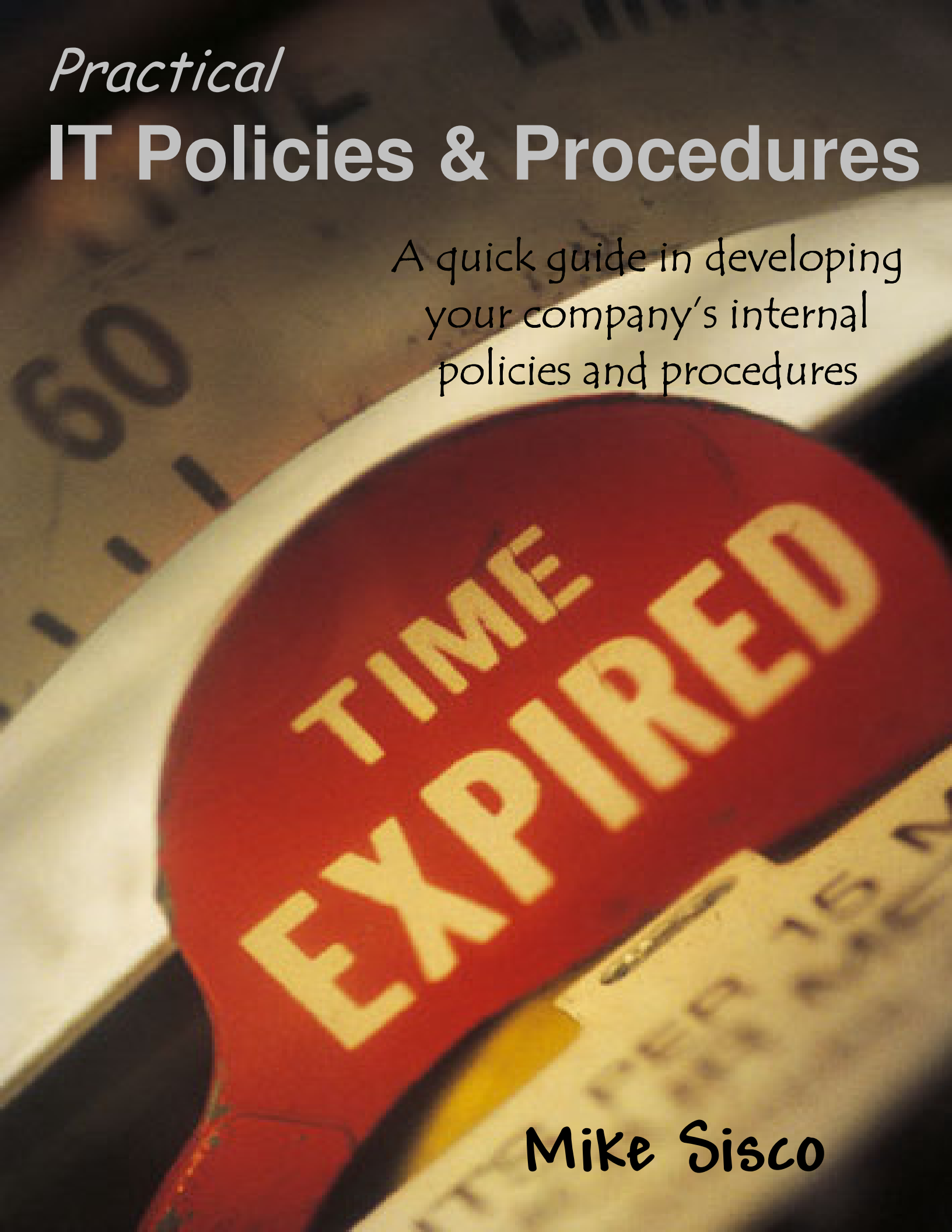
Practical

IT Policies & Procedures

A quick guide in developing your company's internal policies and procedures



Mike Sisco

Practical
IT Policies & Procedures

by Mike Sisco

MDE Enterprises
www.mde.net

Introduction

Practical IT Policies and Procedures has been written to give you a quick approach to developing your internal company IT policies and procedures (P&P). Included in the book are guidelines for developing, maintaining, and communicating the P&P's you develop plus there are many samples that you may find useful for a "quick start".

The sample policies and procedures contained in the book are provided only as examples and should not be considered to be complete for your unique situation. Any time you develop a policy, you must take your company's specific issues and environment into consideration. You may use any of the samples as you determine appropriate but in all cases you must take full responsibility for the impact they have in your specific business operation.

It is highly advisable to have your Human Resources Department and legal resources review any new policies and procedures you develop before implementing them. Having their insight will prevent problems and is well worth the effort.

