, up to and including termination.

7 INTERNET SECURITY POLICY

Introduction

The Company, through the Internet, provides computing resources to its staff to access information, communicate, retrieve, and disseminate organization and business-related information. Use of the public Internet by Company employees is permitted and encouraged where such use is suitable for business purposes in a manner that is consistent with the Company's Code of Corporate Responsibility, the policy on Electronic Communication Systems, and as part of the normal execution of an employee's job responsibilities. In addition, the Company provides intranet facilities as a means of sharing timely organization and business-related information through the Company; as such, it is to be used by employees only for management-authorized purposes.

Standards

1. The use of Company-provided access to the Internet is intended exclusively for management-approved activities.
2. All access to the Internet by employees must be done through the Company-provided method.
3. All publications/content files not classified as PUBLIC in accordance with the Company Information Classification Policy, must be approved by Corporate Communications.
4. All business cases for Internet initiatives must be submitted to Company Network Control and Information Security.
5. Company Internet users must report all security-related incidents to appropriate management upon discovery.
6. The Company's policies regarding Employee Standards of Conduct, Conflict of Interest, Code of Corporate Responsibility, Equal Employment Opportunity and Diversity in the Workplace, Electronic Communication Systems, Information Protection, and Protecting and Developing the Company's Intellectual Property also apply to the Internet.
7. Employees must take precautions to prevent the introduction of viruses within the enterprise when downloading information or files from the Internet.
8. The introduction and use of modems in the enterprise must be authorized by Information Security and the Network Control Group.
9. All Domain names must be requested through the Network Control Group.

10. Noncompliance with any portion of the above may result in disciplinary action, up to and including termination.

8 ELECTRONIC COMMUNICATION POLICY

The Company maintains a voice-mail system and an electronic-mail (e-mail) system to assist in the conduct of business within the Company. These systems, including the equipment and the data stored in the system, are and remain at all times the property of the Company. As such, all messages created, sent, received, or stored in the system are and remain the property of the Company.

Messages should be limited to the conduct of business at the Company. Voice-mail and electronic-mail may not be used to conduct personal business.

The Company reserves the right to retrieve and review any message composed, sent, or received. Please note that even when a message is deleted or erased, it is still possible to recreate the message; therefore, ultimate privacy of messages cannot be ensured to anyone. While voice-mail and electronic-mail may accommodate the use of passwords for security, confidentiality cannot be guaranteed. Messages may be reviewed by someone other than the intended recipient. Moreover, all passwords must be made known to the Company. The reason for this is simple: your system may need to be accessed by the Company when you are absent.

Messages may not contain content that may reasonably be considered offensive or disruptive to any employee. Offensive content would include, but would not be limited to, sexual comments or images, racial slurs, gender-specific comments or any comments, that would offend someone on the basis of his or her age, sexual orientation, religious or political beliefs, national origin, or disability.

Employees learning of any misuse of the voice-mail or electronic-mail systems or violations of this policy shall notify the Director of Human Resources immediately.

These policies can be used to expand and support the organization's overall communication policy.

9 GENERAL SECURITY POLICY

It is incumbent upon Company management to provide a safe and secure workplace for all employees. Senior management and the officers of Company Corporation are also required to maintain accurate records and to employ internal controls designed to safeguard Company assets and property against unauthorized use or disposition. The assets of the com-

pany include, but are not limited to, physical property, intellectual property, patents, trade secrets, copyrights, and trademarks. Additionally, it is the responsibility of line management to ensure that staff is aware of and fully complies with the Company's security guidelines and all laws and regulations. Management is also responsible for having periodic reviews and audits to ensure the compliance level of all policies, procedures, practices, standards, and guidelines. Employees who fail to comply with the policies will be treated as being in breach of Company's employee standards of conduct.

This policy establishes the organization's overall concept of security and what is expected from the Company. As with all policies, the organization wants employees, stockholders, and interested third parties to know what its stance is on protecting all of the assets of the organization.

10 INFORMATION PROTECTION POLICY

Information is an essential asset of the Company. All information created in support of the business process, whether it is computer generated, manually produced, or spoken, is the property of the Company. To ensure that business objectives and customer confidence is maintained, all employees have a responsibility to protect information from unauthorized access, modification, disclosure, and destruction, whether accidental or intentional.

Senior management and the Officers of the Company are required to employ internal controls designed to safeguard company assets, including business information. It is a management obligation to ensure that all employees understand and comply with the Company's security policies and standards, as well as all applicable laws and regulations. Employee responsibilities for protecting Company information are detailed in the Information Protection Policies and Standards.

Company management has the responsibility to manage corporate information, personnel, and physical property relevant to business operations, as well as the right to monitor the actual utilization of all corporate assets. Employees who fail to comply with the policies will be considered to be in violation of the Company's Ethical Standards of Conduct and will be subject to appropriate corrective action.

11 INFORMATION CLASSIFICATION

Policy

Company information includes electronically generated, printed, filmed, typed, or stored information. Information is a Company asset and is the property of the Company. Information must be protected according to its sensitivity, criticality, and value, regardless of the media on which it is

stored, the manual or automated systems that process it, or the methods by which it is distributed.

Provisions

1. To ensure the proper protection of corporate information, the Owner shall use a formal review process to classify information into one of the following classifications:
   a. Public: Information that has been made available for public distribution through authorized Company channels. (Refer to Communication Policy for more information.)
   b. Confidential: Information that, if disclosed, could violate the privacy of individuals, reduce the Company's competitive advantage, or cause significant damage to the Company.
   c. Internal Use: Information that is intended for use by all employees when conducting Company business. Most information used in the Company would be classified Internal Use.

Responsibilities

1. Employees are responsible for protecting corporate information from unauthorized access, modification, destruction, or disclosure, whether accidental or intentional. To facilitate the protection of corporate information, Associates responsibilities have been established at three levels: Owner, Custodian, and User.
   a. Owner: The Company management of the organizational unit, department, etc. where the information is created, or that is the primary user of the information. Owners are responsible for:
      i. Identifying the classification level of all corporate information within their organizational unit
      ii. Defining appropriate safeguards to ensure the confidentiality, integrity, and availability of the information resource
      iii. Monitoring safeguards to ensure they are properly implemented
      iv. Authorizing access to those who have a business need for the information
      v. Removing access from those who no longer have a business need for the information
   a. Custodian: Employees designated by the Owner to be responsible for maintaining the safeguards established by the Owner.
   b. User: Employees authorized by the Owner to access information and use the safeguards established by the Owner.
2. Each Vice President shall appoint an Organization Information Protection Coordinator who will administer an information protection program that appropriately classifies and protects corporate information under the Vice President's control and makes employ-

ees aware of the importance of information and methods for its protection.

3. Declassification — Classified information normally declines in sensitivity with the passage of time. Downgrading should be as automatic as possible. If the information Owner knows the date that the information should be reclassified, then it might be labeled as: *Confidential until (date).* There should be an established review process for all information classified as confidential, and reclassified when it no longer meets the criteria established for such information.

These last two policies are the cornerstone for all of the information security policies. These are not information systems policies, but belong in the corporate policy documents.

Chapter 8
Writing Procedures

1 INTRODUCTION

Procedures are as unique as the organization. There is no generally accepted standard for the proper way to write a procedure. What will determine how procedures look will be how they currently look or what will work best to provide the target audience with what it needs. This means that it might be necessary to use a number of different styles. This chapter examines what some of those procedure styles look like and how they are used.

2 Definitions

2.1 Policy

A policy is a high-level statement of enterprise beliefs, goals, and objectives and the general means for their attainment for a specified subject area.

2.2 Procedure

Procedures spell out the specific steps of how the policy and the supporting standards and guidelines will actually be implemented. They are a description of tasks that must be completed in a specific order.

2.3 Standard

Standards are mandatory activities, actions, rules, or regulations designed to provide policies with the support structure and specific direction they require to be meaningful and effective. They are often expensive to administer and, therefore, should be used judiciously.

2.4 Guidelines

Guidelines are more general statements designed to achieve the policy's objectives by providing a framework within which to implement procedures. Where standards are mandatory, guidelines are recommendations. See Exhibit 1 for the more important keys to writing.

3 WRITING COMMANDMENTS

Write to the Audience: Procedures are created and implemented with the sole purpose of being read and used by the user community. Always

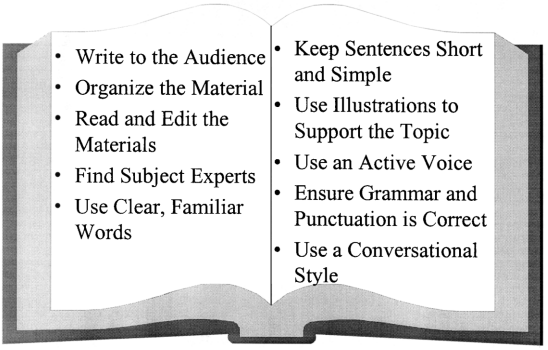

Exhibit 1. Writing's important keys.

keep the audience for these procedures in mind when writing. Before any procedure can be written, it will be necessary to know who the audience is and what its level of knowledge of the subject at hand is.

Every department has its own language; therefore, the procedures must be addressed to them in terms to which they are accustomed. If one writes procedures using the wrong "language," the procedure may as well be written in Sanskrit. The intended audience will not be able to understand it, or will find in difficult to follow.

Organize the Material: The procedures must be written in a logical and flowing manner so that the reader can understand the meaning. If the text is not properly planned, the possibility is great that the intended audience will not clearly understand what is expected. The procedure must be broken into easily digestible bits of information. Do not expect the user to read a long and involved passage and then successfully execute the appropriate processes.

Read and Edit the Materials: Do not just run the spell checker and assume that the editing is complete. Before handing the material to the editor, proofread what has been written and see if it makes sense. If unable to understand what has been written, then it will probably even more difficult for others to understand.

Find Subject Experts: The first step in any procedure development process is to either know the subject or to find someone that does and use their knowledge to write the procedure. The subject expert may not understand the procedure writing process; thus, it may be necessary to sit with him or her and take notes on how the process works and then write the procedure. Make sure that one of the editors is the subject expert. However, the subject expert should not be the person to test the procedure. The

Exhibit 2. Sample of proper words to use in writing policies and procedures.

Eliminate Unnecessary Words	
Words to Avoid	**Familiar Words**
accordingly	so
applicable	apply to
compensate	pay
foregoing	this
furthermore	also
in order to	to
in the near future	soon
subsequently	after

subject expert knows the topic so well that he or she might assume information that is not present in the written procedure.

Use Clear, Familiar Words: The procedure's intended audience will not be pleased if confronted with a document filled with unfamiliar words, expressions, and acronyms. It will be important to have a definition section in some procedures. This should be done up front and provide the reader with whatever is necessary to complete the process at hand.

Do not use big words; remember the reading and comprehension levels of the intended audience. Multiple syllables may be imprecise; avoid the use of the various "ese" languages (financialese, auditese, legalese, securityese, computerese, etc.). See Exhibit 2 for other samples of words to avoid.

Make sure to define all acronyms. There is nothing more irritating than to be reading a text that contains a number of *TLAs* (a TLA is a Three-Letter Acronym for three letter acronyms). The user will lose interest and comprehension if there are undefined terms in the text.

Keep Sentences Short and Simple: Remember the KISS (Keep It Simple Sweetie) principle. Long sentences increase the level of frustration of the user and decrease the level of understanding. An appropriate average sentence length for procedures is between 10 and 15 words. Unless one is a writer of the caliber of a James Joyce, it would be wise to keep the sentences to the 15-word maximum level.

Use Illustrations to Support the Topic: "A picture is worth a thousand words" may be a cliché, but it is true. Whenever applicable, break up the text with a graphic that depicts what is being discussed. These graphics can be pictures, charts (flow, pie, bar, etc.), tables, or diagrams. These will help the user visualize the subject and can provide the material necessary for a clearer understanding of the process.

Illustrations include the use of screen prints. This will help the user when interacting with a computer system. By providing a picture of the screen, the user will be able to visualize what the process looks like and what is expected as a response.

Use an Active Voice: In the active voice, sentences stress what must occur. It will identify who is responsible for what action. For example, a *passive voice* might read as follows: "All tape drives are to be cleaned by the tape operators." An *active voice* might read as follows: "The tape operators are responsible for cleaning the tape drives on each shift." The active voice identifies who is responsible and for what they are responsible.

Ensure Grammar and Punctuation Are Correct: The number-one deadly sin is not taking care of this key element. Too many times, materials have been sent out for content review and the text is filled with errors in grammar and punctuation. It is difficult enough to get a critique of the subject; by presenting the reviewer with error-filled material, he or she will correct the form and forget to comment on the substance. If this is not one's strong suit, find someone that can do these edits.

Use a Conversational Style: This does not mean that the text should be full of slang and idioms; it should just be presented in an informal style. Most people communicate better when speaking than when writing. It could be that many individuals write to impress the reader, as opposed to writing to express an idea. One very easy way around this problem is to write as if one is talking to the intended audience. However, if there is the tendency to speak like William F. Buckley, Jr., then one might want to have someone else review the material. Although a conversational style is preferred, this form does not relieve the writer of the responsibility of being precise.

4 KEY ELEMENTS IN PROCEDURE WRITING

There are four key purposes for writing a procedure.

1. The first is to fulfill some need. If a task or process has to be performed in a specific manner, then there is a definite need for a procedure.
2. Once the need has been established, it will be necessary to identify the target audience.
3. Describe the task that the procedure will cover. It will be necessary to have opening remarks that present the scope of what the procedure is attempting to accomplish.
4. The intent of the purpose should also be made known to the user.

5 PROCEDURE CHECKLIST

Not every procedure will require all of the elements found in the procedure development checklist (see Exhibit 1). Some might even require additional steps. As with any checklist, this is only a series of thought starters. The list that will be used may have additional items, or fewer items.

1. Title: Establish what the topic of the procedure is going to be. Try to avoid being cute with the choice of words. Remember, you are writing for a business environment.
2. Intent: Discuss in general terms what the procedure is attempting to accomplish.
3. Scope: Briefly describe the process that the procedure is going to cover (e.g., implementing a UNIX userid request).
4. Responsibilities: Identify who is to perform what steps in the procedure. Use job functions rather than individual names.
5. Sequence of events: It is very important for the user to understand the timing and conditions for performing the tasks identified in the procedure. Some tasks are not executed at a specific time, but must be performed when a specific condition is met.
6. Approvals: Identify any necessary approvals and when these approvals must be met. Most will be obtained prior to the execution of the procedure process.
7. Prerequisites: List any preconditions that must be met before starting the procedure process.
8. Definitions: Remember the audience. It will be beneficial to include a discussion of any terms and acronyms that are included in the body of the procedure.
9. Equipment required: Identify all equipment, tools, documents, and anything else the individual executing the procedure will need to perform the tasks.
10. Warnings: Some tasks, if operated in an improper sequence, could cause severe damage to the enterprise. Identify those key tasks and review the importance of understanding exactly when the task is to be executed and under what set of circumstances.
11. Precautions: Identify all steps to be taken to avoid problems or dangers (e.g., "unplug before performing maintenance").
12. Procedure body: These are the actual steps to be performed in the execution of the procedure.

6 PROCEDURE STYLES

There are perhaps as many as ten different styles of procedures. Any one of them could meet the needs of an organization. Each of them has its advantages and disadvantages. Sections 6.1 to 6.3 examine three of the most popular forms of procedures and identify the positive side to each, as well as any shortcomings.

6.1 Narrative

Narrative procedure style presents information in paragraph format. It presents the process in a conversational, or narrative, form. This method does not present the user with easy-to-follow steps; it requires the user to

read the entire paragraph to find out what is expected. This method is recommended for such items as policy statements, company philosophy, or background material.

6.2 Flowchart

Flowcharts are pictorial representations in which symbols are used to depict persons, places, actions, functions, or equipment. They give the user diagram of the decision-making process and what is expected at each step when a decision is made.

The flowchart is best used when providing the user with an overview of what the process is going to be. The flowchart will help the user understand his or her portion of the procedure. Users will be able to see where decisions are to be made and what direction to take based on the decision. It will be necessary to have a key to ensure that the user understands what the flowchart symbols mean.

The flowchart procedure style is best used to present an overview for the user and should be considered as a supplement to the actual procedure text. This process of laying out the procedure in a flowchart is actually beneficial to the writer of the procedure. By developing a decision flow process, the procedure writer will have a better chance of developing a logical and correct procedure.

6.3 Playscript

For anyone who has ever been in a play or has had the opportunity to read a play in literature class, this style will be familiar. The process identifies each of the main participants, the actual commands to be entered, and any direction needed to complete the process.

The playscript identifies each individual involved in the procedure. Each step involved in the procedure is described in detail and when each step is to be executed. The playscript is easy to understand and the language used eliminates unnecessary words (adjectives and adverbs). Keep the sentences to the point; remember, you are writing procedure — not the great American novel. A typical statement might be “sign and date forms” or “forward form 1040A to supervisor.”

In the playscript style portrayed in Exhibit 3, it is best to only describe one function in any one step. As part of the definitions section of the procedure, define the key participants in the procedure and use a form of shorthand to call out that participant. For example, instead of having to identify the Corporate Information Officer, use CIO. For the Manager of Information Systems, Operation, and Quality Assurance, one might want to shorten this title to Manager. The key here is to keep it simple, yet eliminate any confusion.

Exhibit 3. Sample playscript procedure.

Requestor	Complete userid template Forward to supervisor for approval
Supervisor	Approve userid template and forward to Account Administration
Account Administration	Process request

Another variation on the playscript style of procedure is the *tree style* (see Exhibit 4). This style uses the same basic layout of the playscript, but it allows the user to drill down to each of the steps identified.

7 SUMMARY

When writing procedures, it is best to keep the language as simple as possible. Attempt to stay away from flowery phrases and multi-syllable words. Keep the sentences short and the terms crisp. Identify what each role is in the procedure and find the style that best meets your organization's needs.

This chapter reviewed the definitions of policy, procedure, standard, and guideline. Exhibit 1 is discussed and the material reinforced what was covered in the Chapters 3 and 4.

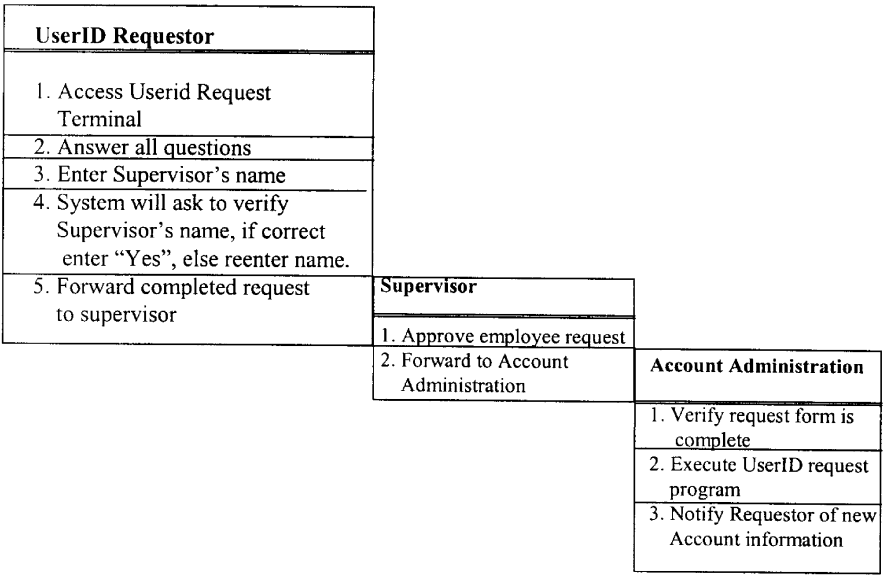

Exhibit 4. Sample playscript drill down procedure.

Also examined were procedure key elements:

- identify the procedure need
- identify the target audience
- establish the scope of the procedure
- describe the intent of the procedure

This chapter also discussed the procedure 12-point checklist and then examined three styles of procedures:

- Narrative
- Flowchart
- Playscript

Chapter 9
Creating a Table of Contents

1 INTRODUCTION

The document that will be most used is the actual procedure document. This will be generally used as a reference document; that is, most employees will not sit down and read the procedures cover-to-cover. Therefore, organizing the procedures based on topics and a good table of contents will be a great asset.

This chapter examines topics that should be considered for information protection policies and procedures.

2 DOCUMENT LAYOUT

Most textbooks, which a policy and procedure document is, have the same general look about them. The physical characteristics will remain about the same regardless of the organization. This chapter reviews what normally appears in the typical policy and procedure document; the next few paragraphs can be used as a checklist for the actual document being prepared. The items discussed are not requirements (standards), but are actually guidelines.

3 DOCUMENT FRAMEWORK

The first section of the procedure document usually contains those pages that are considered to be unnumbered; that is, they normally have some form of roman numeral. These documents are typically as follows.

3.1 Title Page

This is the first page of the document and it identifies exactly what the document is. Some experts recommend that Management Endorsement appear first. What will be required within one's organization depends on how procedure documents are prepared. Keep the title page as clean and simple as possible.

A suggestion — keep the title as brief as possible and choose the words as carefully as possible. The document will probably be known by a word or acronym derived from the full title. Something like Information Protection Policies and Procedures might be shortened to IP3; but something like Customer User Primer (CUP) may not generate the level of respect expected. Choose the title carefully.

When selecting a title, there are some words that one might want to consider avoiding. Among them is the term "security." Security means different things to different people. The term is imprecise; it conjures up images of guards, dogs, fences, guns, and badges. This is not the image that many would want for the information protection document.

3.2 Management Endorsement Page

Of all the important pages to be found in the document, each document should have a message from someone in a position of authority to the document holders. This message ensures that the policies, standards, and procedures contained in the document are implemented by the organization. The endorsement page will provide visible evidence that the document and its contents are backed by management. If at all possible, the signatory should be the CEO, President, Executive Vice President, or the CIO to provide maximum impact.

The Management Endorsement should state briefly the aim of the document: the basis for the document (i.e., industry standards, internal controls, company policy, legislation, regulations, etc.).

3.3 Amendment Record

This is a historical record of all of the updates made to the document. It will identify what changes were made to the document, who submitted the changes, and when the changes were implemented. In many documents, the amendment record establishes that unauthorized revisions are not to be made.

The first of the numbered pages in the procedure document is the Table of Contents. This will list the materials to be found in the text and is divided into the categories of *Section, Topic,* and *Subject,* and the place to find the document (page number). The Table of Contents provides a cover-to-cover review of the contents and the organization of the document.

4 BODY OF THE DOCUMENT

Just as the document itself has a structure, so the subject matter of the document has its own structure. To allow users better access to the material, it will be necessary to order the materials in some logical sequence. To

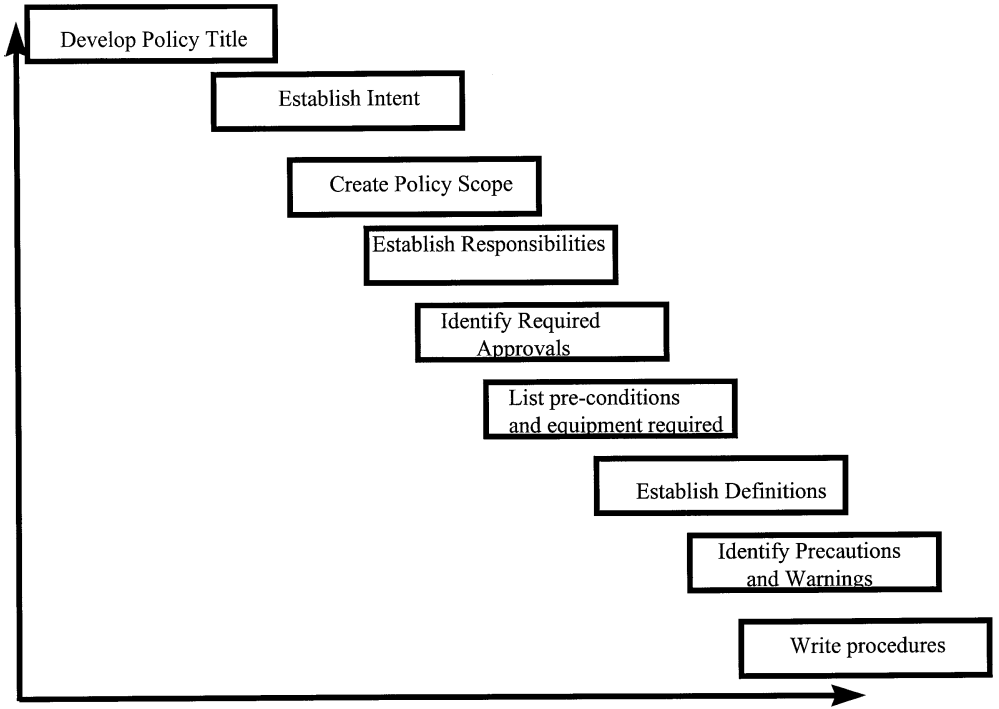

Exhibit 1. Procedure writing checklist.

assist in this process, it is recommended that the body of the document be divided into three divisions:

- Section: the primary division
  - Topic: secondary division
    - Subject: tertiary division

5 SAMPLE TABLE OF CONTENTS

1. Telecommunications
   - 1.1 Remote Access
     - 1.1.1 Modem Usage
     - 1.1.2 Token Cards
     - 1.1.3 User Authentication
   - 1.2 Internet
     - 1.2.1 Firewall Administration
     - 1.2.2 Firewall Services and Usage Policy
     - 1.2.3 Mail and News Groups
     - 1.2.4 FTP Usage and Controls
     - 1.2.5 External Internet Access
     - 1.2.6 Read Security of News Groups
     - 1.2.7 Cookies
   - 1.3 Workstation Administration
     - 1.3.1 Time-out Screen Saver Passwords
     - 1.3.2 Virus Controls
     - 1.3.3 Standard Software Packages
     - 1.3.4 Backups
   - 1.4 Electronic Communications
     - 1.4.1 Telephone Usage
     - 1.4.2 Telephone Log Monitoring
     - 1.4.3 Voice-Mail
     - 1.4.4 Voice-Mail Directories
     - 1.4.5 E-mail Policy
     - 1.4.6 E-mail Privacy
     - 1.4.7 Standardized E-mail and News Special Interest Groups

6 POST BODY DOCUMENTS

The subject *Index* should be organized and written after the document is completed. Many of today's word processor packages will generate the table of contents and the subject index. Follow the instructions for document setup and the software will do the rest. This is a great advancement from the manual method.

The *Appendices* are contained in a separate *Section* at the back of the document. They contain information of a supplementary nature that pro-

vides the reader with background or additional information. The information here is generally not an actual part of the policies or procedures, but is supplementary. The typical information found in the Appendices include:

- glossary of terms
- abbreviations, acronyms, initials, codes
- reference lists
- publication lists
- statistics
- background philosophy
- organization charts, staff lists
- legislation, bylaws

7 PREPARING A DRAFT TABLE OF CONTENTS

Now that the mechanics of the document have been discussed, it will be necessary to identify what topics should be considered for inclusion into a typical information security policy and procedure document. This process will take place after all of the pre-implementation tasks are completed. That is:

- the Core Group established
- the scope or mission statement written
- the critique committee chosen (discussed in Chapter 9)

First, it will be necessary to gather all possible available examples. This activity will help the Core Group when conducting the *brainstorming* process. Read all of the gathered material, search the Internet for information security policy and procedure documents, and do an initial indexing of the subjects that might need to be covered.

It is recommended that once the material has been reviewed, write down the various subjects on post-it notes and post those notes onto the wall of the conference room. Once the subject cards have been posted, assemble the Core Group and review the areas that might be included in the document. It will be necessary to have a facilitator run the meeting. Have the group write down all of the topics that they believe should be part of the document.

To provide form to the process, it might be beneficial to examine one subject category at a time. The team should accept all ideas (initially) and document each entry (usually on a post-it note). Once all of the categories are examined, the post-it notes can be added to the wall and the team then reviews the results to look for duplicates and where similar ideas could be combined. Exhibit 2 depicts the results of one brief brainstorming session.

8 SECTION TO BE CONSIDERED

Having examined how what a policy and procedure document looks like, and how to identify what subject materials might be included, one can

Exhibit 2. Results of brainstorming session.

Telecommunications	Physical Security	Administration	Information Protection
Firewall administration	Whiteboards and sensitive material	Contractor controls (information access, personnel, hiring, discharge, etc.)	Password conventions
Firewall services and usage policy	Desktop protection	Cleaning crews	Protection customer information
Mail and news usage	Line of sight	Change procedures	Information access and authorization controls
Telecommunications	Off-site storage	Communication with the press	Levels of ROOT exposure
Telephone eavesdropping	Company address and phone number usage	Spin teams	Audit logs maintenance and storage
Voice-mail directory for entire company	Asset marking	Investigations	Backups of information
Web access and download	Asset protection	Third-party requests for access	Posting employee lists in public areas
Internet access control (external)	Cabinet controls	Background checks	Information classification (secret, critical, confidential, internal use, restricted, public, private, etc.)
Read security of news groups	Clear (clean) desk policy	Credit backgrounds	Release of information to public
Access control	Critical incident procedures	Ethics policy	Marking classification levels
Token card usage	Network failures	Drug testing	Discussing classified information with third parties
Access authorization levels	Shredding documents	Company identification away from campus	Approval process for release of confidential information
User authentication	Removal of trash	Reception area conversations	Nondisclosure agreements
Login banners	Off-site assessments	Hiring foreign nationals	Confidentiality agreements
Screen saver time-outs	Duress response	Hiring and termination policy	Employee discussion of company business (at work and off site)
Work station administration	visitor procedures	Export regulations	
E-mail policy	Investigations	Monitoring for compliance	
E-mail privacy	Tailgating, piggy-backing	Employee privacy	
Standardized e-mail and news SIGs	After-hours access (employee, contractor, visitor)	Telephone log monitoring	
Server administration	Physical access to building	Threat management	
Modem usage	Employee identification cards	Disaster planning	
	Contractors' identification cards	State and federal law compliance	
	Visitor badges	Intercom usage	
	Hardware protection (on-site, off-site)	Phone usage	
	Mailbox access	Employee training	
	Alarms	Employee standards of conduct	
	Keys and lock controls	Workplace violence	
	Security card and hardware token handling	Health and safety standards	
	Electronic defenses	Risk assessment practices	

Exhibit 2. Results of brainstorming session. *(Continued)*

Telecommunications	Physical Security	Administration	Information Protection
	Physical access (false ceilings, plaster board, etc.) Access control (copy machine, printer, fax machine, etc.) Emergency response plans Business contingency plan Disaster recovery plan Threat assessments (natural, accidental, and intentional)	CERT responsibilities Security incident reporting Jurisdiction and responsibility definitions	Internal system auditing Audit responsibilities System monitoring Protecting company intellectual properties Monitoring Web activities System alarms Intrusion detection Trade secret controls Competitive advantage controls Plans and strategic information Information classification categories Release of employee information Shredding documents Need to know

now examine what topics normally belong in an information protection document.

8.1 Access Control

Access control is the foundation upon which all of the other information protection procedures will be built. In this section, the overall corporate information protection policy is either published or restated. The keys in any information security program are the ability to protect against the disruption, modification, disclosure, or unauthorized use of the organization's information assets. The measure of success of the document will be how effectively these objectives are met.

All access control mechanisms (RACF, ACF2, TopSecret, etc.) must support the overall policy for protection of the information. The policy estab-

lishes the foundation on which the *security architecture* will be constructed. The access control mechanisms must determine:

- who is authorized to access the organization's information processing systems
- what information resources the users are authorized to access once they are authenticated to the system
- how the users will be authorized
- what mechanism will be used by the information owner to identify what assets the user is permitted to access
- what information processing resources the user is authorized to access
- when the user can access the resources

The policy must establish the need for control and the procedures must identify the process needed by the users to gain the appropriate levels of access. The policy will lead the organization to establish *standards.* Included in the access control set of standards are the access control packages, the mechanism for granting authorization, and the process implemented for monitoring user activities.

Access is the ability to do something with an information resource; *authorization* is the means by which that ability is explicitly enabled or restricted.

8.2 Authorization

An overall philosophy must be established on information access. The policies and procedures will identify the corporate direction on such topics as *Need to Know* and *Level of Least Privilege.* In the decentralized processing environment, the implemention of safeguards must be based on the fact that no enterprise has sufficient resources to protect all its information assets.

This section identifies the steps required for an employee to gain access to data, information, and transactions. It reinforces the principles discussed in the information classification section.

Once the information *owner* has approved a user's access, there are a number of methods that can be used to verify if a request for access can be granted. Included in the procedures should be a discussion on the limitations that can be implemented. These will include, but are not limited to:

- *identity:* this is the most common form of authorization access and it revolves around the userid and password
- *roles:* an individual can be assigned to a group or a role and be granted the same authorization levels as the others in that group or role

- *location:* authorization can be restricted to the location of a specific terminal or an IP address
- *time:* authorization can be limited by the time of day or days of the week

Access Control Lists (ACLs) refer to a register of the users, including groups, machines, and processes that have been granted permission to access a specific information resources (including data, information, and transactions). Access is typically permitted for users to:

- read (copy)
- write
- delete
- execute

8.3 Identification and Authentication

Of all the sections to be used in the document, this section will reach the most employees. Included in this section will be the process required to ensure the individual is in fact that person. Elements that might make up this section include photo IDs, remote access requirements, and system access userids.

Identification is the means by which a user provides a claimed identity to the system. *Authentication* is the means of establishing the validity of this claim. There are typically three means of authenticating a user's identity that can be used alone or in combination:

- something the individual knows *(password)*
- something the individual has *(token card)*
- something the individual is *(biometrics)*

It is necessary to discuss which of these methods will be used by the organization, how the usage will affect the user, and what is expected of the user with regard to keeping the authentication methods secret.

The acquisition of a *userid* and a confidential *password* will be the keys to employees doing their jobs. The procedures must address the steps necessary, as well as the levels of control and safeguards to protect the password as an organization-identified *confidential* information resource.

Passwords: It will be necessary to establish the standards for account passwords. Included in this will be the following subjects:

- using alphanumeric characters
- proper password length (five to eight characters)
- choosing passwords that are not inherently weak (names of family, pets, hobbies, etc.)

- passwords should be kept secret, known only by the user
- password change periods (based on the value of the information and transactions being used)
- password history (user being unable to use the five most recent passwords)
- password and related security codes are the property of the organization
- sharing passwords with unauthorized personnel violates organization policy

The *token card* can take on many forms and can even be a "smart" card. A typical "dumb" card is the standard photo ID card that contains the individual's face and must be visually checked for authentication. "Smart" cards include those that are inserted into a reader or held in proximity to a reading device. The procedures should explain to the employees their responsibilities for protecting these cards and what to do if they are lost, stolen, or compromised.

Biometrics use the characteristics (physiological, behavioral, or physical) to authenticate an individual. Such things as fingerprints, retina imprints, voice, signature dynamics, hand geometry, typing dynamics, and facial recognition are part of the biometrics process of authentication.

8.4 Accountability

Accountability is the process that can connect an individual to an action. The document should inform employees of their responsibilities and that there are tools in place to monitor their activities. Included in these discussions will be the retention period for all logs and who is responsible for reviewing those logs.

8.5 Auditability

As discussed in Chapter 1, every publicly held company is required by the Foreign Corrupt Practices Act (FCPA) to maintain a control system designed to provide reasonable assurance that the assets of the organization are adequately protected. That transactions are executed and recorded in accordance with management authorization. The control system must be supported by written policies and the control environment is regularly evaluated to ensure compliance.

Audit trails maintain a record of system activity both by system and application processes and by individual activity. They can assist in detecting security violations, performance problems, and flaws in applications. Employees must be made aware of what the audit trail is used for and that they are accountable for the actions found in the audit trail.

8.6 Sign-on Banner

The initial sign-on banner should contain the following warning: This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all activities on this system monitored and recorded by system personnel.

In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users can also be monitored.

Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, a report will be made to Management and all evidence will be turned over to the appropriate authorities.

It may be necessary to review the organization's employee standards of conduct and insert the following text:

> Company management has the responsibility to manage corporate information, personnel, and physical properties relevant to their business operations, as well as the right to monitor the actual utilization of all corporate assets.

8.7 Encryption

The first step in requiring encryption is the completion of a *risk analysis* to ensure that the application, system, data, and information requires this level of control. The process of encrypting information causes overhead on the system and slows down response time. Only that information that is highly sensitive should be encrypted.

A brief understanding of what encryption is and how it works may be a beneficial topic for this section. A discussion about proper *key* management should be included. An emergency procedure for lost or inaccessible keys should be part of this section (see Exhibit 3).

Exhibit 3. Cryptography matrix.

Distinct Features	Private Key Cryptography	Public Key Cryptography
Number of keys	Single key	Pair of keys
Types of keys	Key is secret	One key private One key public
Protection of keys	Disclosure and modification	Disclosure and modification for private keys and modification for public key
Relative speed	Faster	Slower (about 1000 times slower)

8.8 Business Continuity Planning

The ability to continue to perform business functions during an emergency is an essential part of any organization's overall information security program. For many organizations, the entire focus on this activity revolves around the data center and its disaster recovery plan (DRP). Business continuity planning (BCP) is much more than just data center directed.

The following three elements of a BCP should be discussed:

- *Emergency Response Phase:* those actions to be taken to protect lives during an emergency situation.
- *Recovery Phase:* this will be the most detailed section; it will discuss the steps required to bring critical applications up and provide a limited level of services. The level of services available will be expanded with each day. The initial group of services will be only those that are most essential to the business process.
- *Resumption Phase:* the steps required to return to normal processing mode must be developed.

An effective plan should include discussion of the following topics:

- scope of the coverage
- objectives
- threats and countermeasures
- backup and recovery sites
- backup site facilities
- telecommunications
- staffing and management responsibilities
- contact and deployment plan
- supplies and infrastructure
- budget and cost estimates
- testing plans
- plan maintenance

The procedure documents should contain a discussion on how to identify and classify threats to specific resources. A *threat* is typically looked upon as intent to do something bad to someone or some enterprise. Threats normally fall into three categories:

- natural (flood, hurricane, tornado, tsunami, windstorm)
- accidents (loss of power, fire, liquid leakage, operator error)
- deliberate (alteration of data, fraud, theft, unauthorized use, vandalism)

Once threats to the organization have been identified, the procedure document should provide employees with a way of prioritizing the threats (see Exhibit 4).

Exhibit 4. Sample threat impact analysis worksheet.

Type of Threat	Probability	Impact to Employees	Property Impact	Economic Impact	Total Possible Impact
	High Low	High Impact		Low Impact	
	4 ↔ 1	4	↔	1	
①	②	③	④	⑤	⑥

Note: The lower the score the better.

Instructions for filling out the form and how to use the results should be included in the procedure document.

1. the identified threat
2. the probability that the threat might affect the building, system, or information
3. if the threat occurred, what the impact on employee health and safety would be
4. the impact to the physical facility
5. the impact to the ability to conduct business
6. the total score (those scoring 10 and higher will need to be examined for additional safeguards to lower the score)

8.9 Risk Analysis and Management

Risk assessment is a method for determining the likelihood and impact of loss of information integrity, availability, and confidentiality. The risk assessment method includes information asset evaluation and identification of threats to, and vulnerabilities of, the target information.

Why do a risk assessment? The assessment will result in a prioritized list of the information most at risk and which could cause unacceptable losses to the business. The prioritized list provides direction as to where information protection controls should be applied first and how much to spend on the controls. The assessment results should be reported to management to allow them to make fact-based decisions and provide approval for implementation of controls. Management will not approve controls for all risks.

Where this occurs, management's reasons should be documented for future reference and planning.

The first step in this process is to identify the information assets within the organization. This would not only include information created within the organization, but also any information used by employees. Included will be such items as databases, spreadsheets, original source documents, bid responses, signature cards, etc. Include all information regardless of how it is created or the media on which it is stored.

Once the information assets are identified, consider the impact on the organization. In traditional risk analysis, there are three types of impact:

- unauthorized or undesirable modification of information (loss of integrity)
- unauthorized or undesirable destruction of, or denial of access to, information (loss of availability)
- unauthorized or undesirable disclosure of information (loss of confidentiality)

Each of these impacts can be accidental or intentional. Take a look at threats, vulnerabilities, and loss.

- **Identifying Threats:** Threats are any activities or events that, under certain conditions, could jeopardize the integrity, availability, or confidentiality of information. Threats can be natural (storms, floods, lightning, rodents) or manmade (theft, vandalism, electrical fire). The possible threats to each type of information must be identified.
- **Identifying Vulnerabilities:** Vulnerabilities are conditions that could allow threats to cause loss of information integrity, availability, or confidentiality. If there is no vulnerability, the existence of a threat is immaterial since the threat cannot cause a loss. Identifying vulnerabilities is the process of estimating the likelihood that the threats will cause loss of information integrity, availability, or confidentiality. The vulnerability of each type of information must be identified.
- **Identifying Loss Impact:** Loss impact is the effect on the business when a vulnerability allows information integrity, availability, or confidentiality to be compromised. Loss impact can be identified as a dollar estimate or some other intangible impact such as loss of customer confidence, competitive advantage, or the organization's reputation. Loss impacts must be identified.

8.10 Information Classification

As has been discussed in Chapter 5, any discussion on information classification should include:

- Information as a corporate asset
- What the classification levels are:

  - Confidential
  - Internal Use
  - Public
- Employee responsibilities
  - Owner
  - User
  - Custodian

8.11 Computer Emergency Response Team

A security *incident* is commonly defined as any unwanted change in the security status quo of an infrastructure. Examples include a key resource being unavailable because it crashed due to an operating system bug, virus problems in office PCs, or an attack on the infrastructure by a malicious person, who could be an insider or an outsider.

An organization needs to ensure that its security policy clearly defines what classifies as a violation. This definition is developed by:

- Law — Have local, state, federal, or international laws been broken? Security-related events are crimes under local, state, federal, or international law, including embezzlement, theft, extortion, vandalism, sabotage, and espionage.
- Regulation — Have regulatory controls been violated?
- Contract — Has a contractual relationship been violated?
- Policy — Has the security policy been violated?
- Custom — Has the status quo been violated?
- Expectations — Have personal, organizational, or societal expectations been violated?

8.12 Quality Control

The control of quality includes processes in place to ensure the integrity of information, software, hardware, and other information resources. The procedures should address such topics as:

- change control for system upgrades and modifications
- promotion to production procedures for applications
- proper testing
- design specifications
- development methodology
- metrics

See Exhibit 5 for more security program topics.

9 SUMMARY

The only limits to the sections and topics that can be a part of the information security policies and procedures document are of what can be

Exhibit 5. What topics a security program should address.

1. Information technology security policy statement
2. Microcomputer and local area network security standards
3. Information classification requirements
4. Ownership, custodial, and user information technology security responsibilites
5. Segregation of duties
6. Personnel security measures
7. Physical security responsibilities as they relate to information technology security
8. Risk analysis
9. Contingency planning requirements
10. Security self-assessment process

thought. Some organizations include sections on Information Highway Access and others discuss Employee Privacy. The key to an effective document is to try and anticipate the needs of the organization ad not get bogged down with too many sections and topics.

Do the research that is necessary to understand where the organization is, how it got here, and what topics need to be addressed. If applicable, use the brainstorming method to identify topics and subjects that can be included in the document and keep the process open for changes.

Chapter 10
Establishing a Critique Process

1 INTRODUCTION

As the policies and procedures are developed, they should be reviewed by someone from the organization with a basic knowledge of the topic and some interest in seeing the project completed. The writing process often drives the writer into a closed environment. That is, the writer becomes immersed in gathering materials, reviewing existing documents, and learning to be a subject expert; as a result, objectivity is often lost. The need for information security controls and safeguards becomes more important than the business objectives or the mission of the organization. To ensure that the policies and procedures meet the proper objectives, it will be necessary to have the documents reviewed by others who can provide a fresh point of view.

2 ESTABLISHING REVIEW PANELS

As discussed in previous chapters, there will be a *Core Group* that will be primarily responsible for drafting the documents. This group will do the research and the writing. This group is also responsible for proofreading the documents and ensuring that they make sense. Remember, after running the spell checker, read–check the document. The spell checker does not care what word is used, as long as it is spelled correctly. So, proofread the document.

After the documents have been proofed, and before they can be sent out for any review, there should be an editor who will review the documents for grammar and punctuation errors. Once this is complete, the documents will be ready to be sent to the *Support Team*.

The Support Team is made up of representatives from each of the major business units and from the corporate central support functions (Human Resources, Legal, Corporate Communications, Auditing, etc.). These individuals review the document from a business perspective and offer comments and suggestions. This team can also be used to help sell the

contents back to their business units. By making them part of the development process, the documents will not be seen as coming from one department, but from the organization as a whole. It is very important to get a strong cross-organizational representation as part of the Support Team.

The Support Team is charged with reporting back to their management on the policies and procedures. They can also be used when preparing to sell the documents to management. By including them in the process, they can provide the Core Group with the concerns of their management. This will allow the Core Group to prepare to meet with the individual managers and address their concerns.

3 WHO SHOULD PARTICIPATE

The Support Team should consist of representatives from:

- Information Systems
- Human Relations (Personnel)
- Auditing
- Labor Relations (especially for Union-represented employees)
- Key units, divisions, departments, groups, etc.
- Selected user departments
- Physical Security
- Information Security
- Legal Staff

If the organization has a policies and procedures group, then they too should be part of the review panel. If there are overseas activities, then it is necessary to get representatives from these organizations as well.

When sending out the documents, it is necessary to let the Support Team know in advance that the documents are coming. If possible, schedule a meeting for the Support Team and review the charter and scope of the project and any pertinent information that will assist them in the review process. It might be beneficial to remind the Support Team that comments are needed on the substance of the material. If they find grammar, punctuation, or spelling errors, have them note those — but what is really needed are comments of the textual material.

Once the documents are sent out, it is necessary to ensure that the Support Team members receive their copies (see Exhibit 1). Too often, material gets lost in either the company mail or into the e-mail dead-letter box. If sending an electronic copy, make sure to select the notification that the recipient has opened the document. Follow up to be certain that the document is being reviewed and make members of the Core Group available to answer questions. Allow the Support Team enough time to review the document (perhaps five to ten working days).

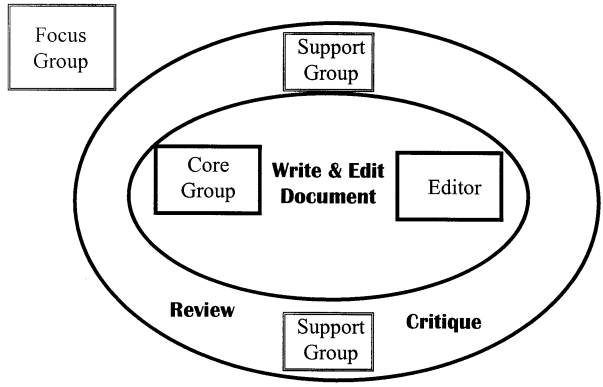

Exhibit 1. Critique and Focus Group visual.

There should be three rounds of reviews. The initial round will be their first review of the document. If possible, indicate in the document what is existing policy and procedure and what is new. If there is new material, identify what area recommended the update. The second or updated round should include as many of the recommendations from the Support Team as possible. It is the responsibility of the Core Group to review every suggestion, and to either implement the suggestion or meet with the group member and explain why no action is being taken.

After all the comments and suggestions have been reviewed and the draft has been updated, send the document out for a second round of review. Try and indicate where the updated draft document is different from the original. As with the initial review process, ensure that all group members get a copy of the document and that they are aware of the deadline for comments to be returned. A proactive approach to this process is strongly recommended. Do not assume that this is a priority task for them. Call them and e-mail them to ensure that their comments can be included in the final draft.