Two tools are used to enhance the material:
Sidebar: *an example or additional information provided to clarify a point.*
Personal Note: *a personal experience or "war story" to reinforce a point or concept.*

Managing organizations at a high level is serious business, and having fun along the way is half the battle. I hope you find the material helpful in your quest and I welcome your feedback. You may contact me at mike@mde.net.

Practical IT Policies and Procedures complements the ten books initially written for my **IT Manager Development Series**. This book and all the others were written to provide a practical perspective, senior management level insight, and "how to" instruction to help any IT Manager achieve more success. To learn more about MDE's other IT Manager publications, log onto www.mde.net/cio .

MDE Enterprises also provides the most comprehensive and practical curriculum of IT Manager education to help IT Managers achieve more success. For more information, go to www.mde.net/schedule for program topics and schedules.

Best of success,

Mike Sisco

Table of Contents

I. Are policies and procedures necessary ? 6

II. Objectives of policies and procedures 9

III. A quick process for developing policies and procedures 14

IV. Components of a good policy 17
- Policy name
- Objective
- Applies to
- Key guidelines (the policy and/or procedures)
- Who to ask for clarification
- Last revision date
- Samples for clarification

V. Keep it simple 21

VI. Pay attention to the targeted audience 24

VII. Implementation tips 27
A. Do your homework
B. Be consistent
C. Be "net" when writing the introduction
D. Why format is important
E. Communication methods

Table of contents (continued)

VIII. Sample IT Policies and Procedures 32

IT_01 Email and Instant Messaging 34
IT_02 Internet usage 37
IT_03 Password security 39
IT_04 Intranet usage 41
IT_05 Phone usage 44
IT_06 Building security and access 49
IT_07 Software usage 51
IT_08 PC software standards 54
IT_09 Travel and entertainment 58
IT_10 Employee conduct 67
IT_11 Employee non-compete 71
IT_12 Employee non-solicitation 73
IT_13 Performance plans and reviews 76
IT_14 Training and reimbursement 79
IT_15 Working from home 81
IT_16 Inventory and equipment 84
IT_17 PC standards 86
IT_18 Equipment requests (Adds, Changes, Deletes) 88
IT_19 New employee startup 91
IT_20 Information security 95
IT_21 Remote access 100
IT_22 Privacy 102
IT_23 Service level agreements 104

IX. Enforcing your policies 106

X. Policy and Procedure Resources 107

XI. Conclusion 109

Appendix A Terms 110

I. Are policies and procedures necessary ?

The question I get a lot is, "Are policies and procedures really necessary?" Many companies, especially smaller ones, seem to operate just fine without them. In fact, if you were to take a poll I would say that the majority of companies in the world do not have formal policies and procedures.

The decision of whether your company needs formal policies and procedures depends upon the risk or exposure not having them has on your company. The issues surrounding a company of $500 million or $1 billion in revenue are much different than that of a company with $5 million in revenue.

I'm the first to suggest that if there is limited exposure or risk related to an issue in your business, don't spend the time and money to develop formal policies and procedures. You have to sit down for yourself to determine the level of risk that might pose a liability for your company and you should do so for every major issue.

I really think there are two or three compelling reasons to develop formal policies and procedures for your company.

1. Eliminate or minimize risk
2. Establish a desired behavior or process you want followed
3. Educating employees

Beyond these three issues, I don't find justifiable reasons to spend the time and effort required to implement, monitor, and enforce formal guidelines.

Every company situation is different so use your best judgement. The real point with this material is to provide you with a "practical approach" by which you can evaluate the extent you should implement formal policies and procedures in your company.

There are two ways to look at this issue. First, you can assess the negative aspect of liability or risk exposure and make a decision from that standpoint. Another way to look at the issue of whether to develop P&P's for your company is to look at the potential benefits formal P&P's might offer.

The real point with this material is to provide you with a "practical approach" to look at policies and procedures for your company.

It is far better to establish a culture that actually operates in the manner you want than to develop a lot of policies and procedures that say one thing but everyone in the company does something else. The important issue is how you actually operate.

Evaluating risks
To evaluate any liability exposure, you need to determine the type of things that can create a liability. In today's litigious society (people and companies like to sue one another), the bigger your company becomes the more exposure you have.

Sure, there are legal devices that can help protect your assets and minimize liability, but you still have the possibility of dealing with a lawsuit. This requires time and money. Losing either of these assets (time or money) is a liability exposure.

There are many issues in our business world that can create liability. Putting formal policies and procedures in place is one way to protect you from many of these nuisances by.

Are you aware that Officers of a company can be financially liable for unauthorized use of software when an employee loads pirated software onto his/her work PC, , , even without the Officer's knowledge?

Putting a policy in place, communicating it, and enforcing it with employees is one way to reduce or eliminate your exposure in such a situation.