After all the comments and suggestions have been reviewed and acted upon, the document will be ready for a final review. The document should be labeled as Final Draft. The term "final" might cause some group members to actually review the document and forward comments. Remember, not all comments need to be incorporated. Also understand that some comments may require a meeting of the groups to iron out any major differences. It is best to resolve the conflict before the document is published.

A number of years ago, this author was working with a Fortune 10 client that decided to implement an executive employment agreement (EEA).

This EEA was structured so that Executive Vice Presidents and above were prohibited from going to work for direct competitors for one year after leaving the company. This policy was drafted by the Legal Staff and Human Resources. As you might suspect, many of the business units were very concerned as to who was impacted by this new policy. To facilitate the resolution of this concern, a meeting was set up and all of the concerned parties were invited to attend. The Legal Staff and HR reviewed the document with the Support Team and answered all their questions. For many of the group members, their need was additional information so that they could report to their bosses just what this policy meant.

4 COMMENT KEY POINTS

When reviewing the suggestions and comments, remember:

- Not every comment or suggestion must be accepted.
- If there appears to be a conflict, set up a meeting to resolve the issue.
- Whenever possible, implement the comment.
- There is a *weighting* system for comments (all comments are equal, some are more equal than others — know who is suggesting what).
- Understand the politics of the organization.
- Ensure special needs are addressed.

Another key point to remember is that the Audit Staff does not write policy. They are charged with ensuring that the organization's policies and procedures are being followed. They do have strong opinions on what is in the best interest of the organization and how certain activities should be conducted. However, as discussed in Chapter 1, policies and procedures are implemented to support business objectives and the mission of the organization.

5 FOCUS GROUP

The final element in the review process is to establish a Focus Group consisting of representatives from the target audience. Allow them to use the procedures or review the policy and then debrief them as to its effectiveness and their ability to understand what has been presented. If this group (and you will probably want to do this more than once) is able to use what is presented, then the policies and procedures are ready for implementation.

6 SUMMARY

The development of a review group or critique committee is actually five steps. These steps are:

1. writing the document
2. proofreading the document

3. editing the document
4. critiquing the document
5. testing the document (Focus Group)

To meet the organization's needs, it is necessary to establish a small, but knowledgeable review panel. This group should be made up of a cross-section of the enterprise and have members from technical and user groups. All suggestions and comments should be reviewed and those not implemented should be explained to the reviewer as to why they were not accepted. Finally, establish a Focus Group to test the documents to ensure they can be used for the purpose intended by the target audience.

Chapter 11
Selling the Policies and Procedures

1 INTRODUCTION

The missing factor in an effective information protection program is employee involvement. Many organizations go to great lengths to develop an extensive set of controls and countermeasures, purchase the latest technology, design in audit trails, and print out security logs — and still security fails. Often times, this is the result of not understanding the culture and direction of the organization and its employees. To assist in the development of an effective information protection program, it is necessary to examine "war stories" to see where controls failed in other organizations. There are six key elements that lead to the breakdown of an information protection program. This chapter examines these key elements and provides means to resolve the dilemma.

2 TARGET GROUPS

There are three groups to which one must sell the information security policies and procedures (see Exhibit 1). Each group has its own set of needs and concerns. The three groups are:

1. Senior Management
2. Line supervisors
3. Users

2.1 Senior Management

Senior Management expects a sound, rational approach to information security. They are interested in the overall cost of implementing the policies and procedures and how this program stacks up against others in the industry. A key concern is how the policies and procedures will be viewed by the Audit Staff and that the security program will give them an acceptable level of risk.

Exhibit 1. Organization groups and selling techniques.

Group	Best Techniques	Best Approach	Expected Results
Senior Management	Cost justification	Presentation	Funding
	Industry comparison	Video	Support
	Audit report	Violation reports	
	Risk analysis		
Line Supervisors	Demonstrate job performance benefits	Presentation	Support
	Perform security reviews	Circulate news articles	Resource help
		Video	Adherence
Users	Sign responsibility statements	Presentation	Adherence
	Policies and procedures	Newsletters	Support
		Video	

When developing the policies and procedures, it is important to remember these four key points and to act on them. An essential element to the success of any program that requires Senior Management support and approval is to keep them informed. There are three key ways to accomplish this task.

1. Use the Support Team members to report back to their management on the status of the policy and procedure development process. Make certain that the Support Team members are given material that explains where the program is, how the research has been conducted, and what the target dates for delivery are. The development of any procedure document can take six months or more. So schedule regular monthly meetings and give the members a formal write-up on the progress.
2. Use benchmarking. Identify similar businesses or organizations in the same field and talk with them about their program. The easiest way to make these contacts is through membership in such organizations as the Computer Security Institute and a local Information Systems Security Association (ISSA) chapter. Both groups can be found on the Internet. Benchmarking will provide Senior Management with the reinforcement they need. While they are interested in security, they generally do not want to be too far away from what is considered the norm.
3. Meet with Senior Management individually prior to submitting the documents for approval. Work with support group members to find out what are the concerns of their management and how the policies and procedures will assist them in meeting their individual missions or goals and objectives.

If at all possible, never take a new policy cold to the policy review team or committee. Spend the time to meet with them individually to give them the background they need. If this is done, the policies and procedures stand a much better chance of not only gaining approval but, more importantly, acceptance.

2.2 Line Supervisors

These individuals are focused on getting their job done. They are not interested in anything that appears to slow down their already tight schedule. To win them over, it is necessary to demonstrate how the new controls will improve their job performance process. As stressed from the beginning, the goal of security is to assist management in meeting the business objectives or mission.

It is self-defeating to tell supervisors that the new policies are being implemented to allow the company to be in compliance with audit requirements. This is not the reason to do anything, and a supervisor will find this reason to be useless. Stress how the new process will give the employees the tools they need (access to information and systems) in a timely and efficient manner. Show them where the problem resolution process is and who to call if there are any problems with the new process.

2.3 Employees

Employees are going to be skeptical. They have been through so many company initiatives that they have learned to wait. If they wait long enough and do nothing new, the initiative will generally die on its own. It will be necessary to build employee awareness of the information security policies and procedures. Identify what is expected of them and how it will assist them in gaining access to the information and systems they need to complete their tasks. Point out that by protecting access to information, they can have a reasonable level of assurance (remember, never use absolutes) that their information assets will be protected from unauthorized access, modification, disclosure, or destruction.

The type of approach chosen is based on whether the organization has an information security program in place and how active it is. For those organizations with no policies and procedures, it will be necessary to convince management and employees of their importance. For organizations with existing or outdated policies and procedures, the key will be convincing management and employees that there is a need for a change.

3 MANAGEMENT PRESENTATION POINTS

When preparing to present to management, it might be helpful to have answers to the following questions in advance:

- Why is a policy and procedure development project being considered?
- What activity prompted management to act at this time?
- Has there ever been an information security program before?
  - If yes, what is its current status?
- Are there any "unofficial" policies and procedures?
- How are new and existing employees being trained in information security?

It is important to do the research to find out why management chose this particular time to spend some of its limited resources to fund such an activity. As discussed in Chapter 2, find out what management expects of you and develop a mission statement or charter that identifies exactly what the deliverables are going to be.

4 WHY CONTROLS ARE NEEDED

The legal obligations of Senior Management fall into two categories: a duty of loyalty and a duty of care. By assuming office, the organization director commits allegiance to the enterprise and acknowledges that the best interest of the corporation and its shareholders must prevail over any personal, individualized interest. This is known as the duty of loyalty.

In addition to owing a duty of loyalty to the corporation, Senior Management also assumes a duty to act carefully in fulfilling the important tasks of monitoring and directing the activities of corporate management. The "Model Business Corporation Act," which has been adopted in whole or in part by a majority of states, reflects the fact that a corporation acts through the individuals who act on its behalf. These individuals, in executing the corporate mission, are subject to the sanctions that govern the corporation. Shareholders, as well as the corporation itself, place their trust and confidence in corporate leaders. Directors and officers, therefore, are expected to exercise due care in conducting business on behalf of the corporation.

The liability for aiding a corporation in such acts as patent, copyright, or trademark infringements can fall directly on its directors and officers. Corporate white-collar crime is the specific focus of the "Federal Guidelines for Sentencing for Criminal Convictions." Whenever it is necessary to apply these guidelines, consideration is given to organizations that have implemented an effective program to prevent and detect violations of the law.

Additionally, directors and officers are charged with responsibility for the management and protection of corporate assets. This area of responsibility is governed principally by the laws of the state under which the corporation is formed.

An effective information protection program is measured by whether the organization exercised due diligence in seeking to prevent and detect criminal conduct by its employee and other agents. In the event of a security breach, corporate officers must be able to show that reasonable care could avert charges of negligence.

5 IMPACT ON PROFIT AND LOSS

Exercising due care can also have a direct impact on the profitability of a corporation. An ineffective or nonexistent internal controls program will leave an enterprise vulnerable to the misappropriation of corporate assets. For example, the 1995 National Retail Security Survey reported that retailers lost $27 billion to a combination of employee and customer theft. A full 20 percent (about $5.4 billion) of this loss was due to administrative error. An effective loss prevention program, part of an overall corporate security program, should be maintained to address this issue. A loss prevention program, specifically designed to control the loss of physical inventory, includes measures such as cabling devices to secure equipment and inventory sensor tags that trigger an alarm when passing through a portal. One of four companies suffered financial losses, often exceeding $100,000 and sometimes $1 million, due to information security breaches, according to a recent Ernst & Young survey of top information systems executives.

Laxness in regard to due care can be costly in other ways as well. The Business Software Alliance (BSA) is running a campaign that encourages employees to call their 800-number and turn in their bosses for copyright infringement. A disgruntled former employee of an automobile manufacturer provided such a tip and the company ended up paying a $260,000 settlement to BSA for copyright abuse. In this instance, top management indicated that they were unaware of the infringement, and the company was still liable for the fine and had to agree to replace unlicensed software with legal software.

6 ELEMENTS OF AN EFFECTIVE PROGRAM

A key to demonstrating due care is the implementation of a comprehensive security program. This would include clearly defined responsibilities that are communicated to all employees. The cornerstone to this would be documented security policies and procedures, which include discussions on proprietary information, patents, and copyrights.

Access control measures must be implemented to protect information, financial, proprietary, intellectual, and physical assets of the corporation. Because information is present throughout the organization, these con-

trols would have to encompass more than just mainframe concerns. Information, wherever it is resident, will have to be addressed and protected. Access control to work stations, e-mail messages, electronically held files, printed documents, and even the trash will have to be addressed.

A comprehensive business continuity plan (BCP) is another integral element of a corporate security program. A BCP goes beyond the traditional data center disaster recovery plan and includes the entire campus facility. Preventative measures such as fire suppression, emergency response procedures, data backup requirements, and recovery procedures to expedite the speedy return of normal operations are all part of an effective BCP.

Monitoring compliance to established security policies and procedures is another measure in a comprehensive information protection program. Establishing auditing and monitoring procedures, including checklists of items to be scrutinized during a review, will facilitate this process and demonstrate an organization's intent to exercise due care as it conducts its business.

7 NEED TO CONTROL ALL "EMPLOYEES"

Contractors and consultants should receive information only if it is relevant to their assignment. There should be a general awareness among internal employees concerning this limitation on access. If contractors are working on long-term projects, diligence tends to grow lax. Nondisclosure agreements (confidentiality agreements) should be signed by all contractors upon hire and should be reviewed with them upon termination, as a reminder. If the contractor's project extends beyond one year, then this agreement should be reviewed at that time. Confidentiality agreements are suitable for internal employees as well.

The safeguarding of custom software is another important issue with regard to the use of contractors. Large corporations often employ contractors to develop custom software. It should be made clear, in the language of the purchase agreement, that the software is owned by the corporation. Contractors must not be allowed to leave the premises with the software. These issues must be documented in the contractual terms of agreement.

Information and systems should be classified according to their sensitivity and criticality. Proper procedures for handling classified information should be clearly defined, communicated, and made available to all employees.

8 NEED FOR INTERNAL CONTROLS

The organization's first line of defense is an effective information protection program. To meet this need, effective internal controls must be implemented. These controls include procedures for adequate separation of

duties for sensitive job functions or transactions and required vacation time or job rotation schedules. A surprising number of fraudulent occurrences are discovered when employees cannot report to work due to some unexpected event such as illness. In a recent case, a major financial institution uncovered a scheme that drained as much as $5 million through fraudulent wire-transfers. The breach was discovered only after a cashier, apparently one of the perpetrators, died suddenly.

Inadequate controls can lead to a poor return on stockholder investment, which can lead to stockholder anger, which can lead to charges of fiduciary negligence. As seen with some Fortune 100 companies recently, stockholders have become militant in their demands to see that the directors and officers of the corporation manage the assets in a prudent and responsible manner.

Since the early 1990s, there has been an awakening with regard to the need for an effective corporate program of information protection. The new direction is that the program must be a corporate one rather than one based in the information systems organization. Many organizations have required each business unit to establish an information protection entity and charge that person with responsibility of ensuring that all employees be made aware of their individual responsibilities. An information protection program is part of the cost of doing business in the next millennium.

To be effective, it is necessary to keep the information protection message visible to all employees. An effective awareness program examines the culture of an organization, the current level of compliance, and management expectations. The most effective way to ensure that a program will meet the organization's business objectives is to understand what causes security programs to falter.

9 WHY DOES SECURITY FAIL?

9.1 Uncontrolled or Inadequately Controlled Access

The ability to control access to systems, data, and information is a vital element of any information protection program. Many times, this first line of defense is breached and problems occur. The following are examples of how access control problems can affect an organization.

An employee working for a manufacturing facility in the Midwest was passed over for a promotion. Wanting to know who was better qualified, he decided to access the human resources system. Once into the system, he found that employees were listed by job classification bands and then rated numerically based on their last appraisal. He felt that this was some good information, so he printed it out and then made enough copies so that he could post them on bulletin boards, coffee machines, and in the caf-

eteria. The investigation turned up who was responsible for the postings and, in his exit interview, it was learned that he had gained access by using the Director of HR's password. The HR Director's password was still the default, new user password, the first four characters of his last name.

A number of years ago, a Canadian software development firm was at an architecture convention and was showing its new computer-aided design package, an "expert system" for designing building facades. The owner and program developer was at one station and his son at a second station. After finishing a demonstration, the son turned his back on the computer for a few seconds. When he returned, a diskette was missing. Because they were updating the writer driver information, the diskette contained the source code. The estimated value of the software package was between $5 and $10 million and represented 12 years of research and development.

In November 1988, Robert Morris, Jr., a graduate student in Computer Science at Cornell, wrote a self-replicating program called a worm and injected it into the Internet. The program was flawed and it began to replicate and re-infect machines at a much faster rate than he had anticipated. In 1988, there were almost 62,000 Internet host systems and it is estimated that Morris brought down about 10 percent of those systems. The estimated cost of dealing with the worm at each installation ranged from $200 to more than $53,000. Today there are nearly 20 million Internet host machines and a worm of the Morris magnitude could cause genuine havoc.

9.2 Vague or Inadequate Responsibilities

Backups have always been a sticking point in the information systems environment. With the movement toward distributed processing, the need for users doing and storing backups has increased. Often times, however, users are not informed as to what their responsibilities are. If backups of a work station are done at all, they are normally stored in the same area as the work station and the same diskettes are reused. A large engineering firm was converting to PCs and having employees move mainframe applications to the desktop. After about six months in the new processing environment, an office administrator called the Help Desk to request that her EXCEL spreadsheet be restored. The Help Desk directed her to the LAN administrator. The LAN administrator asked for her backup diskettes. She asked the LAN administrator about the backups that Operations normally used to restore her old mainframe applications. Six months worth of conversion and updates were lost. Rules were changed and the customer was not informed.

A construction firm in Atlanta had what could be considered a rather lax backup and storage policy for diskettes. It seems that one weekend, 50 diskettes disappeared from the offices. Of these 50 diskettes, 10 were consid-

ered to be "crucially important." These ten diskettes were so critical to the operation of the corporation, that if they were not found, the company faced the real possibility of going out of business. The company was in the process of taking out an ad in the Sunday paper; it would offer a reward, no questions asked. The ad never ran. The police found the diskettes. A maintenance employee had taken the diskettes home and was reformatting them so that his kids could play games on their new home computer. "People don't leave out important diskettes, do they?" was his defense. Just by sheer luck did this company avoid disaster.

A favorite group of people are drafting supervisors. They are a hard-working group and always seem to try to be in compliance with company policies. One supervisor had just attended a workshop on the new database package. Being the conscientious person that he was, he decided to create a database to use what he had just learned. This database contained employee names, social security numbers, home addresses and phone numbers, current salary levels, and most recent appraisal information. He then attended a session on confidential information and wanted to ensure that the database was properly protected. Because he shared the work station with the off-shift supervisors, he did not want to leave the database on the hard drive or a diskette in the shared desk. Being the careful man he was, he decided to hide the diskette under the desk and attached it there with magnets. Sometimes, people get carried away with their desire to secure things.

9.3 Inadequate Training of Personnel

The software police [Business Software Alliance (BSA) and Software Publishers Association (SPA)] are continuing their efforts to crack down on software piracy worldwide. In 1995, the SPA increased its lawsuits and audits by 23 percent (586 organizations) and netted $2.6 million in penalties. Six organizations reached settlements in excess of $100,000. Worldwide software piracy losses were estimated at $13.1 billion in 1995, an increase of 9 percent over 1994 estimated losses.

Both the BSA and SPA have 800-numbers that can be used for a number of reasons, including reporting possible copyright infringements. How do the software police find out about violations of copyright compliance? Initially, they obtained their information from employees contacting the vendor for support. The vendor normally asks for the contact's name, company name, and serial number. If they get different people using the same software, then an investigation would be started. Another way was that visitors, vendors, or contractors would observe the work habits of an organization and then turn them in for whatever reason. A third way was that disgruntled employees would turn in the company. Now, employees

concerned about copyright compliance are calling the 800-numbers and giving information about their organization's practices.

The computer virus problem is large and continues to grow. About 98 percent of all corporations and other large organizations have experienced computer virus infections first hand. As of 1996, about 90 percent of all organizations with more than 500 PCs experience a computer virus encounter or incident each month. The chance of experiencing a computer virus incident is about one chance per 100 PCs per month. The cleanup cost per PC per year is more than $250. For an organization with 1000 PCs or more, one can estimate virus-fighting costs by taking the total number of PCs and multiplying by $250.

A Fortune 100 company discovered the Hi virus at a large division that was heavily networked with nine file servers and 630 client PCs. The site was also connected to 64 other sites around the world. The virus entered the division on a program disk from a legitimate European business partner. The virus was found one day after introduction and, despite eradication efforts, the virus continued to infect the network for an entire month. The total cost of cleanup of the virus was $44,000 and did not include lost data.

With the advent of the information highway, many organizations have been faced with some form of abuse — whether it is an employee accessing improper sites or the spreading of incorrect information. The Chaos Merchants are known to be anti-commercial and anti-establishment hackers who steal the home page of Web sites and leave a trademark picture of a naked woman, as they did compromising Rodney Dangerfield's Web site. With more than 18 million people a day accessing Web sites, hackers such as these could cause real problems for any organization.

The Government Accounting Office (GAO) reports that hackers infiltrate Pentagon computers more than 160,000 times per year. These attacks are rarely detected and seldom investigated. The Pentagon itself reports that as many as 250,000 attempts may have been made to penetrate military computers in 1995, and that 65 percent (162,500) were successful.

An employee working for a media company in Philadelphia was using the company-provided Internet access an average of six hours per day to download pornography into his work station, repackage it, and then sell it at computer fairs.

The use of electronic-mail (e-mail) in business is spreading rapidly; and in many organizations, the e-mail system is now the place for office gossip and other conversations unrelated to work. Although some of the exchanged information on e-mail is personal or frivolous, the system also fre-

quently carries vital organization information. The "information mix" raises many moral and business issues that must be addressed.

In a recent *Detroit Free Press* article, two companies that were in litigation because of alleged discrimination lost their cases because of e-mail messages uncovered in the discovery process. In both instances, *private* communications between supervisors contained language that was used by the plaintiff's attorney to support his client's claims. In each case, the message could have been just an offhand remark made between two colleagues. These offhand remarks cost each company financially and public image-wise.

People do not use the same level of care when they are putting things into a computer. There is a false sense of privacy. When using the e-mail system, people tend to be more honest; it is where they are joking, and it is where they use their creativity. E-mail correspondence is as private as a postcard.

A Manhattan health company was using a new technology that allowed users to tape themselves with a tiny camera built into the monitor of their work station and send a moving image message through the system. A high-level executive decided to use the system one night from her hotel room. Sitting in front of her notebook in the privacy of her hotel room, she purred to the intended recipient, a fellow married colleague, "Hurry to the hotel and here's what you get tonight." With that she did what has been described as a "strip shimmy." Then, instead of sending the message out as private, she inadvertently used the public feature and sent the message to more than 400 employees.

All too often, employees fail to understand the need to protect classified information. When working through the courts to determine if information is in fact trade secret, the courts look for four keys:

1. that there was some cost to develop this product or process
2. that the product or process will provide some form of competitive advantage
3. that the product or process is not generally known
4. that the information is kept secret both externally and internally

Where most organizations fail is in the need to keep the information secret both externally and internally. Many employees fax sensitive information in clear text or discuss such information over cellular or wireless phones. When this behavior occurs, the information is no longer confidential, but becomes public domain.

9.4 Employee Exposure to Unnecessary Temptation

Many of the examples in this category fall under the heading of separation of duties or rotation of assignments. All too often, employees are able

to stay in a job assignment long enough to determine what would trigger an audit or review. One such individual was an analyst working for the federal government. This individual was responsible for reviewing expense reports and then submitting them directly to disbursement for printing. No one checked his work. In fact, no one questioned any of his activities until a mortgage processor was unable to make his assets match his earnings. This individual was purchasing a $350,000 home in the Washington, D.C. area (paying for almost all of it in cash), had a number of very expensive automobiles, country club memberships, original oil paintings, and was remarried with two children. He was able to afford all of this on a salary of $40,000 per year, paying $1,000 a month in child support.

It seems that he found out that many departments were not using all of their travel and expense monies. With what little was left over, it seemed a shame to turn it back to the government. So, he began to create expense reports to himself. Over an 18-month period, he wrote checks to the tune of $1.2 million. The federal government admits that if it had not been for the mortgage processor, they might never have uncovered this scheme.

The company e-mail system is often an avenue for abuse. An Air Force Master Sergeant was convicted of misuse of a government computer, distribution of obscene writing, communicating indecent language on sexual topics, and obstruction of justice for allegedly trying to delete his e-mail.

On many systems, it is easy to send an e-mail message that appears to come from someone other than the actual sender. At a university in New England, a student spoofed an e-mail message from the department secretary canceling an exam. Half the students did not attend. At a university in the Midwest, someone forged a letter of resignation from the Director of Housing to the Chancellor. A New England housewife discovered that a Chicago man was sending obscene messages in her name.

When it comes to the loss of company secrets, one of the most dangerous and difficult to spot is the trusted employee. The most likely candidates are employees who may be disgruntled, or have incurred large debts due to gambling habits, personnel circumstances, or drug use. According to *Insights*, 10 percent of workers are abusing drugs or alcohol on the job. Other reasons include involvement with labor/management disputes or entrepreneurial personalities. The typical computer criminal is a nontechnical user of the system or application who has been around long enough to figure out what would cause an audit.

An electrical supply company in Nebraska had an employee who was responsible for paying the invoices and for reconciling the company checking account. Her scheme was not high-tech; she would receive an invoice, write out the check for the proper amount but would enter a higher amount in the check register and then write out a check to herself for the differ-

ence. In the register for the second check, she would write *void.* When the bank statement came, she would destroy the check to herself and then balance out the account. In three years, she managed to take $450,000. She became remorseful and turned herself into the authorities.

Another area of employee temptation is the theft of notebook computers. A recent *Wall Street Journal* article indicated that over 200,000 notebook computers are reported stolen each year and less than 10 percent are ever recovered. The most significant of these losses was during Operation Desert Storm. A NATO officer had his laptop stolen from his car. The computer contained all of the command codes for the operation.

9.5 Inadequate Protection Against Disgruntled Employees

An employee working for a large manufacturing corporation had a unique solution to a password problem. One Monday morning, after incorrectly entering his password four times and having his access REVOKED, the employee called the Help Desk to inform them that his computer did not work. After verifying who he was, the Help Desk operator reset his password and told him to try again. The employee repeated his problem "My computer doesn't work." After vainly attempting to walk the employee through the process, the Help Desk operator decided to call for level 2 support and have them meet with the employee to determine the problem. After revoking his access, the employee went to his locker and got out a .38 Police Special and fired one round into the CRT. He was correct; his computer did not work any more.

Another employee was let go by a firm but was given a two-week notice. He was their LAN Administrator and felt that he was being unfairly treated during the corporate downsizing. To make things more lively after he left, he decided to put a 4MB cap on the System directory. Three months after he left, the office came to a halt until the problem could be found and corrected.

The Business Software Alliance (BSA) and Software Publishers Association (SPA) have installed telephone hotlines to get and supply information on copyright compliance. Last year, the BSA received 7,000 calls on its hotline; about half of them were employees who wanted to rat on companies that were using unlicensed software. Of the calls to complain, nearly 500 resulted in cases with recoveries totaling almost $4 million.

9.6 Passwords: Failing to Meet the Challenges of the 21st Century

The most cost-effective form of access control is still the use of reusable passwords. However, as long as there are employees using these confidential access codes, there are going to be problems. When doing an initial security review, looking for passwords is no more difficult than turning over a keyboard, opening an unlocked middle desk drawer, flipping to "P" in a Rolodex, or looking for a note posted to the CRT.

When Commonwealth Films, Inc., was shooting the video *Mum's The Word,* the director was setting a scene that had an employee's password taped to the side of the terminal. The technical advisor was concerned that what was being shown was outdated. The company where the video was being made had an extensive employee awareness program that stressed password security. Leaning into the cube across from the video setup, the technical advisor asked, "If you were going to post your password, where would you do it?" The woman pointed to a Post-It note on her work station and said, "Mine's right there." Her rationale was that people would need to know how to access the system in order to use her password.

The Internet has also experienced some incidents dealing with password sniffing. Password sniffer programs monitor the system's network interface port and collect log-in information, including passwords. The program is put into the system after the attacker is able to obtain privileged status on a target host system. This is done by exploiting any of a number of known attack methods. This can normally only happen when the host system has not been properly configured and administered to prevent unauthorized access.

A major problem for every organization is the current status of all individuals who have been granted access. Employees, contractors, vendors, suppliers, customers: all may have been granted access to the system over the years. The difficult part is having someone contact account administration with the same level of urgency when access is to be removed. An automotive company was receiving a monthly bill for $350,000 in usage and storage charges for 688 users of an outside engineering service. During a reorganization, the cost of the service came under question. Over half of the accounts had not been used in 18 months, and the remaining accounts lacked contact information. It took two months to sort out all of the account information, and the end result was a reduction of nearly 80 percent in monthly fees and user accounts.

9.7 Exposure of Sensitive Information in the Trash

Stealing people's garbage is easier than most people think, and it provides a wealth of information. Most trash bins are placed within easy public access and the good spy will always dip into it. All one has to do is go through the plastic garbage bags, checking envelopes and the like, to ascertain whose garbage it is. The garbage can then be removed to a safer place for more in-depth examination. This operation can be conducted on a regular basis with startling results. The Supreme Court has ruled that the Fourth Amendment does not prohibit the search of garbage placed outside the premises. It is legal! Many private investigators now openly advertise garbage retrieval services.

In a boast before friends, the owner of a bottled gas company in the Midwest told friends and colleagues that he "rooted around like a pig" in his competitor's Dumpster and was able to get their customer lists.

Your trash is valuable; encourage the destruction of all waste paper. There should be shredders purchased to meet the needs of all employees, both at work and away. A Chief Financial Officer for a Fortune 100 company contacted the security staff and informed them that his trash was picked up on Thursday evening. The security staff replied that he probably had a clean yard for the weekend. The CFO then added that the rest of the neighborhood had its trash picked up on Friday morning. His work habits were well known; he normally took home two transfer cases of papers to be worked on each evening. The company quickly purchased a shredder for home use.

Many of the teens who have gone on to the bigger and better things got their start by doing some Dumpster diving. Kevin Mitnick and his group were able to begin their work by accessing trash at a number of locations. There are many other such "celebrities" who have gotten into banks, telephone companies, utilities, and other companies. The *2600* magazine (the quarterly guide for the American hacker) ran an article on how to become a member of a contract cleaning crew and gain access to the companies from which one would like to gather information.

10 WE ARE OUR OWN WORST ENEMIES

For the most part, everyone will suffer self-inflicted information protection problems. An organization can establish a policy on copyright compliance, and then turn away when employees try to "save" the company money by "evaluating" software at the office. How can an organization have an effective information protection policy when federal copyright law is ignored? The employees follow the lead set by management. If the policies are established and followed, then the employees will also. However, if employees see that management selects the policies that they feel are worth following, then the employees will be able to rationalize why they do not have to follow certain policies.

Another manifestation of these self-inflicted problems is the introduction of computer viruses into the workplace. Many companies will spend large amounts of money to deploy an anti-virus package across the network, only to have the employees turn them off because the product slows down the boot-up process. Or the company encourages employees to work at home, but fails to provide either an anti-virus product for the home system or does not have virus-scanning stations around the office.

The biggest problem area is the sharing of passwords. Since at least 1974 (the founding of the computer security industry), password abuse has been the number one problem in computer and information security. Al-

though everyone in the industry is aware of the shortcomings of passwords, they are still the most cost-effective first lines of defense. Employees need to be reminded on a regular basis as to their responsibilities with regard to password protection: things like choosing the proper password, not leaving it lying around, and changing it on a regular basis.

11 RESOLVING THE DILEMMA

11.1 Attain Senior Management Approval and Support

Tie security issues to business objectives and the mission statement. Implementing controls to be in compliance with audit requirements is not the reason to do anything. In order to sell an effective program and get buy-in from Senior Management, it will be necessary to identify for them how this process will improve the organization's mission. Every organization has a bottom line; find out what that is and make sure security issues are always discussed in terms of how they will support that goal.

Stress the benefits of an effective program. Learn the needs of the different organizations and make certain that the sales pitch addresses their concerns. Be prepared to identify the costs of having an inadequate program: the loss of customer confidence, competitive advantage, and business.

11.2 Establish Enterprise-wide Policies

The key to any successful program is to have published policies. The policies must meet the needs and the culture of the enterprise. To be successful, the policies must meet the needs of the customers. Find out what concerns the user community has, and structure the policies to meet those needs. When developing policies, remember to keep things simple. The reading and comprehension level of most employees is that of a sixth grader. Keep the information short and to the point.

11.3 Implement an Enterprisewide Awareness Program

It is vitally necessary to keep the message in front of the employees. It is not sufficient to publish policies. Employees must be made aware of their existence, and this must be done on at least an annual basis. To complete this process, it is necessary to develop a method of getting the information to contract personnel. It may not be possible or desirable to include contract personnel in employee training. Because of the legal implications, contract personnel must be informed, but this must be done through contract negotiation with the contract house.

11.4 Monitor Compliance

Whenever a new security project is about to begin, the staff should take an evening or two and do a walk-about. Walk through the office environ-

ment and check to see the current level of compliance to some very minor security controls. During this initial review, check for five key elements:

1. offices are locked
2. desks and file cabinets are locked
3. work stations are secured
4. diskettes are secured
5. information is secured

These five controls will provide a good indication of the current level of concern over computer and information security. Normally, the noncompliance levels during this initial review are 90 percent and higher. Use this information to gage the information protection programs effectiveness by doing another walk-about after program roll-out.

Another key element in monitoring compliance is to establish a positive working relationship with the Audit Staff. If the only time one sees the Audit Staff is when they are in doing an audit, then one probably does not have a very good working relationship. Audit and Information Protection are working the same issues for a company. It would be very beneficial to work together; prepare a consolidated front in getting security controls accepted.

11.5 Make Compliance an Appraisal Item

Most employees are required to read and sign an annual Conflict of Interest Statement. Work with the Audit Staff to create an Employee Rights and Responsibilities for Information Access statement. This document could be included with the Conflict of Interest Statement and reviewed annually with the employees.

For senior level management, it may be necessary to create an Employment Agreement. This agreement is used by many companies for senior-level executives and certain employees that have access to highly confidential and proprietary information. Such agreements restrict employment with a competitor for a period of time after leaving the company. This is a very complicated legal document and requires research and coordination with the Human Resources staff and Legal.

12 SECURITY AS PART OF THE ENTERPRISE INFRASTRUCTURE

The objective of any information protection program is to provide acceptable business controls. The goal is to ensure that Senior Management meets its fiduciary responsibilities with regard to protecting the information assets of the enterprise. For many organizations, it comes as a surprise that information is an asset and is the property of the enterprise. As such, it requires that specific controls be in place to ensure that it is properly protected from unauthorized access, modification, destruction, and disclosure.

An effective program also enhances employee and workplace efficiencies. By putting a business-directed program in place, access to information will become structured. Employees will learn the process and will be able to gain the resources they need in a timely and efficient manner. Additionally, by having business-related controls in place, effort and resources are not wasted on protecting information that does not require it.

By restricting access to the logical and physical assets of an organization, the possibility of theft will be reduced. This does not mean that theft will be eliminated. There will always be some loss due to employee or outsider theft. The goal of an effective program is to reduce the theft to an acceptable level. There was a company in North Carolina that believed that its employees were stealing some company products. This was a chicken processing plant, and management believed that employees were stealing chickens. To prevent the employees from stealing, management decided to lock all but the main exit. This plant had a fire, and when the employees attempted to leave through the fire exits, they found out that the exits had been padlocked. Over 25 employees died because of this decision. Remember that the goal of any protection program is to reduce risk to an acceptable level. Putting employee lives in jeopardy is not an acceptable level of control.

13 FINAL THOUGHTS

Just as steps have been taken to protect employees, it is now necessary to involve the employees in protecting the information assets. Information must be protected from unauthorized access, modification, destruction, and disclosure. If the enterprise fails to do this, there will be a loss of customer confidence, competitive advantage and, ultimately, jobs. Information protection is not rocket science, nor nuclear physics — it is taking basic business principles and applying them to the information assets of the enterprise.

The message of information protection must be first published and then presented to the employees through an effective awareness program. This program must include regular reminders as to the need to protect enterprise assets and who is responsible for protecting those assets.

Once the program is in effect, employees at all levels of the organization will learn that they are responsible for protecting the information and computer resources of the enterprise.

14 SUMMARY

To assist in selling the information security program, it is necessary to address the needs of:

- Senior Management
- Line Supervisors
- Employees

To support your activities, it might be best to investigate other organizations and review their security programs. Questions you may want answered include:

- Did they develop their own policies and procedures or was this done by an outside consultant?
- If a consultant was used, was the organization pleased with the timing and results?
- What resources (employees, time, budget, etc.) were required to develop and maintain the program?

Chapter 12
References

Bryson, Lisa. "Protect Your Boss and Your Job: Due Care in Information Security." *Computer Security Alert.* Number 146, May, 1995, pp. 4 and 8.

d'Agenais, J., and J. Carruthers. *Creating Effective Manuals.* Cincinnati, OH: South-Western Publishing Co., 1985.

DeMaio, H. *Information Protection and Other Unnatural Acts.* New York, NY: AMACOM, 1992.

Fine, N. "The Economic Espionage Act: Turning Fear into Compliance." *Competitive Intelligence Review,* Volume 8, Number 3, Fall 1997.

Fites, P., and M. Kratz. *Information Systems Security: A Practitioner's Reference.* New York: Van Nostrand, 1993.

Guttman, B., and E. Roback. *An Introduction to Computer Security: The NIST Handbook.* Gaithersburg, MD: U.S. Department of Commerce, 1995.

Jordan, K. "Ethics and Compliance Programs: Keeping Your Boss out of Jail and Your Company off of the Front Pages." *Betterley's Risk Management,* April, 1998.

Krause, M., and H. Tipton (eds.). *Handbook of Information Security Management.* New York: Auerbach, 1998.

Lincoln, J.A. "EPA's Policy on Incentives for Self-Policing, Federal Sentencing Guidelines and Other Carrots and Sticks." *Forum for Best Management Practices,* 1997.

Navran, F. "A Decision Maker's Guide to the Federal Sentencing Guidelines for Ethics Violations." *Navran Associates' Newsletter.* March 1996.

Palmer, I., and G. Potter. *Computer Security Risk Management.* New York: Van Nostrand Reinhold, 1989.

Peltier, T. *Policies and Procedures for Data Security.* San Francisco: Miller Freeman Inc., 1991.

Peltier, T. "How to Develop a Mission Statement." *Computer Security Journal,* Volume X, Number 2, 1994, pp. 5–16.

Tomasko, R. *Rethinking the Corporation: The Architecture of Change.* New York: AMACOM, 1993.

Chapter 13
Introduction to Information Security

1 DEFINITION OF INFORMATION

Corporate information is defined as any information relating to company business that becomes known to an employee or contractor during the course of employment. Broadly, corporate information is that information used by the company in its business and is the result of some effort, expense, or investment that provides the company with a competitive advantage, and that the company wishes to protect from disclosure to third parties.

2 WHAT IS INFORMATION SECURITY?

Information Security is the prevention of, and recovery from, unauthorized or undesirable destruction, modification, disclosure, or use of information and information resources, whether accidental or intentional.

3 WHY DO WE NEED TO PROTECT INFORMATION?

Publicly held companies are required to keep accurate records and to maintain internal controls to safeguard corporate assets against unauthorized use or disposition. In addition to the more traditional list of assets such as plant, land, equipment, money, and people, the list of corporate assets also includes information used to support the business. A company's physical assets are protected because lost or damaged assets damage the company's chances of success. In the same manner, protecting the company's information assets enhance its chance of success. Prudent asset security yields improved value for stockholders, better competitive position in the industry, and improved customer service. The following discussions provide some additional basis for safeguarding information.

3.1 Corporate Policies — Information Management (Reference Chapter 7)

Management recognizes the increasing value of information to the efficient and effective operation of the company. Information has not only be-

come critical to company success, but strategic to its long-term survival. Recognizing these facts, the corporate policy on information management was established in June 1991.

This policy identifies information as company property and a corporate asset. This includes all information, regardless of the medium on which it is transmitted or stored. Specifically, the policy includes information that is typed, handwritten, printed, filmed, or electronically generated or stored. Voice-mail is also corporate information. Additionally, the policy charges:

- organization management with the responsibility to [create and] retain information necessary to conduct company business
- managers with the responsibility to develop and administer Information Security programs that appropriately classify and protect corporate information
- employees with the responsibility to protect corporate information from unauthorized access, modification, duplication, destruction, or disclosure
- information providers with the responsibility to authorize access to those with a genuine business need

The policy also establishes that all information must fall into one of three information classifications (Confidential, Internal Use, or Public) and that each employee can have one or more specific roles (owner, custodian, or user) to play in protecting information. Employee responsibilities and information classification guidelines are described in broader detail in Chapters 15 and 16 of this guide.

3.2 Corporate Policies — Security

Policy requires managers or plant superintendents to "develop an emergency preparedness plan to address resumption of business operations and security of employees and property." Thus, management is charged with the responsibility not only to protect the information asset's confidentiality, integrity, and availability, but also to ensure that the organization's business function can be maintained (or minimally, quickly recovered) in the event of a disaster.

3.3 Corporate Policies — Standards of Conduct

Policy charges employees with the responsibility to abide by applicable laws, regulations, and standards of professional conduct. This includes a responsibility to avoid conflicts of interest and actions that have the appearance of being unethical. Employees are expected to safeguard information against theft and unauthorized use, and to observe copyright law. This includes not only corporate information, but also the information of employees, customers, and suppliers.

3.4 Corporate Policies — Conflict of Interest

Employees entrusted with confidential or proprietary information shall restrict access and use to authorized individuals inside and outside the company who have a need to know this information for conducting the Company business.

No employee who has material nonpublic ("insider") information relating to the company can buy or sell securities (stocks and bonds) of the Company, either directly or indirectly. Furthermore, employees cannot engage in other actions to take personal advantage of that information or pass it on to others. Even the appearance of an improper transaction must be avoided to preserve the company's reputation for adhering to the highest standards of conduct.

3.5 Foreign Corrupt Practices Act (FCPA)

The FCPA, which was signed into law in December 1977, made all managers and directors personally liable for the security of corporate assets under their control. The Act requires companies to maintain books, records, and accounts that reflect in reasonable detail the disposition of corporate assets and to implement a system of internal accounting controls. These controls must meet four standards:

1. All transactions affecting corporate information must be authorized by company management.
2. Transactions affecting corporate information must be recorded as necessary to allow preparation of financial statements that conform with generally accepted accounting principles and to maintain a proper accountability of corporate assets.
3. Access to information is permitted only in accordance with management's general or specific authorization.
4. Audit trails must be developed to allow review of and access to corporate information. These reviews are to be undertaken at reasonable intervals. Appropriate action should be taken in the event of any irregularities.

3.6 Federal Copyright Law

It is illegal to make or distribute copies of copyrighted material without authorization from the author or distributor.

3.7 Federal Antitrust Laws

The sharing of one competitor's sensitive information with another competitor can lead to criminal (felony) and civil violations of the federal antitrust laws resulting in fines up to $1 million dollars and triple civil damages. Examples of this type of information are future product plans, mar-

keting strategies, innovative manufacturing processes, and other strategic or sensitive information that is not intended to be shared.

Based on the language of the antitrust law, every company is required to protect competitive information, keep processes secret from competitors, and resist efforts to obtain another company's information.

4 WHAT INFORMATION SHOULD BE PROTECTED?

All information is *not* created equal. Some information may be considered as having higher value if it supports critical business functions, or must be retained due to corporate, legal, or regulatory requirements. To determine which information should be protected and to what degree, each organizational unit should perform an information risk assessment, which includes identifying:

- the business value of the information asset
- possible threats to the information asset
- which threats are most likely to occur
- the impact on the business should the threat be realized

With this data, the organizational unit can apply cost-effective security measures to the most important information that is at the greatest risk. An important element to remember is that the cost of protecting information should not exceed the value of the information to the company. Additional information can be found in Chapter 5. The Information Security group can be contacted for assistance in performing risk assessments.

Chapter 14
Fundamentals of Information Security

1 INTRODUCTION

Information Security is the prevention of, and recovery from, unauthorized or undesirable destruction, modification, disclosure, or use of information and information resources, whether accidental or intentional. A more positive definition is the preservation of the *availability*, *integrity*, and *confidentiality* of information and information resources. The following sections discuss each element.

2 INFORMATION AVAILABILITY (BUSINESS CONTINUITY)

What is information availability? Information is said to be available when employees who are authorized access, and whose jobs require access, to the information can do so in a cost-effective manner that does not jeopardize the value of the information. Information must be consistently available to conduct business. Business continuity planning includes provisions for assuring the availability of the key resources (information, people, physical assets, tools, etc.) necessary to support the business function.

Corporate Policy:	Information **owners** are responsible to assure the accessibility and availability of information and business functions critical to the effective operation of the company. (From: Company Policy on Security)
Recommended Standard:	Organization management is responsible for: • identifying information, applications, processes, and systems required to support critical business processes and functions • assessing the cost to the company of a business disruption • determining the duration that a business disruption could be tolerated

- determining resource requirements for recovery and resumption of business
- determining disruption avoidance procedures and costs
- defining alternate processing methods to sustain business operations while normal processing is being restored
- restoring information required by the business process
- verifying successful recovery

Recommended Standard: Organizational unit management shall maintain a business continuity plan that allows critical business functions to continue in the event that primary business facilities or resources are not available. The following are minimum requirements for business continuity planning.

- A business continuity coordinator should be designated for each organization.
- The organizational unit should review and approve the initial business continuity plan and subsequent annual updates.
- The information **owner** should determine what information is to be backed up and the frequency of backup. This activity is to be coordinated with the **custodian.**
- The organizational unit head is responsible for ensuring that information deemed critical is backed up and stored in a secure location away from the primary usage site.
- All critical hardcopy documents should be identified and copies stored off-site.
- The organizational unit head should review the plans of the **custodian** to ensure that the unit's needs are met.
- All continuity plans should be reviewed and updated at least semi-annually.
- All continuity plans should be tested at least annually.

Discussion: Information, which is considered to be an inherent part of the company's business process and without which operations would be curtailed or otherwise severely impacted, should be identified by the **owner** as *critical.* For critical information and business functions, the information **owner** must consider such key elements as recovery of resources necessary to continue the business function or availability of alternate resources. Consideration should be given to human resources, physical facilities, equipment, information, finances, and forms necessary to

perform critical functions. If the function depends on a computer system, additional consideration should be given to processing hardware, system software, and application programs. For those programs, applications and systems identified as *critical*, the **owner** must decide how long the organizational unit can function without access to these resources.

Each organizational unit head should conduct a business impact analysis. This process identifies the information created or used within the organization and what the consequences would be to the company's business process if the information were altered or destroyed, or that the method used to process the information was not available.

One of the most important things that can be done to protect the company's business process is to establish a living, working, tested business continuity plan. A business continuity plan is a plan for keeping information and computer systems available in the event of an emergency. Such a plan may make the difference between having just a "problem" or having a business-threatening catastrophe.

3 INFORMATION INTEGRITY

Information integrity is defined as the assurance that the information used in making business decisions is created and maintained with appropriate controls to ensure that the information is correct, auditable, and reproducible.

As each organization develops its own policy on information integrity, it must consider the practical day-to-day operation of the business process, the classification level of the information, and the risk to the company if the information is improperly altered or destroyed.

There are several techniques that can be used to increase confidence that information has integrity. Batch totals and record totals are examples of techniques that help ensure that the information "adds up." Other techniques can be used to help ensure against fraud. There are two basic principles that should be considered: separation of duties and rotation of assignments.

3.1 Separation of Duties

Recommended Policy: No single individual should have complete control of a business process or transaction from inception to completion.

Discussion: This control principle limits error, opportunity, and temptation. Separation of duties can be defined as segregating incompatible functions (giving these duties to two or more people). The activities of a process are split among several people. Mistakes made by one person tend to be caught by the next person in the chain, thereby increasing information integrity. Unauthorized activities will be limited since no one person can complete a process without the knowledge of another.

3.2 Rotation of Assignments

Recommended Policy: Different individuals should be rotated periodically to various critical tasks involving the business process or transaction to ensure business process integrity.

Discussion: There are always some assignments that can cause the organization to be at risk unless proper controls are in place. To ensure written task procedures are being followed, as well as provide manpower backup on critical activities, employees should be assigned to different tasks at regular intervals.

Some maintain that rotation reduces job efficiency. However, it has been proven that an employee's interest declines over time when doing the same job for an extended period of time. Additionally, employees sometimes develop shortcuts when they have been in a job too long. By rotating assignments on a regular basis, the organization can compare how the task was being done and where changes should be made.

In general, *separation of duties* is designed to ensure that unauthorized practices require the collusion of several individuals. The *rotation of assignments* is a complementary principle that removes one of the colluding parties from the task, thus exposing the other(s) to detection.

4 INFORMATION CONFIDENTIALITY

In order for the maximum information value to be realized, the information **owner** is obligated to make information accessible to the widest possible company audience having a demonstrated business need. That is, the **owner** is responsible to maximize the value of information by sharing it with others while assuring its integrity and confidentiality. Confidentiality

means that the information should only be disclosed to a select group, either because of its *sensitivity* or its *technical nature.*

For example, most would agree that personnel and medical records should not be widely available because this would provide little additional value and represents a serious invasion of employee privacy. To protect employees and the company, this type of information should be highly restricted. Additionally, technical information, or premature, unauthorized information on company stocks (future dividends, splits, etc.), would be difficult for most to interpret correctly. To protect against misuse, misinterpretation, and resultant misinformed business decisions, disclosure of this type of information should also be restricted, either temporarily or permanently.