Personal note: In a company acquisition, my IT due diligence discovered the fact that the company we were acquiring had considerable software compliance issues. In the Due Diligence Report I wrote, it included this issue as well as my estimated costs of getting the business compliant once the purchase was completed.

Three weeks after we closed the deal, our company was contacted by an outside agency about unauthorized use of software. Fortunately, I was able to pull out the Due Diligence Report and show them that I had identified several things:

1. Quantified the problem.
2. Included in the budget model the cost of rectifying the problem.
3. Included in the immediate transition plan my planned action to take care of the problem within 60 days of acquiring the company.

Having this information readily available saved our company considerable problems as the agency simply dropped it and only required me to send copies of invoices that validated our follow-up actions to resolve the issue.

By the way, the agency was contacted by a disgruntled employee who lost his job as a result of the changes made in the acquisition transition.

It only takes one phone call to cause lots of problems unless you have a policy and procedure in place to offset it. That's exactly what my IT Due Diligence Report provided for me and my company in the example discussed above.

Another type of risk deals with safety. Putting policies and procedures into place that protect worker safety is not only important, it is every company's obligation to take care of its employees when known safety issues exist.

Benefits
If one of the reasons to develop formal policies and procedures is to reduce or prevent risk, another reason is to take advantage of benefits they can provide your company.

Benefits can come in many forms. Obviously, as we have just discussed, the opportunity a policy and procedure provides in reducing employee injury or mitigating other liability issues is a benefit to the company.

Other benefits are there for the taking as well. For example, getting all your people to follow a desired process can boost employee productivity, improve relationships between departments, even boost morale.

Another benefit is that policies can actually be used to help educate your new employees with the company. That's why I try to develop policies and procedures with the audience in mind. Make the effort to make your policies and procedures easily understood and that make sense to your employees.

When you include Best Practices in your procedures, you create an opportunity of enhancing your company's image with clients and employees alike. For example, the outside world sees thousands of email messages from your company's staff and officers. You should consider including Best Practices guidelines in your email policy that promotes professional use of email and electronic correspondence.

There are many benefits in having your employees follow guidelines that promote productivity, reduce risk, protect assets, etc. Use the management tool you have in implementing policies and procedures wisely and judiciously. It can make a tangible difference in your company and can reinforce the professional atmosphere you are trying to maintain.

II. Objectives of policies and procedures

Every policy and procedure you develop should have a clear set of objectives. Otherwise, it's not worth the time to develop them.

The three general areas we discussed that warrant developing a formal policy include:

- Avoiding risk
- Establishing desired behavior
- Educating employees

You may have more reasons you think should be included in these three areas. If so, add them. Remember, they are going to be "your" policies and procedures so they should reflect what "you" want and need for "your" company.

When you begin developing a particular policy and procedure, you should state a specific objective. In other words, what should this policy and procedure accomplish?

In my opinion, the more specific you can be the better. Stating your specific objective highlights the purpose and helps the reader "get it". There is no need for a subtle message here nor do you want to trust that the employee (reader) will get your "subliminal" message.

One of the sections in the policies and procedures that I develop and have included in the samples within this publication is the ***Objective*** section. It is one of the first parts to be read as it establishes exactly what you want from the policy and procedure.

Let's discuss more about the idea of establishing desired behavior. Don't underestimate the power that policies and procedures might offer you in getting people to behave the way you need them to.

For example, if you are having a particularly difficult time getting people to follow a process you know will improve productivity, improve quality of service, or enhance client satisfaction, maybe you should think about developing a formal policy to create a stronger emphasis in "working this way".

I know that I've done this in small companies that had no formal process of managing programming change requests and delivery of those changes. When you encounter a "loose" culture where department managers like to make programming requests at the water cooler and don't want to be involved, it often takes stronger measures to convert the culture to one that can be productive and more predictable.

Policies and procedures, whether formal or informal, can be an effective tool to help you convert the "non-believers" such as the example that follows.

Personal note: I've encountered several programming organizations that needed a "facelift". The scenario normally goes something like this:

- The programming staff is so busy trying to keep pace that the quality of their work is poor.
- Users aren't knowledgeable in the applications so their requests are often a waste of time or misdirected.
- Improving the quality of the work is perceived to take too much time which would be another negative to the User client base.
- The relationship between the User Department and IT is poor.

The bottom line is that the client service relationship is poor because quality is poor which leads to low productivity. Poor quality and low productivity kills efforts to improve client service.

Initially, I try to make the improvement without putting a formal policy in place. My attitude is that if I can make the change happen without a formal policy, I will usually try to take that approach unless there are significant risk implications.

When it doesn't work, I create a formal quality assurance policy within my Programming organization and with our user clients.