4.1 Authority to Disclose

Corporate Policy: Information required to perform company business should not be disclosed to others except with the authorization of the information **owner**. (From: Company Policy on Conflict of Interest)

Recommended Standard: **User** access to information does not imply or confer authority to act as spokesperson for the company concerning such information or to discuss such information with others.

User access to information does not imply or confer authority to allow access to others either internally or external to the company.

Discussion: While an open climate of information sharing is desirable to satisfy both the needs of the business and employees, there is a clear need to safeguard corporate information. Access to corporate information should be based on a clear business need. Corporate information is not to be discussed with family or friends, as such discussion can lead to unauthorized third-party disclosure. Discussion of corporate information could result in a significant disclosure that could damage the business interest of the company.

An official company announcement relieves an employee of his or her responsibility to maintain secrecy to the extent of the information included in the announcement. Speculative press reports provide no excuse for comment on or disclosure of corporate information. Substantial

competitive advantage can be sacrificed through untimely disclosures and could result in a loss of customer confidence or business.

4.2 Need-to-Know

Corporate Policy: Access authority should be granted to those with a business "need-to-know." (From: Company Policy on Information Management)

Discussion: All employees and contractors must be granted sufficient access to perform their assigned duties. For some **Internal Use** information, group or department access may be reasonable. However, at the classification level of **Confidential**, access must be granted on an individual basis. The key to proper control is individual accountability.

Each employee with access to corporate information should be assigned a specific set of functions, privileges, restrictions, and capabilities. The overriding principle of *need-to-know* should govern this process. Under this principle, employees or **users** are assigned only the level of access required to perform their specific job function.

Chapter 15
Employee Responsibilities

1 INTRODUCTION

Although company shareholders are the ultimate **owners** of all information created and utilized in the course of company business, all company and contract personnel are responsible for maintaining the confidentiality, integrity, and availability of corporate information to facilitate its effective and efficient use for company business. (Although not employees of the company, reference below to "employee" is intended to apply to company employees as well as contract personnel performing company business.)

Three responsibility classifications have been defined to assist employees in understanding their roles and responsibilities when using corporate information. Depending on the specific information being accessed, the employee may fall into more than one category. For example, an employee with a desktop work station becomes the **owner, custodian,** and **user.** This individual is managing a data processing center and is responsible for it.

The definitions and responsibilities described below represent the minimum level of detail necessary for all organizations across the company. Each organization may decide that additional detail is necessary to adequately implement an Information Security Program within their organization.

Corporate Policy: Individuals and management responsible for creating, administering, or using corporate information are identified as information **owner, custodian** or **user.** (From: Company Policy on Information Management)

2 OWNER

Definition: The information **owner** is the person who creates the information or is the primary **user** of the information. The information **owner** is assigned the responsibility to exer-

cise the company's ownership rights to manage the corporate information resource.

Recommended Standard:

Minimally, the information **owner** is responsible for:

- judging the value of the information and assigning the proper information classification, including a periodic review of this information to determine if the information classification should be changed
- assessing and defining appropriate controls to ensure that information created is correct, auditable, and reproducible (i.e., integrity)
- specifying access and control requirements that assure confidentiality, integrity, and availability, and communicating these requirements to the information **custodian** and **users**
- encouraging access by company personnel who have a business need and could benefit from the information, and preventing access by individuals without a business need-to-know
- assessing the risk of loss of information confidentiality, integrity, and availability and assuring that adequate controls are in place to mitigate that risk
- performing periodic reviews of access and control requirements to ensure that information access and control requirements remain appropriate and are functioning adequately
- ensuring that a disaster recovery plan is available

Discussion:

The information **owner** is usually the creator of the information (or someone assigned by the organizational unit head of the area that created the information) and therefore, on behalf of the company, is assigned the responsibility to maximize its value to the company while maintaining confidentiality, integrity, and availability. The responsibilities of the information **owner** are continuous and, as such, require periodic (possibly annual) review to ensure that information is properly safeguarded.

The information **owner** may delegate these responsibilities to another individual (for example, director to employeee), although not normally to someone outside the organizational unit. However, the **owner** may also be a committee of several primary **users** who have agreed to share the ownership responsibility.

3 CUSTODIAN

Definition: The information **custodian** is responsible for protecting the information resource in accordance with the **owner**'s specific directions.

Recommended Standard: At a minimum, the **custodian** is responsible for:

- providing physical security for equipment, information storage, backup, and recovery
- providing a secure processing environment that can adequately protect the integrity, confidentiality, and availability of information
- administering access to information as authorized by the information **owner**
- implementing procedural safeguards and cost-effective controls

Discussion: The information **custodian** is responsible for the safe storage and recovery of *information.* The information **custodian** is *not* generally responsible for the recovery of the **owner**'s organization that creates this information. A corporate policy on business continuity planning should charge managers and plant superintendents with the responsibility of developing an appropriate plan to recover their business operations in the event of a business interruption.

4 USER

Definition: The **user** is the individual, or organization, who has been authorized access to the information asset by the **owner**.

Recommended Standard: At a minimum, **users** are responsible for:

- using the information only for the purpose intended
- maintaining the integrity, confidentiality, and availability of information accessed consistent with the **owner**'s expectations while under the **user**'s control

Discussion: Being granted access to information does not imply or confer authority to grant other **users** access to that information. The availability of **confidential** information must be limited. Therefore, if granted access to **confidential** information, **users** should seek the approval of the information **owner** before allowing any other person access. However, for information classified as **public**, the information **owner** is assumed to have granted full disclosure authority to all **users** (unless specifically and explicitly limited).

Chapter 16
Information Classification

1 INTRODUCTION

Information, wherever it is handled or stored (e.g., in computers, file cabinets, desktops, fax machines, voice-mail) needs to be protected from unauthorized access, modification, disclosure, and destruction. All information is **not** created equal. Consequently, segmentation or classification of information into categories is necessary to help identify a framework for evaluating the information's relative value and the appropriate controls required to preserve its value to the company.

Three basic classifications of information have been established. Organizations can define additional subclassifications as necessary to complete their framework for evaluating and preserving information under their control.

When information does require security, the security must be consistent. Often, strict access controls are applied to data stored in the mainframe computers but not applied to office work stations. Whether in a mainframe, client/server, work station, file cabinet, desk drawer, waste basket, or in the mail, information should be subject to appropriate and consistent security.

The definitions and responsibilities described below represent the minimum level of detail necessary for all organizations across the company. Each organization may decide that additional detail is necessary to adequately implement information classification within their organization.

Corporate Policy: All information must be classified by the **owner** into one of three classifications: **Confidential, Internal Use,** or **Public.** (From: Company Policy on Information Management)

1.1 Confidential

Definition: Information that, if disclosed, could:

- violate the privacy of individuals,
- reduce the company's competitive advantage, or
- cause damage to the company.

Examples: Some examples of **Confidential** information are:

- personnel records (including name, address, phone number, salary, performance rating, social security number, date of birth, marital status, career path, number of dependents, etc.)
- customer information (including name, address, phone number, energy consumption, credit history, social security number, etc.)
- shareholder information (including name, address, phone number, number of shares held, social security number, etc.)
- vendor information (name, address, product pricing specific to the company, etc.)
- health insurance records (including medical, prescription, and psychological records)
- specific operating plans, marketing plans, or strategies
- consolidated revenue, cost, profit, or other financial results that are not public record
- descriptions of unique parts or materials, technology intent statements, or new technologies and research that are not public record,
- specific business strategies and directions
- major changes in the company's management structure
- information that requires special skill or training to interpret and employ correctly, such as design or specification files

If any of these items can be found freely and openly in public records, the company's obligation to protect from disclosure is waived.

Discussion: Information should be protected according to its sensitivity, criticality, and value. Most often, people think of issues of sensitivity when the word "confidential" is used. However, sensitivity is only one possible element in this classification. Most understand the need to protect the individual's right to privacy and even the need to keep secret (at least for awhile) plans that are being contemplated concerning the future of the company or an organization. Premature disclosure of such plans (especially when they are not firm) could reduce the effectiveness of the plan, removing the element of surprise (necessary in a competitive environment for new product

or service offerings) or damaging the company's reputation (in the case of a preliminary "what if" rate case study, for example).

Some information, while not sensitive, is technical in nature and should not be available even to those with a need to know without expert interpretation by the information **owner.** The nature of the information requires special skill or training for correct interpretation. Access to this information without expert interpretation would likely cause the information to be misinterpreted and decisions that could damage the company's opportunity to operate efficiently and effectively.

Access to this information by individuals not conducting company business is not authorized (except as required by law); access is highly restricted.

It is estimated that approximately 5 to 15 percent of corporate information should be classified as **Confidential.** Due to the nature of their work, some organizations will have more confidential information than others (e.g., those organizations dealing with personnel and legal matters). Information regarded as sensitive should be labeled as **Confidential.**

1.2 Internal Use

Definition: Classify information as **Internal Use** when the information is intended for use by employees when conducting company business.

Examples: Some examples of **Internal Use** information are:

- operational business information and reports
- noncompany information that is subject to a nondisclosure agreement with another company
- company phone book
- corporate policies, standards, and procedures
- internal company announcements

Discussion: This classification represents information that is used in the daily operation of the business and generally would not include planning or strategy development activities. Any information that cannot be classified as **Confidential** or **Public** is classified as **Internal Use.** Normally, **Internal Use** information is not labeled as such.

It is estimated that 70 to 90 percent of corporate information can be classified as **Internal Use.** However, organizations such as customer accounting, legal, and personnel departments can be expected to have a larger percentage of **Confidential** information.

Access to this information by individuals not conducting company business is not authorized (except as required by law); access by individuals conducting company business is generally open for inquiry but highly restricted for update.

1.3 Public

Definition: Classify information as **Public** if the information has been made available for public distribution through authorized company channels. **Public** information is not sensitive in context or content, and requires no special security.

Examples: The following are examples of **Public** information.

- corporate annual report
- information specifically generated for public consumption, such as public service bulletins, marketing brochures, and advertisements

Discussion: Generally, information that is readily available from the public media or is a matter of public record is classified as **Public.** Information should *not* be classified as **Public** merely because the information is outdated or appears to have no opportunity to damage the company. Information in this classification should be limited to that required by law or regulation and that which is specifically intended for public consumption. To allow other information to be viewed by the public would serve only to provide a potential advantage to competitors and provide the media with the opportunity to shed an unfavorable shadow on the company's reputation. It is estimated that 5 to 15 percent of corporate information can be classified as **Public.** Inquiry access to this information by company and noncompany personnel is authorized. Update access to this information is generally restricted by the information **owner.** Normally, **Public** information is not labeled as such.

2 CLASSIFICATION PROCESS

Recommended Policy: The **owner** is responsible for classifying information upon creation.

Discussion: Upon creation of the information (whether in a computer, memo in a file cabinet, message in an office automation tool, voice communication, etc.), the creator of that information (generally the information **owner**) is responsible for immediate classification. This immediate classification assists any recipient of the information to appropriately safeguard its value to the company against unauthorized disclosure, loss of availability, and loss of integrity.

Information's value to the company is heavily influenced by the extent to which its integrity is maintained and is available to those with a business need. That is, if the information is not correct or not available to those that need it, it has no value. The information **owner** is responsible to take particular care to assure the integrity of the information for which he or she is responsible and to actively encourage its accessibility by those who can use the information effectively.

The information **owner** must be careful not to over-classify information created. Over-classification might slow down the business process due to the extra precautions required for secure handling and storage. Information that is over-classified will soon cause employees to disregard the classification system, rendering organization Information Security programs ineffective.

3 RECLASSIFICATION

Recommended Policy: The **owner** should review the classification of information at least annually for possible reclassification.

Discussion: The sensitivity of most classified information decreases over time. **Confidential** information may become **Internal Use,** and **Internal Use** may eventually become **Public.** Because **Confidential** information often has a more restricted audience than **Internal Use** information, it is important that information be properly classified to give the widest and most appropriate audience possible. By maintaining an appropriate classification, the information will provide the maximum value to the company.

If the information **owner** knows the date that information should be reclassified, he or she might label it with "**Con-**

fidential until (date)." Unless specifically identified otherwise, declassification of **Confidential** information is automatically reclassified as **Internal Use.**

Declassification can also be tied to a public statement, as in the quarterly earnings reports. Prior to the announcement of quarterly earnings, the information is classified as **Confidential.** Once the announcement is made, however, the information can be reclassified as **Public.**

Chapter 17
Information Handling

1 INTRODUCTION

The following chapter sections identify standards and guidelines to help safeguard information during its useful life.

2 INFORMATION LABELING

Recommended Standard: All **Confidential** information must be clearly labeled with the word "**Confidential**." Any information not specifically labeled should be treated as **Internal Use**.

Recommended Procedure: All **Confidential** information is to be marked as follows:

- The name of the **owner** and the date of preparation are to appear on the face of the document.
- The document or any reproduction is to be stamped or marked **Confidential** at the top of the outside cover (if applicable) or on the title page.

Discussion: Proper classification by physical marking, notation, or other means serves to alert the holder the degree of security required for that information. It is *highly* recommended that all organizations employ the standard and procedure listed above. Only through this consistency across organizations can information shared across organizations be protected in accordance with the expectations of the **owner**.

Only **Confidential** information requires labeling. **Public** information should be labeled to identify its intended audience; but, if not labeled, there is little damage to the company beyond lost opportunity to communicate with the public. Information not labeled should be protected as **Internal Use**.

3 INFORMATION USE AND DUPLICATION

Recommended Standard: Information for which access has been authorized may only be used for purposes identified to and authorized by the information **owner**.

Discussion: When the information **owner** provides access to information, it is authorized on the basis of the requester's established business need. Access to information is approved for a stated purpose and does not imply that the requester has unrestricted use or authority to use for other purposes. For example, by virtue of being granted access to information, the requester does not have the automatic authority to duplicate or distribute this information to others.

Sometimes the authorization given by the information **owner** to the **user** needs to be formal and written. In other cases, verbal authorization or a clear understanding between the information **owner** and **user** is sufficient. It is the responsibility of the information **owner** to determine the level of formality required. Often there is the understanding that the information provided will be analyzed, summarized, and input into some process of the requester for distribution to others. The essential point is that there be a clear understanding between **owner** and **user**.

4 INFORMATION STORAGE

Corporate Policy: Organizations shall retain records in the most economical and practical method and location, and shall destroy or relocate them to more economical storage when appropriate. (From: Corporate Policy on Information Management)

Recommended Standard: Information must be stored in a manner consistent with its classification as follows:

- When not in use, information is to be appropriately stored.
- **Confidential** information is to be stored and maintained only where it can be verified that access can be adequately controlled.

Discussion: Information, particularly **Confidential** information, must be safeguarded not only while in use but also when

stored to protect against unauthorized access, modification, or disclosure. This may mean that paper-based information may need to be stored in locked cabinets or desks while not in use. For computer-based information, this may mean physically locking up the computer while not attended by an authorized individual or installing an access control software package to protect against unauthorized access.

5 INFORMATION DISPOSAL

Corporate Policy: Organizations shall retain records in the most economical and practical method and location, and shall destroy or relocate them to more economical storage when appropriate. (From: Corporate Policy on Information Management)

Recommended Standard: Information must be appropriately destroyed in accordance with the organization's records retention schedule.

Information no longer of value to the company should be destroyed.
Confidential information must be destroyed beyond ability to recognize and recover.

Discussion: When the information no longer has value to the **user**, his or her copy of the information should be destroyed. When the information no longer has value to the company, the information **owner** is responsible for disposal of the information originals. For **Internal Use** information, this might mean simply throwing the report in the trash or deleting the file from the computer.

For **Confidential** information, however, additional care is necessary to ensure that the discarded information cannot be recognized or recovered by anyone. For example, shredding reports and writing over a computer file (just deleting it does not prevent recovery) are effective against recovery. **Owners** and **users** also need to ensure that all data backups of the information are also destroyed beyond recovery.

Chapter 18
Tools of Information Security

1 INTRODUCTION

Information **owners** are assigned the responsibility to manage the confidentiality (disclosure), integrity, and availability of information they create or manage. For information processed in electronic media (such as computers, voice-mail, and fax), the providers of these services should have tools available for **owners** to utilize in fulfilling this function. For nonelectronic media (such as paper-based forms, memos, reports, etc.), the information **owner** is responsible to implement, or arrange to have others implement, appropriate controls to ensure acceptable information security.

There are four key control areas for the information **owner** to consider when safeguarding information: **Access Authorization, Access Control, Backup/Recovery,** and **Information Security Awareness**.

2 ACCESS AUTHORIZATION

Recommended Policy:	The information **owner** is responsible to define access authorization.
Recommended Standard:	It is the responsibility of the information **owner** to identify information assets created or managed, how they are to be protected, who is permitted access, and under what conditions.
Discussion:	For information to have value, it needs to be available and have integrity. For information to have maximum value, it needs to be accessible to those who need it and, conversely, inaccessible to those without a business need. Additionally, to maintain its value, this accessibility needs to be tailored to the **user** to provide only the level of access required to perform his or her job. That is, most need only to reference or read the information, while se-

lect others, who share in the responsibility to keep the information up to date, may need to modify it. Properly tailored access authorization will help preserve the information's value.

3 ACCESS CONTROL

Recommended Policy: Implementation of **owner**-designated access control authorization is the responsibility of the information **custodian**.

Recommended Standard: Each **user** should have an identification (userid) within the company's computing system and network environment to authenticate the **user**'s identity; and each identification should be unique, representing one and only one **user**. This identification is normally classified as **Internal Use**.

Recommended Standard: (The following user identification format standard for computer-based applications and telecommunication systems is maintained by the Information Systems Organization.) The **user** identification (userid) should be in the format X9999 for employees and C9999 for contract employees. For noncomputer-based activities, a similar individual identification scheme may be appropriate.

Recommended Standard: For computer-based systems, each **user** should have a userid that carries a **confidential** password to authenticate his or her identity. These passwords should:

- be kept **confidentia**l and not shared
- not be displayed or stored in readable text
- changed at least every 90 days
- be a minimum of five characters in length

For noncomputer-based systems, appropriate procedures should be implemented that will maintain the integrity of the **user** authentication process.

Discussion: The first way in which a system provides security of corporate assets (whether computer-based or manual) is by permitting access to only those employees with an approved business need. This process is accomplished by identification and authorization.

Identification is the way an employee tells the system (e.g., computer, voice-mail, electronic messaging, etc.)

who he or she is. This is accomplished by establishing a unique **user** identification (userid) code.

Authentication is the way a **users** prove to the system that they are who they say they are. This authentication element is known as a password and represents a secure and secret dialogue between the **user** and the system. Coupled with the userid, these two elements allow an authorized **user** access to the various computer systems and information. Because the password opens access to applications and information that a specific individual has been approved for, the password should be:

- kept secret (do not share passwords with others)
- difficult for others to associate with you (e.g., no names of spouses, children, hobbies, name variations, home address, etc.)
- combination of numbers and letters that do not represent a pattern (e.g., ABCD1234 and AAAA1111 are bad passwords)

This process of identification and authentication has been developed to ensure individual accountability. By ensuring that individual userids are assigned to each **user** and by having the **user** assign a unique password known only to them, information **owners** are assured that only authorized **users** have access to the information.

4 BACKUP AND RECOVERY

Recommended Policy: Information critical to the business function must be backed up (copied) regularly to ensure that the information can be restored should the primary information source be damaged or lost.

Recommended Standard: The frequency of information backups should be commensurate with its cost of reconstruction and value to the company.

Information backups should be stored off site from the primary information source.

Discussion: Despite all efforts to protect the integrity and availability of information, at some point the information might become lost or corrupted. Regular backup of the primary information is necessary to ensure that it can be recovered when necessary.

The frequency of backup is determined by the information's value to the company (its volatility, criticality, cost of reconstruction, and required availability). For example, customer information changes every second, is critical in providing responsive customer contact, and is expected to be available instantly on request. Real estate holdings information, however, is critical to Plant Accounting, but is much less volatile and **users** could probably tolerate some "downtime" while the information is being restored/rebuilt. The frequency of customer record backup may be nightly with ongoing transaction logging during the day. This would allow recovery up to the minute of failure. Real estate records might be backed up weekly with manual recovery from last week's backup.

5 AWARENESS

Corporate Policy: Each manager shall develop and administer an Information Security program that makes employees aware of the importance of information and methods for its security. (From: Corporate Policy on Information Management)

Recommended Standard: Organizational unit coordinators should present awareness materials at least semiannually to organization employees.

Discussion: The single greatest factor in successful information security is the employee. For effective security, employees will need to make the safeguarding of information as natural as answering the phone.

Publishing a set of policies and procedures is no assurance that they will be read and followed. An active awareness program is required, one that will inform employees *why* established policies and procedures make good business sense.

Chapter 19
Information Processing

1 GENERAL

Recommended Policy: Corporate information will be used only to conduct authorized company business, unless specifically authorized by the information **owner**.

Company-provided resources will be used only to conduct authorized company business, unless specifically authorized by management.

2 RIGHT TO REVIEW

Corporate Policy: Auditing has unrestricted access to all records, personnel, and physical properties relevant to audit assignments. (From: Responsibility Statement on Auditing)

Corporate Policy: Company management has the responsibility to manage, review, and monitor information, personnel, and physical properties relevant to their business operations. (From: Standards of Conduct)

Discussion: With the expanding complexity of the technological and competitive environment in which the company operates, it becomes increasingly necessary for management to efficiently manage its operations. In order to effectively manage its operations, management must have the ability to review the details of that operation.

Employees often have the expectation that certain areas of their business environment are private/personal. However, management has the responsibility to manage the information of the business wherever it is found. Whether

using a mechanism that is used to transport information (such as electronic-mail, voice-mail, phone/communication lines, or company mail) or store information (such as work station/computer storage, desk drawers or file cabinets), these resources have been provided by the company for business use. Although federal law allows management to monitor information, personnel, and properties of the company, recent litigation indicates that a written policy is a key element in avoiding misunderstanding (concerning an individual's expectation of privacy) and potential legal action.

3 DESKTOP PROCESSING

Desktop systems are defined as microcomputers, personal computers, portable computers, laptop or notebook computers, desktop computers, work stations, and small business computers.

Recommended Policy: The employee's management will provide all necessary desktop hardware, software, and other required information processing resources required by employees to perform their assigned responsibilities.

Recommended Standard: To ensure proper control and asset security, employees should not bring their own desktop hardware, software, or diskettes into any company facility without prior authorization from the employee's management.

Recommended Guideline: An organization desktop coordinator should be appointed for each work area with responsibility for coordinating desktop acquisition, use, and security.

4 TRAINING

Recommended Standard: Organizational unit management is responsible for ensuring that all employees using company-provided resources have adequate training. This training at a minimum should include:

- proper use of the resources
- proper use of proprietary software programs
- precautions to be taken to minimize loss of information
- compliance with corporate policies and proprietary licensing agreements

5 PHYSICAL SECURITY

Corporate Policy: Each organizational unit head is responsible for ensuring that there is proper security for all hardware, software, documentation, data, and information. (From: Company Policy on Security)

Recommended Standard: The following are minimum requirements for physical security:

- Conduct, maintain, and periodically reconcile an inventory of all units, including all hardware and software.
- Ensure that the unit is secured from unauthorized access whenever left unattended.
- Maintain a secure environment for all system control units, file servers, or master units that control or serve shared units and allow only authorized personnel access to these units.
- Backup data and programs on a regular basis.
- Store the backups in a secure off-site location.
- Store removable diskettes containing classified corporate information or programs in a locked storage device when not in use.

6 PROPRIETARY SOFTWARE — CONTROLS AND SECURITY

Corporate Policy: All employees are required to comply with federal copyright laws, nondisclosure, and vendor licensing agreements governing the installation, use, and distribution of purchased software. (From: Company Policy on Standard of Conduct)

Recommended Standard: Any employee who learns of any misuse of proprietary or licensed software or related documentation within the company should notify his or her supervisor, local information security coordinator, or Auditing.

Recommended Standard: Each organizational unit should conduct an annual software audit on its desktop units, comparing the software installed with software proof-of-purchase documentation or the original diskettes.

Discussion: The company is licensed to use the computer software from a variety of vendors. The company does not own this software or its related documentation and, unless

specifically authorized in the license for the software, does not have the right to reproduce it.

7 SOFTWARE CODE OF ETHICS

Recommended Policy: Unauthorized duplication of copyrighted computer software violates the law and is contrary to corporate standards of conduct. The company prohibits such copying and recognizes the following principles as a basis for preventing its occurrence.

- The company will neither commit nor tolerate the making or use of unauthorized software copies under any circumstances.
- The company will provide legitimately acquired software to meet all legitimate software needs in a timely fashion and in sufficient quantities.
- All employees shall comply with all license or purchase terms regulating the use of any software acquired or used.
- The company will implement and enforce strong internal controls to prevent the making or use of unauthorized software copies, including effective measures to verify compliance with these standards.

8 COMPUTER VIRUS SECURITY

Recommended Policy: Information **custodians** are responsible for providing a safe and secure processing environment in which information can be maintained with integrity.

Recommended Standard: **Custodians** of information processing systems must ensure that the system is free from destructive software elements (such as viruses) that would impair the normal and expected operation of the system.

Recommended Guidelines:

- Where available, a virus prevention, detection, or recovery package should be installed.
- Employees having access to computer systems should attend a training session on the virus threat to understand the damage a virus infection can inflict and understand their personal responsibility for protecting their own systems.
- Viruses often are transmitted through public domain software. Software that is public domain (i.e., nonlicensed software also called “shareware” or “freeware”)

or the employee's personal property should not be permitted on company equipment without the explicit authorization of organization management and after being scanned for viruses.
- Turn off or lock up your desktop system at the end of the workday to prevent unauthorized access and possible virus contamination.
- Use the "write security" tabs on diskettes whenever possible.
- Report any type of unauthorized access, theft, or virus infection to the Information Security group or the Customer Service Center upon discovery.

9 OFFICE AUTOMATION

Office automation is a catch-all phrase that includes such technologies as desktop publishing, electronic messaging, electronic-mail, voice-mail, calendars, fax, and other such efficiency tools. With the implementation of such electronic systems, certain steps must be taken that will provide an adequate level of security. While each of these systems provides the **user** greater communications possibilities, they also provide additional risks to the information they carry. Additionally, the company employs resources such as interoffice mail, filing cabinets and desks, and long-term records retention facilities to transport and store information.

9.1 Phone/Voice-Mail

Recommended Policy:	**Confidential** information shall be transmitted via phone/voice-mail only when necessary and only with proper controls to safeguard it from unauthorized disclosure.
Recommended Standard:	**Confidential** information is not to be retained in voice-mail boxes.
Recommended Standard:	Voice-mail systems are to be secured with a confidential password known only to the mail box **owner**.
Recommended Standard:	**Confidential** information must be transmitted with receipt confirmation.
Discussion:	Several rules are identified in the *Handbook for Employees, **The Company** & You* concerning the proper usage of company-provided telephones. As the technologies continue to become more sophisticated, one must ensure that information transmitted over phones and stored in voice-mail boxes is properly controlled with appropriate

password security. Because these systems are targets of phone hackers, passwords should be difficult to guess and **Confidential** information should be removed as soon as possible.

9.2 Standards of Conduct for Electronic Communication

Recommended Policy:

The Company's policies regarding Employee Standards of Conduct, Conflict of Interest, Equal Employment Opportunity and Diversity in the Workplace, Communication, and Information Protection also apply to electronic messages (e-mail), telephone messages (voice-mail), and other internal and external electronic communications, including, but not limited to, computer bulletin boards, news groups, and the Internet.

Transmitted messages are to be created, handled, distributed, and stored with the same care as any other business document. This includes complying with information-access prohibitions, accessing information only for legitimate business purposes, and protecting information from access by unauthorized persons.

Users should be aware that these systems, and the information stored within them, are the property of the Company and are to be used only for Company-approved activities. The Company maintains the right to monitor the operation of these systems.

Since confidentiality is not assured, these systems are to be used only for transmitting information considered "Public" or for "Internal Use." (The definitions for "Public," "Internal Use," and "Confidential" can be found in the Company Policy on Information Protection.) "Confidential" information should not be communicated using these electronic systems. The Company's prohibition of derogatory and offensive comments also applies to messages communicated through these systems. Special care should be given to ensure that the style and tone of messages are appropriate.

Every effort should be made to send messages only to those who "need to know." The Company Policy on Communication details the approvals required before distrib-

uting information externally or internally through the use of company mailing lists.

Employees are responsible for using these systems appropriately. Inappropriate use could result in disciplinary action.

Recommended Standard: **Confidential** information is not to be retained in electronic-mail boxes.

Electronic-mail systems are to be secured with a confidential password known only to the mail box **owner**.

Confidential information should be transmitted with receipt confirmation.

Discussion: As with phone/voice-mail systems, the technologies continue to become more sophisticated. Consequently, one must ensure that information transmitted and stored in electronic-mail boxes is properly controlled with appropriate password security. Because these systems are targets of computer hackers, passwords should be difficult to guess, and **Confidential** information should be removed as soon as possible.

9.3 Cellular Phones

Recommended Policy: **Confidential** information should not be discussed on cellular phones.

Discussion: Cellular or wireless phones broadcast conversations via radio waves that are subject to interception by inexpensive devices readily available from any electronics store. One of the legal tests for **Confidential** information is the organization's efforts to keep the information secret. By discussing **Confidential** information over a cellular or wireless telephone, the test of secrecy is lost. From a legal point of view, there is no expectation of privacy, since the sender is unable to determine who is actually gaining access to the information. Whenever in custody of **Confidential** information, it is essential that this information not be discussed on these devices.

9.4 Fax Machines

Recommended Policy: Special precautions are to be taken when faxing **Confidential** information.

Recommended Standard: Send **Confidential** information by fax only when the authorized recipient is the only person who can access it.

Discussion: Sending information via fax machines can compromise the secrecy of the information. Often, faxed documents are left at the receiving station for hours, thus allowing anyone who wanders by the opportunity to view the information. If sending **Confidential** information by fax cannot be avoided, it is critical that the intended recipient be informed by phone that the information is being sent so he or she can attend the fax station during transmission. This will ensure that only the intended recipient has received the transmission.

9.5 Interoffice Mail

Recommended Policy: Special precautions are to be taken when sending **Confidential** information by interoffice mail to ensure confidentiality is maintained.

Recommended Procedure: When transporting **Confidential** information by interoffice mail, the envelope is to carry no labeling to indicate its contents contain **Confidential** information; however, the first page of the document or cover sheet must clearly label the document as **Confidential**.

Recommended Guideline: When needing to send **Confidential** information, the sender should consider having the information delivered by a trusted courier rather than by interoffice mail.

The sender of critical information should consider use of a "Valuable Letter Receipt" to request confirmation of receipt by the intended recipient.

Discussion: When employing interoffice mail, the document will pass through several hands and be left unattended many times during the process of delivery. The interoffice couriers, mailroom sorters, and secretaries or office specialists will all have a hand in delivering a document to the recipient. It is important to avoid specifically labeling the envelope during this process. When one identifies the contents of the envelope as containing **Confidential** information, one attracts the attention of the curious. By avoiding external labeling, the envelope looks like any other.

9.6 Office File Cabinets and Desks

Recommended Policy: Information contained in office file cabinets and desks must be adequately protected against unauthorized access.

Recommended Standard: File cabinets and desks containing **Confidential** information are to be locked when no one is in attendance.

Discussion: File cabinets and desks hold a significant amount of information that one uses daily in the performance of any business function. Whether the information is classified as **Confidential** or **Internal Use**, this information requires the same level of security one might expect is provided to computer-based information. Confidentiality, integrity, and availability considerations are just as critical; but because this information is always so close at hand, one often ignores its value to the operation. It is necessary to consider the disruption that loss of this information could cause and take prudent steps to ensure its security.

9.7 Records Management

Corporate Policy: Organization management is responsible for the identification of records required to meet regulatory requirements and operations needs, and the establishment of retention and destruction guidelines for each type of record. (From: Company Policy on Information Management)

Recommended Standard: The official copy of information, regardless of media, is to be promptly destroyed upon expiration of the retention period unless precluded by pending litigation or investigation.

At least annually, the organizational unit shall verify that records are being retained according to the organizational unit's established program.

Recommended Guideline: Organizations should work jointly with Business Services (Records Management) to identify statutory requirements for records retention.

Chapter 20
Information Security Program Administration

1 INTRODUCTION

Publishing a set of policies and procedures is no assurance that anyone will ever read them. Creating an employee awareness program is necessary to bring the information security message to all employees. Before employees can accept an Information Security (IS) program, they must first understand why the program is necessary and what they will gain from its implementation.

To ensure that all employees have access to Information Security support, representatives from each unit throughout the company have been selected and trained in presenting this program to the employees within their organization. To facilitate this process, a structure has been established to administer the program, its direction and scope.

2 CORPORATE INFORMATION SYSTEMS STEERING COMMITTEE

This committee, consisting of senior management, was established to effectively capitalize on available and emerging information technologies to improve efficiency and effectiveness to meet the competitive challenges that lie ahead. This group has approved and supports the vision and goals of the Information Security program. They provide guidance, ensuring that the program is consistent with company goals, measures, and targets. They ensure the availability of resources necessary for successful implementation and maintenance of the program.

3 CORPORATE INFORMATION SECURITY PROGRAM

3.1 Corporate Information Security Manager

This individual will support and direct the corporate Information Security program. This will be accomplished by ensuring that necessary resources are available.

3.2 Corporate Information Security Coordinator

This individual is responsible for maintenance of the program's vision, goals, and elements, and for proposing necessary changes to the IS Steering Committee for approval. This individual will train and coordinate the organization IS coordinators, supporting them with regular contact, information security awareness tools, consultation, and ideas. To ensure progress throughout the IS program life cycle, this individual will monitor each organizational unit's progress and keep the Corporate IS Manager updated. The Supervisor of the Information Security group has been charged with this responsibility.

4 ORGANIZATION INFORMATION SECURITY PROGRAM

4.1 Organization Management

Organization management has a large impact on the effectiveness of the Corporate IS Program. They will be asked to promote the program by providing appropriate staff and other resources to ensure security of corporate information assets. It is crucial that they also support their organization IS coordinators in the development and maintenance of a local information security program.

4.2 Information Security Coordinators

4.2.1 Organization Coordinators. An Organization Information Security Coordinator is appointed by organization management to develop, implement, and maintain an organization IS program consistent with corporate and organization objectives. These individuals should meet with organization personnel at least semiannually to build their awareness of information security issues, responsibilities, and solutions. They act as liaison with the Corporate IS Coordinator to report the progress and activities concerning the organization IS program. The Organization IS Coordinator, together with the Corporate IS Coordinator, comprise the Corporate IS Team.

4.2.2 Group Coordinators (Optional) . Group Information Security Coordinators assist the Organization IS Coordinator in large organizations. Group IS Coordinators are appointed by the management of groups within an organization to perform group-level duties that support the organization IS program. These individuals should perform group-level information risk assessments and may meet with group personnel to build their awareness of information security issues. They act as liaison with the Organization IS Coordinator to report the progress and activities concerning the group's IS activities. The Group IS Coordinator, together with the Organization IS Coordinator, comprise the Organization IS Team.

4.2.3 Area Coordinators (Optional). Area Information Security Coordinators assist the Group IS Coordinator in large groups within an organization. Area IS Coordinators are appointed by the management of areas within a group to perform area-level duties that support the organization IS program. These individuals should perform area-level information risk assessments and may meet with area personnel to build their awareness of information security issues. They act as liaison with the Group IS Coordinator to report the progress and activities concerning the area's IS activities. The Area IS Coordinator, together with the Group IS Coordinator, comprise the Group IS Team.

Chapter 21
Baseline Organization Information Security Program

1 INTRODUCTION

Information Management Policy states:

> Each manager shall develop and administer an Information Security program that appropriately classifies and protects corporate information under their control and makes employees aware of the importance of information and methods for its security.

Management has appointed Organization Information Security Coordinators (OISCs) to administer the programs for their organizations. Larger organizations have also appointed Group Information Security Coordinators (GISCs) and Area Information Security Coordinators (AISCs) to assist the OISC.

This section of the Information Security Reference Guide is designed to assist IS coordinators with the development, implementation, and maintenance of their Information Security program. Each section below is formatted to supply background information and instruction. *Baseline Program Recommendations* are supplied to serve as possible starting points. Some *How-to:* sections are also provided.

Contact the Corporate Information Security Coordinator if you have any questions or require additional guidance.

2 PRE-PROGRAM DEVELOPMENT

2.1 Designing Your Organization's Program

What is an Information Security program? An IS program is a series of actions that:

- identifies information requiring security
- develops methods to protect the information
- documents security methods in a plan that includes specific security goals
- organizes resources to implement security methods
- implements and maintains security methods
- provides security guidance through policy and awareness activities
- monitors security method and program effectiveness
- reports plans, progress, and effectiveness to management

The purpose of the IS program is to protect the value of an important business asset — corporate information.

Where should you start? Consider those areas that are going to produce noticeable, short-range results and will make a significant contribution to management's overall objectives. The new program should also promote activities that:

- have high visibility
- have a high chance of success
- can produce high returns on relatively low investments

If there is a near and present danger such as frequent disclosure of confidential information, unavailability of critical information, or proliferation of computer viruses, then the program must address those problems quickly.

The Information Security program is not something apart from the company's business. It is a business activity that supports the business. As with any business activity, the program must make good business sense. Exhibit 1 shows two important business sense requirements that the program must meet.

A program that fails to meet these requirements has no valid reason to exist as part of the business.

An effective and efficient Information Security program is one that provides the highest level of security that is consistent with an organization's requirements for productivity and cost-effectiveness. The program must have a strong organization identification and fit into the organization's environment, culture, and objectives.

Exhibit 1. Business sense requirements.

1. The *cost* of the program should never exceed the *value* of the information that it protects.
2. The *goals* of the program should be clearly aligned with, and supportive of, the goals of the organization.

Last, the program must *enable* employees by ensuring that the information they need is as accurate and available as required by the organization. The program must not disable them by protecting information to the extent that employees cannot use it. Ultimately, organization management must determine the proper level of security required.

2.1.1 Orienting the Program Toward Business Goals. An Information Security program oriented toward business goals should:

- concentrate mostly on protecting the information that supports the organization's *critical* business functions
- be structured to avoid the effects that loss of integrity, confidentiality, or availability of information resources will produce on these critical functions
- offer preventive and reactive measures that are based on a business rationale

Repeating — the program must be business justified. **It must improve your organization's business.**

2.2 A Phased Approach to the Program Process

As the organization's program is developed, take a phased approach. Convince management to allow *adequate time* to develop the program properly. Maintaining a program is a *process*, not an event. Program projects start and end, but the program does not.

Program phasing is a useful method that allows one to take a step-by-step approach toward implementation of the program elements. There are three types of phasing. The one that works best depends on how information is processed in an organization.

Functional Phasing: Functional phasing involves a series of program steps, each of which is carried out throughout the entire target organization before the next step is taken.

Organizational Phasing: With organizational, or group, phasing, one completes the entire process in one group before going on to the next. This may be required by management so that they can see the effect of the program on a test business unit before going on to other groups.

Hybrid Phasing: Hybrid phasing is a combination of the first two types of phasing. It can appear in many variations.

Baseline Program Recommendation

Use Functional Phasing. The guidance supplied in this section of the ISRG takes this approach by breaking the process into three sequential phases:

1. Program Development phase
2. Program Implementation phase
3. Program Maintenance phase

2.3 Getting Assistance

Before getting into program development, always remember **— you are not alone.** There are several employees like yourself who have been given the task of developing a program for their organization. Very few had any experience with Information Security before the responsibility was assigned to them.

Baseline Program Recommendation

Contact the areas below to get help with Information Security or program development.

- Corporate Information Security Coordinator
- Internal Audit
- Fellow Organization Information Security Coordinators

3 PROGRAM DEVELOPMENT PHASE

The development phase of the organization Information Security program includes determination of the program scope, assessment of the information environment, and development of the program elements (policies and procedures, controls, business continuity plan, awareness program, effectiveness monitoring).

3.1 Determining Initial Program Scope and Obtaining Approval

Before assessment can begin, the scope of the program must be identified. Will it include one group, several groups, or the entire organization? If not applied to the entire organization, what is the sequence of implementation? Will some groups or some information types be excluded from the Information Security program? These questions should be answered with input, support, and approval of organization management.

By approving the Information Security Policy and the Corporate Information Security Program, Senior Management has expressed their commitment to the implementation of the security program. What will be important to you is to create a program that meets your organization's business needs and fulfills the requirements of the Corporate Policy on Information Protection.

To meet the expectations of management, it is necessary to understand the business objectives and directions of the organization. Before beginning to develop the organization's program, take a little time and establish where the organization is headed and what the goals and objectives are for

the coming year. The program should complement the established business objectives. Once the organization's program is developed, it will be necessary to present the program to management for their review and approval. This approval process should be documented.

Baseline Program Recommendation

1. Contact the Corporate Information Security Coordinator for help in preparing for meetings with organization and group management.
2. Determine who in organization management must approve initial program activities and the finished program.
3. Establish a draft program scope.
4. Meet with organization (top) management.
   a. Describe the need for them to provide guidance so that the scope of the program can be established.
   b. Request the appointment of Group Information Security Coordinators for large groups, or for groups that may require extensive Information Security activities. (The IS coordinators comprise the organization IS team.)
   c. Describe the assessment process (see below) that will be used with each group.
   d. Have them identify the groups where program implementation will take place. If some will be initially exempt, ask management to identify the date of their inclusion.
   e. Have management identify the *organization* information resources that will be included. If some will be initially exempt, ask management to identify the date of their inclusion.
5. Determine who in group (lower) management must approve the initial program activities and the finished program.
6. Meet with the organization IS team to discuss the information assessment.
7. Meet with group management where information assessment is planned. (Work with Group Information Security Coordinators if they have been appointed.)
   a. Explain the assessment process and request their support and assistance. (This is a good time to describe the advantages of cost-effective security of *this group's* information.)
   b. Have management identify the *group* information resources that will be included. If some will be initially exempt, ask management to identify the date of their inclusion.
   c. Have management identify the **owners, custodians,** and **users** of the information resources. Where none are designated, work with management to establish them.
   d. Have management identify other organizations that may be involved and the nature of their involvement.

8. Provide reports to organization management indicating status of meetings with group management, listing exclusions and dates the exclusions will be addressed. (Forward a copy to the Corporate Information Security Coordinator.)
9. Provide semiannual progress reports to organization and group management. (Forward a copy to the Corporate Information Security Coordinator.)

3.2 Assessing the Information Environment

The early steps of the program consist of fact gathering and assessment. Before any program can begin, it is important to identify the organization's information and the impact on the business process if the information was modified, destroyed, or disclosed in an unauthorized or undesirable manner. Therefore, it will be necessary to assess the information within the organization. This will require an understanding of how the organization functions.

3.2.1 Identifying Critical Systems Applications and Confidential Information. What is meant by a *critical system*? A critical system is defined as any system that, if unavailable, would seriously impair the ability of an organization to perform key business functions. The designation *Critical* is **not** one of the official classification categories defined in the Information Clarification Policy. It is an indicator of how important the system is to conducting business. Generally speaking, employees understand the need to protect information classified as **Confidential**, but are sometimes confused over the need to protect critical systems and applications.

The highest information classification level at the Company is **Confidential**. Confidential information is defined as any information which, if disclosed, could violate the privacy of individuals, reduce the company's competitive advantage, or cause damage to the company (monetarily, legally, public perception, customer and shareholder confidence, etc.).

Two key questions must be answered when determining if information is confidential. The first questions is — what would be the impact on the company if the information was disclosed? If there is a high risk of loss of privacy, competitive advantage, or damage, then the information should be classified as **Confidential**. The second question to be answered is — how many individuals will need access in order to perform their jobs? A key requirement of confidential information is the ability to keep the information secret both internally and externally. The greater the number of employees requiring access to the information, the less likely that it will be kept secret. If this is the case, then a special subclassification could be established for the organization. This would allow an organization to add a category that meets its needs. The special classification category would

fall under an existing classification category and would allow for tighter controls than identified by corporate policy.

Section 3 in Chapter 22 is a worksheet that could be useful when identifying information, its confidentiality, and its criticality.

3.2.2 Assessing Risk. What is *risk assessment*? Risk assessment is a method for determining the likelihood and impact of loss of information integrity, availability, and confidentiality. The risk assessment method includes information asset valuation and identification of threats to, and vulnerabilities of, the target information.

Why do a risk assessment? The assessment will result in a prioritized list of the information most at risk and which could cause unacceptable losses to the business. The prioritized list provides direction as to where Information Security controls should be applied first and how much to spend on the controls. The assessment results should be reported to management to allow them to make fact-based decisions and provide approval for controls to be implemented. Management will not approve controls for all risks. Where this occurs, management's reasons should be documented for future reference and planning.

The first step in this process is to identify the information assets within the organization. This would not only include information created within the organization, but also any information used by employees. One will want to include such items as databases, spreadsheets, original source documents, bid responses, signature cards, etc. Include all information regardless of how it is created or the media on which it is stored.

Once the information assets have been identified, consider their impact on the organization. In traditional risk analysis, there are three types of impact:

1. unauthorized or undesirable modification of information (loss of integrity)
2. unauthorized or undesirable destruction of, or denial of access to, information (loss of availability)
3. unauthorized or undesirable disclosure of information (loss of confidentiality)

Each of these impact types can be accidental or intentional. Take a look at threats, vulnerabilities, and loss.

Identifying Threats: Threats are any activities or events that, under certain conditions, could jeopardize the integrity, availability, or confidentiality of information. Threats can be natural (storms, floods, lightning, rodents) or manmade (theft, vandalism, electrical fire). The possible threats to each type of information must be identified.

Identifying Vulnerabilities: Vulnerabilities are conditions that could allow threats to cause loss of information integrity, availability, or confidentiality. If there is no vulnerability, the existence of a threat is immaterial since the threat cannot cause a loss. Identifying vulnerabilities is the process of estimating the likelihood that the threats will cause loss of information integrity, availability, or confidentiality. The vulnerability of each type of information must be identified.

Identifying Loss Impact: Loss impact is the effect on the business when a vulnerability allows information integrity, availability, or confidentiality to be compromised. Loss impact should be identified as a dollar estimate. Loss impacts must be identified.

3.2.3 Identifying Security Controls. Information Security controls are measures that are designed to minimize or eliminate a vulnerability. For each type of information, the risk assessment should identify the likelihood and magnitude of losses that the business could experience. Naturally, the greatest concern should be for information that has high vulnerability and high loss impact. This is where controls should be applied first. The control should be designed to minimize the probability that the vulnerability will occur. The cost of the control should be governed by the loss impact of the vulnerability. It makes good business sense to spend $100.00 per year to prevent a likely $1,000.00 loss over the same period.

A typical control is to ensure that only employees with a business need are given access to confidential information. Another control would be to establish a systematic backup process for spreadsheets used by the department. When establishing controls, remember that the key element is to ensure that the business process can function while limiting vulnerability and losses to an acceptable level. Controls are discussed in later sections.

Baseline Program Recommendation

1. Identify the organization's information resources using the Information Identification Worksheet in Section 3, Chapter 22. (The worksheet will help document the organization's business functions, and the identification, classification, criticality, and **owner** of the information supporting the business functions.
2. Identify the risk to the organization's information resources (identified in 1 above) using the Information Risk Assessment Worksheet in Section 4, Chapter 22. (The worksheet will help identify and document the threats to, vulnerabilities of, and loss impact of each type of the organization's information.)
3. Identify recommended Information Security controls.
4. Transfer data from the Information Identification Worksheet and the Information Risk Assessment Worksheet to the Summary and Con-

trols Worksheet in Section 5, Chapter 22. Prioritize the implementation order of the recommended controls based on the information's classification, criticality, vulnerability, and loss impact; and on the priority of the business function that the information supports.