The policy and procedure establishes checkpoints along the project life cycle of delivering a programming request change. Quality problems at each of these checkpoints are tracked to help me determine where our quality problems exist.

Programming quality problems exist in one of the following areas:

- Requirements definition
- Design
- Programming
- Internal IT QA
- User QA
- "Live" production implementation

If you know where the problems exist in the life cycle of providing programming changes and enhancements, you know where to improve. When you improve quality, you almost always improve productivity.

Let's see now, what does this say?

If programming output improves with higher quality, don't you think the client service relationship will improve?

Yes, it does every time.

So, what's the problem?

The problem will be encountered within your own programming staff. Your senior programmers have helped put the process (to the extent there is one) in place and they evolved into this process thinking it is the best way to respond to their user needs.

Be sure to take note of this comment:
*The process that exists in the company evolved to this point with a **genuine desire** to serve the Client effectively.*

Your senior programmers are conscientious people. I always know that and respect it whenever I encounter this type of situation. The problem is that they don't know how to look at the programming delivery aspect in business terms. Essentially, their approach takes a "work harder" method as opposed to a "work smarter" method.

When I introduce a formal QA process within my IT group and suggest that we are going to "slow down" so we can "go faster", there is always this glazed over look in the eyes of my programming staff. Not only that, the senior members of the team will usually "push back" and resist the change stating that it's only going to make our relationship with such and such department worse since we will be getting less accomplished every month.

In at least one case when my selling skills didn't get agreement from my team, I had to ultimately put my foot down and state, "This is how we are going to do it for 90 days."

The result is always one of the best parts of being an IT Manager. When the backlog numbers start showing that we are having fewer quality problems and that more programming backlog hours are getting completed per month, you see the light bulb turn on in your senior programmer's eyes. It's a very gratifying feeling.

I only implement a formal policy to improve the quality of our services when I have to as mentioned earlier. There are times when the culture of how the staff is doing things is so entrenched that you have to take strong measures to get them to look at the situation another way, especially if you are the "new manager on the block".

In this example, the ***Objective*** I might state is to improve the quality of software change releases by 80%. Before I make such a bold statement, I will have gathered sufficient data to understand the level of quality issues that exist and know that the goal is achievable. It will be important to establish a baseline so your staff and Users can see the progress you will make.

I won't go into all the details of such a quality program, but there are many things that go into the procedure that will help you track issues, identify where to help specific people, and will actually give you the answer to your quality and productivity issues.

The point is that a formal policy can help you change the culture so you can improve.

Policies and procedures are not a "panacea"
Just because you have a policy in place does not mean you are "home free". You can document your position on an issue all day long, but it's irrelevant if you don't communicate and enforce it.

In order to help you create the "risk barrier", your policies must support how you operate. Remember me saying earlier that it is much more important to operate well than to have a formal policy that doesn't support how you run your business?

Policies and procedures are elements to support your business, they are not the answer. That's why I emphasize taking a practical look at them in terms of:

- To what extent do you need policies and procedures?
- Which policies and procedures make sense?
- To what level of detail do you need to develop them?
- What are effective means of communicating them?
- How do you inspect and enforce them?

Taking a "practical" look at how formal policies and procedures fit into your company means using your best judgement as to whether they provide tangible benefit. Don't spend your time developing them just because the company down the street has them. It's totally irrelevant what others have in place.

If you can't define the value that formal policies and procedures will provide in either mitigating risk or defining behavior you want followed, spend your time on more important issues.

With that said, don't take the path of simply ignoring the value of formal policies and procedures either.

We don't buy life insurance because we plan to die nor do we purchase auto insurance because we are planning to have an accident. We invest in these items in case we do.

The same principle is true for why we put formal policies and procedures into place. One difference is that certain policies and procedures can actually affect behavior and the way people conduct themselves and can be a proactive tool to help you create the culture and actions you want in your company.

An example of this is when you put into effect a software "change management" policy and procedure and enforce using it. By giving employees of your company the policy you expect them to adhere to and the procedures to follow, the entire company will gradually start using your process until it becomes second nature.

No longer will you continue to receive programming requests from unauthorized requestors and every request will include sufficient justification and approval. If you have ever worked in an environment that has no formal change management process in place for programming changes, you know what a difference this will make.

The bottom line here is that there are big benefits to the company. The users of business applications and the IT staff benefit because there will be a significant improvement in productivity in managing the programming backlog.

In addition, client service is enhanced when users, clients, and the IT Organization have a process of getting things done plus the guidelines that help everyone utilize the company's investment in technology support to best advantage.

Remember, the IT Organization is a company asset just like available cash is for your company. Companies work diligently to make the best use of cash and likewise they want to do the same in using its technology support assets.

Policies versus procedures
Policies are used to establish what it is you want while procedures are used to give employees the "how" you want the policy adhered to.

For example, a Programming Change Policy states the requirement you put in place to manage programming requests. The procedure part of the policy provides the specific steps to follow and the forms to use to help you train employees and create a consistent process.

In some cases, there may not be a procedure included in a policy. For example, a company's vacation policy is announced each year to identify the specific days holidays will be observed by the company. Policies like this normally do not include a procedure.

III. A quick process for developing policies and procedures

Let's get started. In my books, you will find that I don't waste a lot of time. My belief is that if you can get your message across in 40 pages versus 240, then you should save the paper and the time required to read all the extra "stuff".

The following section is a simple process you can use in determining the policies and procedures you should develop for your company. Later in the book, there 23 samples you may use to get off to a fast start in developing them for your company.

Step 1 - List areas of risk
So, let's take a shot at listing things that can cause a company risk. Here are just a few to get you started thinking:

- Software licensure compliance
- Employee safety issues
- Security
- Data backup and recovery
- Illegal access to company systems
- Infringing on privacy
- State and federal regulatory issues
- Email spam
- System viruses
- Company confidential information
- Losing clients
- Systems downtime
- Inappropriate use of company assets (equipment, facilities, money, etc.)

One company may consider all of these issues worth the time to develop formal policies and procedures while a similar company of comparable size and in the same industry may consider just a few worthwhile for its company.

I will keep emphasizing that what's important and useful for one company may be very different from another. That's the "practical" application of reviewing your situation and deciding for yourself what's important for your company.

Step 2 - List desired behavior or processes you want
List the processes you want and the behavior that's important to a smooth running operation. Don't worry about whether it has policy and procedure ramifications; we will discuss that part later. For now, simply start listing things that are important in the operation of your company that you truly think make you more productive or better at what you do.

Here is a quick list of items to consider:

- Programming change requests
- Vacation and time off requests
- Purchase authority and approval
- Equipment change requests
- Travel expense management
- Employee performance planning and reviews
- New employee orientation and quick start guidelines
- IT escalation steps to resolve downtime issues
- Use of company cell phones

Step 3 - Assign a "relative importance factor"
Step 3 is to assign a relative weight of importance to each risk issue or desired behavior so you can decide on whether you want to put in a formal policy and procedure to address the issue.

This step is somewhat subjective. Actually, it's very subjective and reinforces what I have been saying. It's "*your"* company and the determination of whether a risk issue is important or potentially tangible enough to cause you to decide to develop a formal policy and procedure is up to you.

It's the same as buying life insurance. Some of us prefer to have a lot while others go with much less. Who is right or wrong? I'm not so sure there is one person more right than the other; everyone's situation is different. Companies are all unique as well.

Once you identify the policies and procedures that are important enough to develop formal documentation for your company, you can determine how to develop them.

Step 4 - Define the list of policies and procedures you need
Identify a specific policy and procedure that addresses the risk or behavior issues you have deemed to be of major importance in Step 3.

For example, if your company is having difficulty in managing travel expenses, you may decide to develop and implement a formal *Travel Expense Guidelines* policy.

Step 5 - Prioritize your list of policies and procedures
Spend time on your most important policies and procedures first. One way to determine importance is to develop an estimated dollar value for the risk exposure or estimate the value of improving productivity or reducing costs by implementing a policy to address a specific issue you have identified to be important.

The point is that you want to focus your priorities on the issues that give you the best return on your time investment as possible.

Step 6 - Determine how you will develop your policies and procedures
There are essentially three ways to approach this task:

1. Write them yourself.
2. Obtain copies from a company in your industry to use as a starting point.
3. Research sources for examples to provide a starting point.

It's important to remember one of the comments made earlier. You must take full responsibility for the content of any policy or procedure you develop. It is simply not enough to take one that addresses for example a *Company Travel Expense Policy* from a company and use it "as is".

Every company has unique situations and whenever you decide to develop a policy or procedure, you need to consider your unique issues. Only you and others in your company can take the responsibility for the policies and procedures you implement.

Step 7 - Develop and implement your policies and procedures
There are three important aspects from this point forward.

1. Assign responsibility for writing each policy and procedure with deadlines, objectives, and important points that should be included.
2. Define your review process: who, how, when, review criteria, etc.
3. Define your implementation or "roll-out" process. This will probably be different for different policies and procedures. More will be discussed in a later chapter when we discuss *Implementation Tips*.

Step 8 - Monitor and enforce your guidelines
It really doesn't do a lot of good if you document what you want to happen but don't enforce your new guidelines. In fact, it can do more harm than good if employees of the company perceive your company is not really serious. You want to be certain that if you decide to develop a formal guideline and introduce it to the company that the company is prepared to back up what it says.