5. Additional assessment data can be developed by completing the Self-Assessment Questionnaire in Section 6, Chapter 22. (This questionnaire identifies specific controls that should be addressed by the program. Take the document and modify it for your own use. As part of the initial program, the questionnaire is to be completed by each OISC and the results submitted to the CISC. Questionnaire results can be used in the future as a benchmark to monitor how well the organization's program is progressing.)

3.3 Developing the Program Elements

The sections below describe the major elements of the program. These include:

- Program Plan
- Policies and Procedures
- Controls
- Awareness
- Effectiveness Monitoring

The descriptions contained in each section are recommended starting points. Each organization must decide how they should be applied to best protect their business information.

3.3.1 Program Administration. The first organization program element is program administration. This element provides direction for the program and is critical to its success.

3.3.1.1 Organization Management. Organization management is required to appoint an Organization Information Security Coordinator (OISC) to oversee the program. In larger organizations, management may also appoint Group Information Security Coordinators (GISCs) to assist the OISC. Together they form the **Organization Information Security Team**.

In addition to appointing coordinators, a successful program depends on management to do the following.

- Management should demonstrate and communicate an active interest in having an effective program.
- Management should put the program under the authority of people who have the skills and motivation to make it work.
- Management should provide money and resources.
- Management should support the recommendations of the Organization Information Security Team.

3.3.1.2 Organization Information Security Team. The Organization Information Security Team is a group appointed by management to administer the organization's program. The team may have one or more Organization Information Security Coordinators and several Group Information Security Coordinators. Normally, the OISC will be responsible for most or all of an organization, while the GISC will be responsible for one or more groups within the organization. Organizations with many groups will have several GISCs. Large groups within the organization may have Area Information Security Coordinators (AISCs) supporting the GISC. The qualifications and duties of all coordinators are similar.

IS Coordinator Qualifications — A **Company** employee who:

- has broad familiarity with the organization or group, which allows him or her to understand its Information Security needs and concerns
- has easy access to all levels of management in the organization or group
- is familiar with information technologies
- has good presentation and speaking skills

IS Coordinator Responsibilities include:

- attending training conducted by the Corporate Information Security Coordinator
- working with organization and group management to develop, implement, and maintain an Information Security program consistent with the corporate program
- OISCs meeting with GISCs, and GISCs meeting with AISCs on a regular basis to develop their Information Security responsibilities
- conducting Information Security awareness sessions on a regular basis in area of responsibility
- OISCs keeping the Corporate Information Security Coordinator informed of progress and activities concerning the development and maintenance of the organization Information Security program. GISCs do the same, but keep the OISC informed. AISCs do the same, but keep the GISC informed.

Typical IS Coordinator Commitment:

- Development Phase (8–12 weeks) — OISC less than half-time, GISC less than quarter-time, AISC less than ten percent of time.
- Implementation Phase (8–12 weeks) — OISC less than half-time, GISC less than quarter-time, AISC less than ten percent of time.
- Maintenance Phase (ongoing) — OISC 2 to 4 hours per week, GISC 2 to 4 hours per week, AISC 1 hour per week.

Information on the Corporate Information Security Team and its relation to the Organization Information Security Team can be found in Chapter 20, "Information Security Program."

3.3.1.3 Organization Information Security Program Plan. The plan documents the purpose and goals of the organization program. The plan should be:

- initially written by the OISC with the assistance of the organization's IS team
- reviewed and revised annually, preferably early in the year prior to budget submission, by the OISC and the organization IS team
- approved by organization management prior to release and implementation
- compatible with and supportive of the corporate IS plan

A final approved copy of the annual program plan should be forwarded to the Corporate Information Security Coordinator.

The program plan should contain a mission statement, program objectives, and program goals.

Program Mission Statement

The mission statement defines the role of, and the need for, the organization IS program. It also serves to notify management and organization employees as to the overall direction of the program.

Baseline Program Recommendation

Here are two sample IS program mission statements.

- To provide cost-effective security for organization information assets to ensure their availability, integrity, and confidentiality; and to protect management from charges of imprudence in the security of information assets.
- To ensure that organization information resources are protected in a manner that is cost effective and reduces the risk of information loss, modification, or disclosure to a level that is acceptable to management.

Program Objectives

The objectives are general descriptions that define what the program is designed to do for the organization.

Baseline Program Recommendation

Basic program objectives include:

- Protect and ensure the accuracy and integrity of information.
- Protect sensitive, confidential, and competitive information from unauthorized disclosure.
- Provide security from acts that would cause destruction of information.
- Maintain organization Information Security policies and procedures.

- Maintain an organization information security awareness program.
- Maintain organization group business information continuity plans.
- Provide organization groups with direction and technical support to ensure the availability, integrity, and confidentiality of corporate information.
- Ensure the ability of the organization to continue business after disasters.

Additional Program Recommendations

Additional program objectives include:

- Submit an annual information security budget.
- Provide recommendations to organization groups on how to develop and maintain policies and procedures.
- Provide information security awareness sessions and materials to organization groups.
- Provide and recommend cost-effective information security measures.
- Maintain a high-performance Information Security program that achieves the balance of security and productivity desired by management.
- Build a comprehensive Information Security environment capable of meeting the changing needs of internal and external customers.
- Ensure management awareness of the need to protect information, and their support in development of policies.
- Identify and bring to management's attention possible vulnerabilities relating to the security of information assets.
- Protect management from charges of imprudence in the event of a compromise of information security.
- Monitor laws and regulations, utility industry activities, and the Information Security industry for changes that may affect the security of information assets.

Program Goals

The program goals are usually more detailed than the program objectives and should contain measurable targets. It is recommended that both one-year and two-year goals be developed. But remember Business Sense Requirement #2: "The goals of the program should be clearly aligned with, and supportive of, the goals of the organization." Goals are first established when the program is initially implemented and should be reviewed and rewritten at the start of each year.

Baseline Program Recommendation

Some sample one-year goals for a **new program** include:

- Establish an Organization Information Security Team by (*date*).

- Develop and implement organization Information Security policies and procedures and document them in an organization policies and procedures manual by (*date*).
- Develop and implement an organization Information Security awareness program by (*date*).
- Develop and implement organization business information continuity plans by (*date*).
  - Perform an initial assessment of the organization's information environment by (*date*). It should identify:
    - information that is sensitive or critical to business functions
- information most at risk to unauthorized access, modification, disclosure, or destruction.
- Develop and implement Information Security controls by (*date*).
- Develop methods to monitor for compliance to policy by (*date*).
- Develop methods by (*date*) to encourage compliance (rewards) and discourage noncompliance (enforcement) to policy.

Some sample program goals for an **established program** include:

- Review and maintain the organization Information Security policies and procedures manual.
- Review and maintain the organization Information Security awareness program.
- Review and maintain organization business information continuity plans.
- Perform reassessment of the organization's information environment to identify:
  - information that has become, or no longer is, sensitive or critical to business functions
  - information that has become, or no longer is, at risk to unauthorized access, modification, disclosure, or destruction
- Review and maintain Information Security controls.
- Monitor for compliance to policy.
- Encourage compliance (rewards) and discourage noncompliance (enforcement) to policy.
- Evaluate new Information Security technologies.

3.3.1.4 Organization Information Security Program Budget. Organization information assets cannot be protected unless resources are provided by management. The largest cost will be for IS coordinator labor hours required to administer the program and to develop, implement, and maintain Information Security policy, awareness, controls, and compliance monitoring. Some cost, however, will be incurred for educational resources (books, magazines), training, awareness materials (videos, posters, pamphlets), and technical controls such as computer access control and virus-scanning software. As a result, Information Security costs will primarily be Op-

Exhibit 2. Sample organization 1995 budget estimate.

Item	OISC (1)	GISC (3)	AISC (6)	Item Total
O & M Budget:				
Part-time labor	$2000	$6,000	$6,000	$12,000
Vendor training	$2500	$7,500	$0	$10,000
Professional memberships	$150	$450	$0	$600
Capital budget:				
Awareness materials	(videos, posters, pamphlets, etc.)			$1,000
Physical access controls	(file cabinets, disk storage boxes)			$1,000
PC/Mac access controls	(software for 50 computers)			$2,500
PC/Mac virus security	(software for 50 computers)			$2,500
	Total			$29,600

erations and Maintenance (O&M) budget items, along with some Capital Budget items.

The IS budget should be prepared and submitted with the organization's other budgets. The budget should include the two-year goals described in the Organization IS Plan prepared earlier in the year.

As one prepares the budget, do not forget Business Sense Requirement #1: "The cost of the program should never exceed the value of the information that it protects." The value, or criticality, of the information being protected should be determined, or at least estimated, as part of the self-assessment (described above) or the Business Impact Analysis (described below).

Baseline Program Recommendation

Exhibit 2 displays a 1995 budget estimate for a sample organization with one OISC, three GISCs, six AISCs, and 50 PC/Mac computers. OISCs and GISCs spend two hours per week, and AISCs spend one hour per week on Information Security.

This sample organization should plan on a *total* IS expense of $30,000 per year. Since 40 percent of the cost is for part-time labor (no additional personnel hired), the actual additional cost to this sample organization is approximately $18,000. It should be easy to show that the value of this organization's information is much greater than the amount spent next year to protect it.

3.3.2 Developing Organization Policies and Procedures. Policies and procedures are the foundation of the IS program. Their purpose is to clearly communicate consistent, effective, and efficient guidance throughout the organization. Organizations should develop their own policies and procedures under the following conditions:

- where there is a clear business need to provide employees with guidance
- when adequate guidance is not already provided from other sources

In addition to policies and procedures, organizations may find it necessary to develop standards and guidelines as well. Below are some definitions to provide consistency and understanding.

Policy: A general statement that provides direction and establishes the basic philosophy of the organization in areas where controls must be established. Compliance with policy should be mandatory.

Standard: A statement of design or implementation that is a norm for measurement. Use of standards is usually restricted to situations where performance to specific measurement is required. Compliance with standards should be mandatory.

Procedure: How-to instructions presented in a series of steps that support some part of a policy or standard. Compliance with procedures should be mandatory, with some method for seeking variance.

Guideline: How-to instructions that are an outline of policy and that support some part of a policy or standard. Guidelines should be advisory and allow some level of local option or management interpretation.

The need for policies, procedures, standards, and guidelines can be identified by the IS self-assessment and by reported damage to information assets (incident reports).

Some tips to help with the development effort include:

1. Before you start:
   a. know organization culture
   b. determine the level of control allowed in the organization
   c. obtain existing policies, procedures, standards, and guidelines
   d. determine who writes them
   e. determine if there is a real business need to give employees guidance
   f. justify the need by using information assessment results and incident reports
2. When you start:
   a. identify the audience
   b. make it clear; use simplest appropriate wording
   c. avoid absolutes (all, never, always, etc.)
   d. determine the objective
   e. determine the scope
   f. determine the purpose
   g. provide definitions where necessary
   h. identify responsibilities
   i. identify who, if any, are exempt from requirements
   j. record revision date

Exhibit 3. Document checklist.

For a POLICY, STANDARD, GUIDELINE, or PROCEDURE; does the document:

☐ Meet the stated objective?
☐ Clearly describe WHO is responsible to perform desired behavior?
☐ Clearly describe WHEN the behavior is expected?
☐ Clearly describe who is exempt, when, and why? (If required)
☐ Contain simple, unambiguous, and appropriate wording?
☐ Contain proper wording for the intended audience?
☐ Fit the level of control acceptable in the organization?

For a POLICY or STANDARD, does the document also:

☐ Clearly describe WHAT behavior is expected?
☐ Clearly describe WHY the behavior is expected? (Optional, depends on culture)

For a STANDARD, does the document also:

☐ Clearly describe HOW MUCH security is expected?

For a GUIDELINE or PROCEDURE, does the document also:

☐ Clearly describe HOW TO attain the expected behavior?

3. Use the checklist in Exhibit 3 after writing the first draft.
4. Finally:
   a. have organization IS team review the document and provide comments
   b. make revisions to include accepted comments
   c. obtain management approval

Baseline Program Recommendation

Refer to Chapters 14 through 19 of this guide to obtain recommended policies, standards, procedures, and guidelines for specific IS subject areas. It is recommended that each organization develop policies in the following areas:

- business continuity planning (Chapter 14, Section 2)
- information classification (Chapter 16)
- information handling, labeling, etc. (Chapters 17, 19, and 22, Section 1)
- information backup and recovery (Chapter 6, Section 4)
- desktop processing (Chapter 19)
- monitor and control of proprietary software (Chapter 19)

Organizations that develop several IS policies, procedures, standards, and guidelines should consider organizing them into an IS policy manual.

For additional help, contact the Corporate Information Security Coordinator.

3.3.3 Developing the Awareness Program. Many employees will approach the new IS program with concern that it will inhibit their job activities. Some will not understand why it is necessary to implement such a program now — "After all, haven't we been doing fine up until now?" When the program is presented to the employees, be prepared to answer such questions. An awareness program is actually a sales pitch. Remember that the employees already know what is expected in the workplace. The goal is to remind them that information asset security is part of that process.

The awareness program is a management control rather than a technical control. The value of awareness is made clear in the following quote.

> The secret to enforcement is prevention, and the key to prevention is education.
>
> — R. Wallace Hale

Employees must be educated, or made aware, that they will be expected to protect information. Education increases their insight and understanding and teaches why they should protect information. Employees must also be told what to protect, when to protect, and how they should protect information assets. One wants to be sure that no one thinks that security is the coordinator's or some other employee's responsibility. All employees, including contract employees, are part of the Information Security process.

The utility business environment is changing. In the past, utilities were able to share information freely. As the business world heads into deregulation, competitiveness will require the **Company** to protect some information from disclosure to other utilities. Conducting business as in the past will not allow us to meet the needs of the future. With more and more people having access to company information, it will be necessary to have the proper controls in place to protect the interests of the **Company**. The first presentation in the awareness program could be designed to show employees that disclosure of, or unauthorized access to, business-sensitive information could happen in one's own organization.

The Corporate Information Security Coordinator has developed some tools that can be used by one's organization in implementing an employee awareness program. Video tapes, posters, brochures, and other such materials will be available for the program.

Baseline Program Recommendation

1. Refer to the results of your information assessment and identify problem areas in the organization. Target these areas as topics for awareness sessions.

2. Include organization policies as a topic for an awareness session.
3. Ask management for awareness session topics.
4. Include the awareness session schedule in the Organization Information Security Plan.
5. Contact the Corporate Information Security Coordinator for assistance in developing the awareness program.

3.3.4 Developing Information Security Controls. Information Security controls can be separated into two types: management controls and technical controls. Already discussed were management controls in the form of program administration, plans, budgets, awareness, and policies. Other management controls, which are covered below, include business continuity planning, awareness, and compliance monitoring. Technical controls include physical access controls such as locked file cabinets or locked computer keyboards. Technical controls also include software to prevent computer and file access, software to detect and remove computer viruses, software to check that proper passwords are being used, and software to manage computer security.

3.3.4.1 Developing the Business Continuity Plan. The business continuity plan (BCP) is a management-type control to ensure that *critical business functions* can be performed after a disruption of normal business operations. The scope of the BCP includes activities that should be performed before, during, and after such a disruption to business. But what does this have to do with Information Security? Many critical business functions are dependent on the availability of information assets. Each organization IS team should coordinate the development of a BCP that identifies the organization's critical business functions and the information required by those functions. Before writing the plan, a Business Impact Analysis should be done.

Performing a Business Impact Analysis

The purpose of a business impact analysis (BIA) is to determine the effect on the organization of loss of critical business functions. The critical business functions directly support the primary goals of the organization and enable the fulfillment of its Value Added Role.

How-to: (See Information Identification Worksheet, Chapter 22, Section 3)

1. Identify the organization's critical business functions.
2. Establish the priority of each critical business function.
3. Determine how long the organization can do without each critical business function.
4. Identify the resources, especially information resources, required to support the critical business functions.

5. Estimate the tangible and intangible impacts on the organization of loss of each critical business function.

One may notice that the business impact analysis is similar to the information risk assessment described earlier. The main difference is that a threat-vulnerability analysis is not performed here.

Writing the Business Continuity Plan

A business continuity plan usually includes four major sections: preventive measures, continuity measures, exercising the plan, and plan maintenance.

How-to:

1. Develop and document the **Preventive Measures**. These include the actions that should be taken *before* a business disruption occurs. Preventive measures are of three types:
   a. Measures that prevent events that could cause loss of critical business functions. Examples include safety measures that prevent injury to personnel and housekeeping measures that prevent fires or damage to equipment.
   b. Measures that minimize negative effects to critical business functions if disruptions occur. Examples include personnel evacuation procedures and fire detection and suppression systems.
   c. Measures that allow restoration of critical business functions if disruptions occur. Examples include having backup personnel trained and copies of documentation, software, and data stored off-site that are periodically updated and available when needed.
2. Develop and document the **Continuity Measures**. These include the actions that should be taken both during and after a business disruption occurs. Continuity measures are divided into three phases:
   a. Emergency phase measures: Procedures that describe actions to be taken during and immediately after disruptions to critical business functions.
   b. Backup phase measures: Procedures that allow critical business functions to be performed in a minimal, temporary environment after a disruption occurs.
   c. Recovery phase measures: Procedures that provide restoration of the normal business environment and the restarting of business operations in the normal environment.
3. Develop and document procedures to **Exercise the Plan**. To be sure that the procedures in the plan will achieve the desired results, portions of the plan must be exercised (tested) periodically. This requires that procedures and scenarios be devised to exercise the plan.

4. Develop and document procedures to **Maintain the Plan**. The plan must be updated periodically to reflect changes in the business environment and to include required revisions that were identified during plan exercises. The person responsible for review of the plan and the length of time between plan review and revision should be documented.

Additional information on business continuity planning can be found in Chapter 14 or by contacting Information Security and Disaster Recovery Planning.

Baseline Program Recommendation

1. Identify the organization's primary goals or objectives
2. Perform a Business Impact Analysis. (See Performing a Business Impact Analysis below.)
3. Develop a Business Continuity Plan. (See Section 5.4.3 in Chapter 21: Organization Information Security Program Plan and Writing the Business Continuity Plan below.)

3.3.4.2 Common Technical Controls. Technical controls are methods that can be applied to prevent or minimize the loss of information availability, integrity, and confidentiality. Effective technical controls cannot be easily bypassed and are applied when management controls such as policy and awareness either fail to produce desired results or are less cost effective than technical controls.

A detailed discussion of all of the types of technical controls available is beyond the scope of this guide. Even so, some of the technical controls described earlier in this guide are: information handling (Chapters 17, 19, and 22), access controls and backing up information (Chapter 18), virus security and licensing agreements (Chapter 19), and encryption (Section 1 in Chapter 22). More information can be obtained from the Corporate Information Security Coordinator.

Baseline Program Recommendation

1. Refer to the results of your information assessment and identify where technical controls can be useful and cost effective.
2. Provide locks for file cabinets and rooms where information is stored.
3. Provide access control software for computers.
4. Provide easy-to-use backup methods such as making copies of documents, software, and data and storing them in a safe place away from the primary copies.
5. Provide virus-scanning software for desktop computers. This may be available from the Corporate Information Security Coordinator.

3.3.5 Developing Effectiveness Monitoring. It is important that IS coordinators and employees understand that management follows up on approved plans and programs. This follow-up is achieved through effectiveness monitoring. Effectiveness monitoring, or compliance monitoring, is another management-type control. There are two primary things that should be monitored for effectiveness: the *Information Security program* itself and the *controls*, both management and technical, that the program has implemented.

Program effectiveness can be demonstrated by achievement of the program goals. The Organization Information Security Program Plan (described above) contains the objectives and goals of the program. The program's effectiveness in achieving these goals should be monitored.

Baseline Program Recommendation

1. Check that the plan goals are measurable whereever practical.
2. Determine who, how, and when progress toward goal milestones will be monitored.
3. Determine who, how, and when progress will be reported to management.

The second area where effectiveness monitoring should be applied is on the implemented IS controls. Controls such as policy and awareness should deliver the IS message to employees. Delivering the message, however, is not enough. Compliance monitoring and enforcement are necessary to determine the effectiveness of the controls and to let employees know that compliance is being monitored. Also, a method is needed to report incidents where information has not been adequately protected. Last, there should be some method to provide rewards for compliance, additional awareness for initial noncompliance, and reprimands for continued noncompliance.

Baseline Program Recommendation

1. Develop methods to monitor control effectiveness and employee compliance.
2. The awareness program should encourage employees to remind one another of methods to protect information and to comply with policy.
3. IS coordinators who discover employee noncompliance should discuss it with the employee.
4. Where 2 and 3 above fail, develop incident reporting methods for employees and IS Coordinators to report noncompliance to local management.
   a. First-time offenders should receive additional awareness from the local IS coordinator.

b. Continued noncompliance should result in reprimands from local management.
5. Develop incident reporting methods to allow employees to report ineffectiveness of management controls and technical controls.
6. Develop methods to provide rewards and recognition to employees and groups that effectively protect information and comply with controls.

Organizations that desire additional advice on compliance monitoring should contact the Corporate Information Security Coordinator or the General Auditor. The Organization Information Security Coordinator should be notified of any special problems or need for additional support.

4 PROGRAM IMPLEMENTATION PHASE

The implementation phase of the Organization Information Security program follows the development phase and is the introduction, or roll-out, of the program to organization employees. Although short in duration, this phase is critical to employee acceptance since "you will never get a second chance to make a good first impression." Employees must be told about the program elements, including corporate and organization program administration, policies and procedures, IS controls, the business continuity plan, the awareness program, and effectiveness monitoring.

4.1 Program Implementation Plan

As with the program development phase, one should work with organization management to plan the program implementation phase. The implementation, or roll-out, is similar to an awareness presentation. Normally, awareness activities tell the target audience *what* you want them to do, and *why* they should do it. Before you can do that, however, you need to tell them *what* the program elements are, and *why* they are being implemented. The goal of the implementation plan is to do this in a manner that encourages employees to *want* to support the program's efforts. Here are some recommendations on what to put in the implementation plan.

Communication Methods

- Presentations
  - Management (1 hour)
  - Employees (1.5 hours)
    - Organization management conducts introduction
- Pamphlets
  - Corporate and organization policies
- Video
- Handouts
  - Organization program details

Presentation Contents

- Organization IS Program Elements
  - Program Administration
    Organization Information Security Teams
    Corporate Information Security Team
    IS Plan: Mission, Objectives, Goals
  - IS Policies and Procedures
    Corporate Policies
    Organization Policies
    [*Note:* This will be the first time that an audience may have seen any of these policies. Whenever possible, presentations should *stress the positive* (work can be done more quickly and efficiently if information is available and accurate); however, there are certain elements within that all employees need to be made aware. Keep the policy discussion short and try to provide them with just an *overview* of the policy contents. Inform employees as to where and how they will be informed about organization policies.]
    Information Classification
  - IS Controls
    Access controls, information handling, copying/backing up information, licensing agreements, virus security, etc.
  - Business Continuity Planning
    [Disclosure of information or unauthorized access can happen right in your organization. With the changes in the utility work environment, as we head into deregulation, the need to be competitive will be the making or breaking point for the **Company**. Conducting business as in the past will not allow us to meet the needs of the future. With more and more people having access to our information, it will be necessary to have the proper controls in place to protect the interests of the **Company**. (At roll-out, there may not be many controls to talk about. This will be covered in later awareness presentations.)]
  - Awareness Program
  - Effectiveness Monitoring
    Program Effectiveness
    Effectiveness of IS Measures

Baseline Program Recommendation

1. Meet with the organization IS team to develop a draft program implementation plan.
   a. Determine how and when you will roll-out the program to the organization.
   b. Determine each IS coordinator's roll-out responsibilities.

c. Determine the goal of the implementation plan.
d. Determine the contents of communications.