More will be discussed in the *Implementation Tips* section.

IV. Components of a good policy

The elements that make a good policy and procedure are similar to what makes a good book, a good project plan, or any other document. I believe the key to developing any document of real value is that it accomplishes several things:

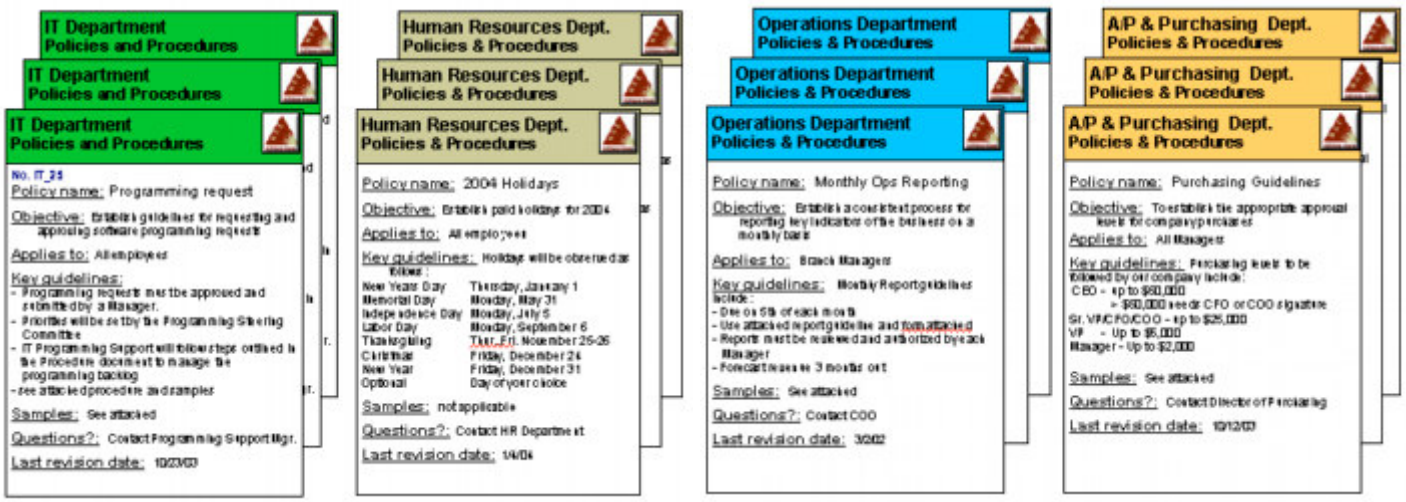
- gets to the point
- keeps it simple
- has a clear message
- it is organized and easy to follow

Policies and procedures must be easy to follow or you won't get the results you want. A rule to remember is: "If I can't understand it, I won't follow it."

I recommend you include several parts and use the same template for all your policies and procedures. Depending upon the size of your company and the preferences of senior management, you may use different formats for different departments of the company. However, the more consistent they are the more you create easy recognition.

One suggestion is to use different color schemes for the different organizations in your company but try to keep the content format structure the same. That way, employees will be able to quickly recognize two things:

1. This is a policy or procedure.
2. The color scheme defines which department authored it.



I include several parts in all of my policies. These sections help you organize the content that is very important for easy reading, and it helps you present your policies consistently.

Presenting them consistently is more important than you might realize. When you send out a policy to a thousand employees or more, you want immediate recognition that this is an important document from the company and management team. Establishing a standard "look" and a consistent format early on makes these documents very visible and more likely to be read because employees will quickly recognize them as an important company document.

Use your creative ideas here. Policies don't have to be boring, terribly written documents that no one wants to read. In today's progressive world, your policies should reflect the culture of your company. If that culture is a business suit environment, you may strive for a more formal look and style. If your company goes to work in jeans and company t-shirts, a more casual approach will work just fine.

The point is that company documents that address your employees should reflect the business image your company portrays. Be consistent with both the format and look of your policy documents and use them to reinforce who you are as a company.

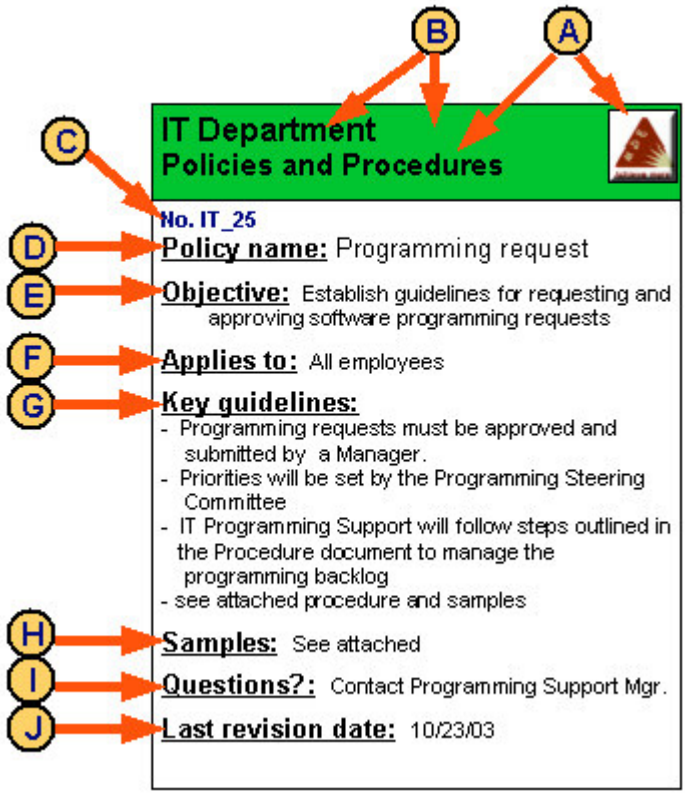
I typically use the following sections in policies developed for my company:

- Policy name
- Objective
- Applies to
- Key guidelines (the policy and/or procedures)
- Samples
- Questions (Who to call for assistance)
- Last revision date

These sections of the policy provide the content of the policy. However, in the sample we will discuss, there is much more to the policy document that will help you achieve its objectives

Let's break each part of a sample policy and procedure down and discuss how each piece works in helping you get the message across as simply and effectively as possible.

This is just an example of one way to organize and structure your policies. Remember, your personal preference is important as long as you try to be consistent with other departments in your company.



A. Company logo and "Policies and Procedures" title
In "my example", the Company logo and the title, Policies and Procedures identifies the document as a company endorsed product and exactly what it is.

B. Banner color and Department name identify the source of the policy
In "my example", I use the color green and part of the title to identify this as a policy that comes from the IT Department.

C. Policy Reference ID
Reference ID helps identify the policy. I like to use the Department ID such as "IT" as part of this identifier for easy reference.

D. Policy name
Give every policy a short descriptive name. Be as specific as possible to help others understand what it is.

Consider whether you will want to organize your policies by Policy Name in either an index or file folder. If so, the Policy Name takes on additional significance.

E. Objective
State the specific objective you are trying to achieve. Be as clear as possible to achieve the desired objective you have for implementing this particular policy.

F. Applies to
Tells everyone to whom the policy is addressed. It may be directed to only managers, a specific department, or all employees. Here is your chance to make it clear.

G. Key guidelines
This is the substance of your policy. My preference is to put the guidelines in short and simple bullet format and to use supporting documentation as needed. The essence of what you want to accomplish here is to get across the key thoughts surrounding the policy. Use whatever level of detail you desire, but remember that an effective policy does not have to describe every aspect of your issue in excruciating detail.

State the guidelines and keep it simple. More people will read what you have to say.

H. Samples
Identify appropriate samples that help the reader understand the policy and procedure. You may include samples as an attachment to the policy, list a web page link to your company Intranet, or point to a document or page in an internal company manual.

I. Questions?
This tells the reader where to go if he or she has questions about the policy. Be as specific as possible to avoid wasting your reader's time in finding the answer to their question. This might include a FAQ (Frequently asked questions) section on your Intranet, or it could be the sponsor/owner of the policy. It is usually wise to list a position and phone number within a department than a person's name to avoid having to update the policy in the case of turnover.

J. Last revision date
Including the most recent revision date helps you insure you are discussing the latest and greatest document pertaining to the subject. It will also help you monitor whether certain policies are still appropriate based upon changes that have occurred with the company, technology, or other elements of your business.

If you do some research on sample policies and procedures used by companies and organizations, you will find many different formats. They probably all work. My emphasis is that you should keep your message to the point and organize it in a way so that when someone reads it, they are familiar with your approach because it's consistent throughout the company.

My personal belief is that when you put good, prudent thought into developing a policy, it's hard to go wrong. However, it's probably more damaging when you "over kill" the issue by developing too many policies than it is to have too few. Too much can create a "stifling" environment.

Use them wisely and judiciously. Policies and procedures can be valuable tools but used to an extreme will have a lessening effect on those you are trying to reach.

V. Keep it simple

I believe keeping things simple is important in most of what we do. How many times have you been in a conversation with someone that talks endlessly about a subject and could have easily gotten the point across in about six to ten words?

Documents that you need to read are the same.

When writing articles for a publication, I review and edit my finished article several times to try to "tighten it up". People want the answer and not necessarily all the "stuff" that you could expound on for hours to support the answer.