2. Meet with organization management and present the implementation plan. Revise as required and obtain approval.

5 PROGRAM MAINTENANCE PHASE

The IS program is not a development event or an implementation event. Information Security is an ongoing process. Due to changes in the business environment and information technology, the Information Security measures implemented today could be less effective or obsolete within a few months. That is why the IS program and its effectiveness must be monitored and reviewed constantly. This allows effective measures to be retained and ineffective ones to be modified or replaced. Here are some suggestions for the maintenance of the organization's programs.

5.1 Conducting Periodic Information Security Team Meetings

Team meetings should be held periodically to:

- review the IS program and its effectiveness
- discuss changes in the business environment and their effect on Information Security
- discuss information technology changes and their effect on Information Security
- determine if program efforts have retained their business justification
- review if efforts are following your Information Security plan
- reinforce team communication
- review corporate IS program activities

Baseline Program Recommendation

1. The OISC should schedule a meeting of the organization IS team, at least once every two months, to review program progress and effectiveness.
2. Meeting minutes and action items should be recorded and sent to absent coordinators, organization management, and the Corporate Information Security Coordinator.

5.2 Maintaining Knowledge of the Information Environment

Since the business environment and information technology will change, the information environment will also change. This requires that information and risk assessments be conducted periodically in order to maintain the proper level of Information Security (neither too restrictive nor too permissive). The assessment procedure described earlier, or a procedure modified for use in the organization, should be performed periodically to identify the current information environment.

Baseline Program Recommendation

1. At least once per year, the OISC should coordinate the efforts of the organization IS team to conduct an assessment of the organization's information environment. This should be done in December prior to the annual review of the organization's IS plan.
2. The results of the assessment should be collected and made available to all coordinators prior to the annual review of the organization's IS plan.
3. A summary of the assessment should be sent to organization management and the Corporate Information Security Coordinator.

5.3 Maintaining the Information Security Plan and Budget

The original IS plan documented the purpose and goals of the organization program. At a minimum, the plan should be reviewed and revised annually by the organization IS team. This should be done early in the year prior to budget submission. The plan should be compatible with and supportive of the corporate IS plan.

The review of the plan should not be difficult if IS team meetings were conducted and documented as described in the previous section. The task remaining is to review the program mission statement, objectives, and goals to determine if revisions are needed due to changes in the business environment or information technology over the last year.

Baseline Program Recommendation

1. The OISC should schedule a meeting of the organization IS team in January to review the plan mission statement, objectives, and goals to determine if revisions are needed due to changes in the business environment or information technology.
2. The results of the last information assessment should be available to all coordinators.
3. Last year's one-year goals should be reviewed for level of success.
4. Last year's two-year goals should be reviewed and incorporated into this year's one-year goals. New one-year goals should also be identified and documented.
5. This year's IS budget should be reviewed in light of the one-year goals identified.
6. Two-year goals should be identified and documented. They should be included in budget requests for the following year.
7. The draft plan should be compatible with and supportive of the corporate IS plan.
8. The draft plan and budget request should be sent to organization management.

9. The approved copy of the annual program plan should be forwarded to all organization coordinators, organization management, and the Corporate Information Security Coordinator.

5.4 Maintaining the Program Elements

5.4.1 Maintaining Policies and Procedures. Policies, procedures, standards, and guidelines are the foundation of the IS program. If the foundation is not maintained, the program will become ineffective. Policies must be reviewed periodically to ensure that they continue to provide guidance and a strong foundation for the program.

The need for policies, procedures, standards, and guidelines may be identified by the IS self-assessment and by reported damage to information assets (incident reports).

Baseline Program Recommendation

Perform the following policy review steps once per year.

1. The IS team should assess the current environment.
   a. Determine if there have been changes in organization culture.
   b. Repeat the information self-assessment to determine if there have been changes in the quantity or type of organization information.
   c. Determine if there have been changes in the level of control allowed in the organization.
   d. Determine if there have been changes in the original audience.
   e. Follow up on incident reports to determine if improper policy guidance caused the incident.
   f. Determine if there continues to be a real business need to give employees guidance.
2. Once the current environment is known, the IS team should identify its impact on policies.
   a. Determine if there is a need to revise the objective.
   b. Determine if there is a need to revise the scope.
   c. Determine if there is a need to revise the purpose.
   d. Determine if there is a need to revise responsibilities.
   e. Determine if there is a need to revise the group exempt from requirements.
3. Once the above is known, the maintenance process can be completed.
   a. The coordinator should make required revisions.
   b. The coordinator should have the IS team review the revisions and provide comments.
   c. The coordinator should include accepted comments.
   d. The coordinator should record the revision date on the document.

e. The coordinator should obtain management approval for revisions.

5.4.2 Maintaining the Awareness Program. As with other areas of the IS program, awareness is not an event — it is an evolving process. Employees need to be reminded periodically that information must be protected. They also need to be reminded of the methods to protect information. New employees that have not attended earlier awareness sessions will need to be introduced to Information Security.

The utility business environment will continue to change. Deregulation an re-regulation will require changes in the way companies do business, changes in their information, and as a result, changes in the awareness message that reflect the new environment.

The Corporate Information Security Coordinator will continue to develop the tools that can be used by the organization for its employee awareness program.

Baseline Program Recommendation

1. Use the results of recent information assessments to identify new problem areas in the organization. Use these problem areas as new topics for awareness sessions.
2. Include changes in policies or the program topics for an awareness session.
3. Add topics that reflect recent changes in information technology.
4. Ask management for additional awareness topics.
5. Include the updated awareness session schedule in the Organization Information Security Plan.
6. Contact the Corporate Information Security Coordinator for assistance in maintaining the awareness program.

5.4.3 Maintaining Information Security Controls. Ongoing changes in the information environment and information technology will require that Information Security controls be revised to keep up with these changes. Both management controls and technical controls need to be maintained. Maintaining management controls in the form of policy and awareness are described above. Maintaining the business continuity plan type of management control and maintaining other technical controls are described below.

5.4.3.1 Maintaining the Business Continuity Plan. The business continuity plan (BCP) must be reviewed and revised to keep it applicable to the changing environment. The last section of the plan, entitled "Maintaining the Plan," should describe the plan maintenance procedures. The plan must also be exercised periodically to determine if it still has its intended effect.

Updating the Business Impact Analysis

The business impact analysis (BIA) must be revised as the environment changes.

How-to:

1. Determine if there have been any changes in the organization's critical business functions.
2. Determine if there have been any changes in the priority of the critical business functions.
3. Determine if there have been any changes in the length of time the organization can do without each critical business function.
4. Determine if there have been any changes in the resources, especially information resources, required to support the critical business functions.
5. Estimate the tangible and intangible impacts on the organization of loss of each critical business function, being sure to include any changes.

Updating the Business Continuity Plan

Each of the four sections of the business continuity plan must be reviewed and revised periodically.

How-to:

1. Review the Preventive Measures documented in the plan. Focus on changes required in the actions that should be taken *before* a business disruption occurs.
2. Review the Continuity Measures documented in the plan. Focus on changes required in the actions that should be taken both *during and after* a business disruption occurs.
3. Exercise the Entire Plan. If that is not practical, exercise portions of the plan periodically. Document the results of the exercises. If exercising the plan does not give the desired results, revise it as required and reschedule the exercise. Continuity plan exercises should be documented in the Organization IS Program Plan schedule.
4. Review the procedures to Maintain the Plan. If the plan is not being properly maintained, revise the plan maintenance procedures to correct the problem.

Baseline Program Recommendation

1. Periodically review your organization's primary goals or objectives.
2. Periodically update the Business Impact Analysis.
3. Periodically update the business continuity plan.

Additional information on business continuity planning can be found in Chapter 21 or by contacting the Corporate Information Security Coordinator.

5.4.3.2 Maintaining Common Technical Controls. Technical controls such as virus scanners, backups, and access controls are initially selected depending on the target information environment. Over time, the target environment changes. As a result, the existing environment must be reviewed periodically. Where changes have occurred, the technical controls must be reviewed to determine if they are still protecting the target environment.

Baseline Program Recommendation

1. Refer to the results of the last information risk assessment to identify the target information environment and the technical controls implemented at that time.
2. If the target environment has changed significantly, another risk assessment should be performed and the technical controls revised.
3. If the target environment has not changed significantly, the current technical controls should be reviewed to determine if they are still effective.
4. Ineffective controls should be updated or replaced by new controls.

5.4.4 Maintaining Program Effectiveness Monitoring. Effectiveness monitoring, or compliance monitoring, must be continuous in order to provide feedback on the program. Again, two areas should be monitored for effectiveness: the Information Security program and the IS controls that have been implemented.

The Organization Information Security Program Plan (Chapter 21) contains objectives and goals. The program's effectiveness in achieving these goals should be monitored.

Baseline Program Recommendation

1. Review the plan goals and verify that they are measurable where practical.
2. Check that progress toward goal milestones continues to be monitored.
3. Check that progress is being reported to management.

Compliance monitoring and enforcement are necessary to determine the effectiveness of the controls and to let employees know that compliance is being monitored. Also, a method is needed to report incidents where information has not been adequately protected. Last, there should be some method to provide rewards for compliance, additional awareness for initial noncompliance, and reprimands for continued noncompliance.

Baseline Program Recommendation

1. Review the methods being used to monitor control effectiveness and employee compliance.
2. Review the effectiveness and attendance of the awareness sessions.

3. If used, review incident reports, their effectiveness, and the methods used to follow up on them. Also, check if employees are using incident reports to describe ineffectiveness of management controls or technical controls.
4. Review methods used to provide rewards and recognition to employees and groups that effectively protect information and comply with controls. Where recognition is not effective, determine why.

For additional advice on compliance monitoring, contact the Corporate Information Security Coordinator or the General Auditor. The Organization Information Security Coordinator should be notified of any special problems or need for additional support.

Chapter 22
Appendix

1 INFORMATION HANDLING PROCEDURES MATRIX

1.1 Printed Information

Confidential	Internal Use	Public
Labeling of documents		
Document should identify owner and be marked "CONFIDENTIAL" on cover or title page	No special requirements	Document may be marked "PUBLIC" on cover or title page
Duplication of documents		
Information owner to determine permissions	Duplication for business purposes only	No special requirements
Mailing of documents		
No classification marking on external envelope; "CONFIDENTIAL" marking on cover sheet; confirmation of receipt at discretion of information owner	Mailing requirements determined by information owner	No special requirements
Disposal of documents		
Owner observed physical destruction beyond ability to recover	Controlled physical destruction	No special requirements
Storage of documents		
Locked up when not in use	Master copy secured against destruction	Master copy secured against destruction
Read access to documents		
Owner establishes user access rules; generally highly restricted	Owner establishes user access rules, generally widely available	No special requirements; generally available within and outside company
Review of document classification level		
Information owner to establish specific review date (not to exceed one year)	Information owner to review at least annually	No special requirements

1.2 Electronically Stored (Computer-Based) Information

Confidential	Internal Use	Public
Storage on fixed media (access controlled)		
Unencrypted	Unencrypted	Unencrypted
Storage on fixed media (not access controlled)		
Encrypted	Unencrypted	Unencrypted
Storage on removable media		
Encrypted	Unencrypted	Unencrypted
Read access to information (includes duplication)		
Information owner to authorize individual users	Information owner to define permissions on user, group, or function basis	No special requirements
Update access to information		
Information owner to authorize individual users	Information owner to define permissions on user, group, or function basis	Information owners to define permissions
Delete access to information		
Information owner to authorize individual users; user confirmation required	Information owner to define permissions on user, group, or function basis; user confirmation required	Information owner to define permissions
Print hardcopy report of information		
Output to be routed to a predefined, monitored printer	Information owner to define permissions	No special requirements
Internal labeling of information at the application or screen/display level		
Notification of "CONFIDENTIAL" to appear at top of display	No special requirements	Notification of "PUBLIC" may optionally appear at top of display
External labeling of exchangeable media		
Media must identify owner and be marked CONFIDENTIAL	Marking at discretion of owner	No special requirements
Disposal of electronic media (diskettes, tapes, hard disks, etc.)		
Owner observed physical destruction beyond ability to recover	Physical destruction	No special requirements
Disposal of information		
Delete by fully writing over information	Delete files through normal platform delete command, option, or facility	No special requirements

Confidential	Internal Use	Public
Review of classified information for reclassification		
Information owner to establish specific review date (not to exceed one year)	Information owner to review annually	Information owner to review annually
Auditing access activity		
Log all access attempts; information owner to review all access and violation attempts	Log all violation attempts; information owner reviews as appropriate	No special requirements
Access report retention requirements		
Information owner to determine retention of access logs (not to exceed one year)	Information owner to determine retention of violation logs (not to exceed six months)	No special requirements

1.3 Electronically Transmitted (Computer-Based) Information

Confidential	Internal Use	Public
By fax		
Attended at receiving fax	Information owner to define requirements	No special requirements
By WAN		
Confirmation of receipt required; encryption optional	No special requirements; encryption optional	No special requirements
By LAN		
Confirmation of receipt required; encryption optional	No special requirements; encryption optional	No special requirements
By interoffice mail		
No external labeling on envelope; normal labeling on document	No special requirements	No special requirements
By voice-mail		
Confirmation of receipt required (sender); remove message after receipt (recipient)	No special requirements	No special requirements

Confidential	Internal Use	Public
By electronic messaging (e-mail)		
Confirmation of receipt required; encryption optional	No special requirements	No special requirements
By wireless or cellular phone		
Do not transmit	No special requirements	No special requirements

2 GLOSSARY

Access: the ability of a subject to view, change, or communicate with an object. Typically, access involves a flow of information between the subject and the object.

Accountability: a security principle stating that individuals must be able to be identified. With accountability, violations or attempted violations can be traced to individuals who can be held responsible for their actions.

Audit: to record independently and later examine activity.

Audit Trail (Management Trail): the chronological set of records that provides evidence of activity. These records can be used to reconstruct, review, and examine transactions from inception to final results.

Authentication: the process of proving that an individual is who he or she claims to be. Authentication is a measure used to verify the identity of an individual and the ability of that person to access certain information.

Authorization: the granting of privileges to an individual, a program, or a process.

Backup: copying of data to a medium from which the data can be restored if the original is destroyed or compromised.

Business Continuity Plan: a documented and tested plan for responding to an emergency.

Classification: the process by which information is identified as to its level of sensitivity and importance to the company.

Confidentiality: a security principle that keeps information from being disclosed to anyone not authorized to access it.

Decryption: the act of making information readable by unscrambling the characters in a predefined manner determined by a private key; encryption makes the information unreadable.

Encryption: the act of making information unreadable by scrambling the characters in a predefined manner determined by a private key; decryption returns the information to readable form.

Guideline: recommended "how-to" instructions that support some part of a policy or standard.

Integrity: a Security principle that keeps information from being modified or otherwise corrupted, either maliciously or accidentally.

Modem: a device that connect computers or terminals via a telephone line.

Need-to-know: a security principle stating that an individual should have access to only that information needed to perform a particular function.

Network: a data communication system that allows a number of systems and devices to communicate with each other.

Password: a confidential sequence of characters used to authenticate an individual's identity, usually during a logon process.

Policy: high-level statement of the company's beliefs, goals, and objectives and the general means for their attainment for a specified subject area.

Privacy: a security principle that protects individuals from the collection, storage, and dissemination of information about themselves and the possible compromises resulting from unauthorized release of that information.

Privilege: a right granted to an individual, a program, or a process.

Procedure: required "how-to" instructions that support some part of a policy or standard.

Recovery: the actions necessary to restore a system and its data files after a system failure or intrusion.

Risk: the probability that a particular security threat will exploit a particular vulnerability.

Secrecy: a security principle that keeps information from being disclosed to anyone not authorized to access it.

Security: freedom from danger or risk.

Separation of duties: a security principle that assigns security-related tasks to several distinct individuals. Usually, each of them has the least number of privileges needed to perform those tasks.

Standard: mandatory statement of minimum requirements that support some part of a policy.

Trust: reliance on the ability of a system or process to meet its specifications.

User: an individual who or a process that has been granted access to a system or information.

Userid (or user name): a unique code or string of characters with which the system identifies a specific user.

Virus: a code fragment that reproduces by attaching itself to another program. It may damage data directly, or it may degrade system performance by taking over system resources.

3 INFORMATION IDENTIFICATION WORKSHEET

Organ.: _____ IS Coordinator: _____ Date: _____

Business Function	Priority (M, H)	Information Supporting the Business Function	Classification (CN, IU, PB)	Criticality (C, N)	Information *Owner* Name

Priority: H (high) = Business function is critical to group's Value Added Role; M (medium) = Business function of less importance to Value Added Role.

Classification: CN (Confidential): Could violate individual's privacy, reduce competitive advantage, or damage company.
IU (Internal Use): Used by employees to conduct business. Not to be released outside company.
PB (Public): Has been released to public through authorized channels.

Criticality: C (Critical) = High need to conduct important business functions; N (Normal) = Average need to conduct business.

4 INFORMATION RISK ASSESSMENT WORKSHEET

Information Type: _____ Business Function/Priority: _____/_____ Date: _____

		INTEGRITY Loss of Accuracy	AVAILABILITY Loss of Accessibility	CONFIDENTIALITY Unauthorized disclosure
Accidental nature, errors, omissions	Threats			
	Vulnerability			
	Loss Impact			
	Proposed Controls			
Intentional voluntary, malicious	Threats			
	Vulnerability			
	Loss Impact			
	Proposed Controls			

Threats: Number of events or activities that could possibly occur to jeopardize the integrity, availability, or confidentiality of the information: Low = few; Medium = some; High = many.

Vulnerabilities: Likelihood that the identified threats could cause loss of integrity, availability, or confidentiality: Low = unlikely; Medium = somewhat likely; High = very likely.

Loss Impact: How the loss of integrity, availability, and/or confidentiality could adversely affect the business. Each level should be quantified in dollars where possible. (Sample scale: Low = <$1000; Medium = $1000 to $10,000; High = >$10,000.)

Low = _____ Medium = _____ High = _____

Proposed Controls: Controls that will remove or minimize the information's vulnerability to a threat.

5 SUMMARY AND CONTROLS WORKSHEET

Organ.: _____ IS Coordinator: _____ Date: _____

Information (Type or Description)	Classification (CN, IU, PB)	Criticality (C, N)	Vulnerability (L, M, H)	Loss Impact (L, M, H)	Bus. Func. Priority (M#, H#)	Proposed Information Security Control	Control Implementation Priority (#)

6 RISK ASSESSMENT: SELF-ASSESSMENT QUESTIONNAIRE

6.1 Information Security

Corporate information is defined as any and all facts, data, records, reports, news, programs, knowledge, and intelligence relating to The Company, its processes, business, customers, and employees. This includes, but is not limited to, information about employees of The Company and the technical data, and business information of the Corporation that The Company has not made available to its competitors, suppliers, and the public, whether manually or computer generated.

SELF-ASSESSMENT QUESTIONNAIRE

6.2 Information Security Standards

1. Have you read and do you understand the contents of the Information Security Policy?
2. Have you implemented the policies?
3. Have you noted and documented variations from ?
4. Have you noted and documented any other security exposures not covered by ?
5. Have you noted a variation from the policy or some other significant security vulnerability? Has it been resolved?
6. If not, is satisfactory progress toward resolution being made?

6.3 Information Classification System

7. Do you understand the Company Classification System?
8. Has all information within your area of control been classified?
9. Are required steps being taken to ensure that proper security is being afforded the information?
10. Is the level of security reviewed to ensure its adequacy?
11. Have local Company owner(s) been established for each application system and formally communicated to other employees as appropriate?
12. Has all Company CONFIDENTIAL information or material been properly marked to ensure proper handling?

6.4 Employee Information Security Awareness

13. Are employees periodically, informed of their information security responsibilities?
14. Has awareness of Information Security been disseminated to all levels of your department?
15. Has an Information Security Awareness Program (ISAP) been implemented within your area of control?
16. Is compliance to standards monitored periodically?

6.5 Records Management

1. Have you read and understood the various Records Management policies within the Corporate Retention Schedule?
2. Is your work area in compliance with the Corporate Retention Schedule for:
   a. Retention of records?
   b. Disposal of records?
3. Has your unit established Records Management for all media (i.e., paper, microfilm, electronic, etc.)?
4. Has the unit investigated and documented statutory and regulatory requirements for Records Management (Corporate Retention Schedule)?
5. Has your unit established guidelines for an annual purge?
6. Has your unit destroyed all records/information beyond retention, regardless of media?
7. Has the necessary hardware and software been retained to read all records/information stored in electronic media?
8. Has your unit instituted a hold on records/information subject to litigation or investigation and suspended regular Records Management practices?
9. Does your unit maintain a storage area for records/information that:
   a. Adequately protects them from adverse environmental condition?
   b. Controls access to the materials?
10. Are the records/information retained by your unit clearly identified (per Corporate Retention Schedule) as to:
    a. The type of information?
    b. Type of media?
    c. Its retention period?
11. Has an annual review been performed on records/information retained across all media to ensure integrity of the contents?

6.5.1 Specific Requirements

12. Are records/information in support of government business being retained in accordance with established Corporate Retention Schedule?
13. Has your unit selected a Records Management Coordinator?

6.6 Computer Security

1. Have all employees been informed that the Company management and the Corporate Audit Staff (per Policy) have the right to review, audit, or observe, at any time, all data files stored on:
   a. Company-provided computers?
   b. Computer storage media (i.e., diskettes, cartridges, tapes, reports, etc.)?

c. All data-processing resources used to support the Company business activity?
2. Have employees been informed that use of information-processing systems (including all owned, leased, and contracted services involving word processing, micro- and minicomputers, mainframes, and service bureaus) are to be used only to conduct authorized company business, unless otherwise documented by local management?
3. Have all incidents of unauthorized access or modification to computer information, unauthorized access to computer systems, or detection of the existence of computer anomalies such as viruses and Trojan Horses been reported to Information Security upon discovery?

6.7 Microcomputer Security

Microcomputer refers to desktop computing, whether that entails PCs, Macs, work stations, or stand-alones.

6.7.1 Administrative

1. Have employees been made aware of published standards for the use and security of their microcomputers?
2. Have employees been informed of their responsibilities and accountabilities for microcomputers and microcomputer data in their work area?
3. Has a Microcomputer Coordinator with responsibility for coordinating microcomputer use and microcomputer security been appointed for each work area?
4. Is a separation of responsibilities for data entry, computer operating, and programming maintained in the microcomputer environment?
5. Is adequate training provided for users?
6. Are users instructed in the proper care of microcomputer media?
7. Are users trained in security awareness and security procedures?
8. Are microcomputer users cautioned against copying proprietary programs?

6.7.2 Physical Security

9. Has the annual inventory of hardware and software been completed?
10. Is the equipment adequately secured against theft?
11. Are your policies and procedures relating to the removal of equipment or storage media in compliance with corporate policy?
12. Are microcomputers protected with power surge protectors, line filters, and uninterruptible power if processing critical applications?
13. Is backup storage media kept off site?
14. Are diskettes left in machines unattended?
15. Are diskettes labeled: contents, classification, department, and company id?

16. Are internal components protected from removal by lockable covers or similar devices?
17. Are reports, file layouts, file dumps, etc. locked up when not being used by authorized persons?
18. Has an anti-virus software package been installed on microcomputers where required?
19. Have employees been made aware of the Company's policy against the introduction of Public Domain (i.e., nonlicensed software, also called "shareware" or "freeware") or personal software into company-provided microcomputers?

6.7.3 Data Integrity

20. Is access control installed to protect data on hard disks from unauthorized access?
21. Is it possible to alter financial data without producing an audit trail?
22. Can outdated or incorrect files be inadvertently processed?
23. Is diskette access tightly regulated?
24. Can users create data for use outside their departments?
25. Is an access control system provided?
26. Is plain-text version of encrypted files deleted?
27. Are copies of all user-written production software, purchased software, and all data files stored off site?
28. Have all applications and macros been properly documented?
29. Has microcomputer utilization been approved by management?

6.7.4 Miscellaneous

30. Has the department developed an alternate processing plan (Business Continuity Plan) in the event that normal processing capabilities are unavailable?
31. Have local procedures been developed to control use of portable PCs?
32. Is the log of portable equipment and its location current?

Index

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U