When they get the answer, they will seek out the supporting information if it's important for them to know it. Or, at least, that's what I think most of us do.

When writing your policies and especially when developing a process or a procedure, the simpler you can make it the better. Get to the point, make your case, and move on.

Sidebar: One of the things I tell managers that report to me is that when I ask questions, I'm usually looking for the answer. I don't need to know the inner workings of a Swiss watch to understand what time it is. Just give me the answer to the question and any extraordinary issues that are significant for clarification and we can move on, , , and move on faster and more productively.

In developing a young manager, I have to be able to let him/her make mistakes. You aren't empowering them if you continue to make all the decisions. The key is to help prevent a new manager from making the catastrophic mistake that causes significant damage or possibly ruins a career.

Policies and procedures are similar to the extent that they don't have to spell out every possible scenario that might happen within a given subject area.

It's especially true when you are developing policies for the first time. Strive to hit all the critical issues that address 80% of the possible issues you might encounter. I'm sure you have heard of the 80-20 Rule. Spend 20% of the time it takes to address 80% of the issues. You will be much more productive and very well may find that the new policy works exceedingly well for you.

Plus, you can always revisit a policy and tighten it up later as needed.

There are two important thoughts to remember in this regard:

1. People do not require every "i" dotted and every "t" crossed as long as you address the critical issues that allow the policy and procedure to be effective.
2. Try to include every possible aspect of detail and you may never finish.

"Keeping it simple" entails several aspects of writing, some of which we have discussed but worth repeating:

- The format should be easy to read and look neat and organized.
- Bullet points can be very effective.
- Work on your writing style to be "net". Short and simple statements are good. Not only that, they can be much more powerful.
- Be sure to edit your work for a logical flow.
- Walk through your procedures and test them. Be sure they actually work.

Writing effectively is not easy work, especially for most of us. If your writing style is weak, find someone in the organization that does a decent job of writing. A quick interview with an employee with more capable writing skills where you lay out the key points to be included in a policy can be a very good way to develop a polished product.

Another way is to jot down the bullet points and give them to your writer. You can edit the draft and fine tune the finished work.

Getting others involved in developing policies and procedures for your department can be a rewarding initiative for your employees. Before you choke on this statement, let me assure you that if you are a respected manager, employees will jump at the chance to work more closely with you on such a project, especially if you value the importance of such a project.

I have used employees in my organization to develop a core set of policies and procedures upon joining a new company and finding there were no processes in place. I always take the lead role in defining the policies we need but will assign specific policy development initiatives to employees to give them a chance to be involved and an opportunity to work directly with them.

One caution is that you normally have to help your employee manage the scope of the project. They may try to put more into the policy and procedure than what's needed.

All right then, how do you go about determining the right level of detail that should go into a new policy and procedure?

Simple question that has an answer of, "It depends."

Before you start thinking I'm "copping out" on you, here is what I mean. Every company situation and IT Organization you encounter will have very different dynamics. It's sort of like handling children in that one response or way of handling one son or daughter will not necessarily work for your other children.

When I encounter a new company situation, I will approach that business the same way I approached my last company - I start assessing the situation. Where the assessment leads to can't always be predicted fully.

For example, I may know early on that a software change process is non-existent and that quality improvements are badly needed. That's the easy part. But what it takes is time to learn whether the IT Organization is able to respond to new direction or whether I will need to establish a formal policy to help me change the existing culture and point the staff in a direction that improves the delivery of software.

I'll use a formal policy as the last resort, but if the situation is bad enough I will implement a policy and procedure quickly to get us on a positive path. In other words, I don't wait too long to determine whether the staff is going to respond to my coaching.

Your staff may not have the experience or knowledge to make the turn, even with your coaching. If that appears to be the case, let's install a policy that helps us make the turn sooner than later.

Client relations are dependent upon seeing positive change in the organization and a structured policy and procedure applied correctly can be a big help.

VI. Pay attention to your targeted audience

One of the sections we discussed that I include in the policies and procedures I develop is the ***Applies to*** section. This identifies the target audience you are essentially writing the policy for.

What do I mean when I say, "Pay attention to your targeted audience"?

Let's break it apart and it will become much clearer.

In the process we discussed to help you identify and develop a policy and procedure, we identified reasons as to why we needed certain policies. Those reasons were to solve something such as to reduce risk, create a desired behavior, or to achieve a certain benefit that following a policy and procedure would provide.

As we develop a policy, we determine who the policy affects. As we mentioned, it might be a certain type of employee such as all managers, it could be used only for a certain department of the company, or it might affect all employees of the company.

This determination essentially defines the ***Applies to*** "target audience".

Now that we know who the target audience is, we should step back a bit before jumping in and starting to write the policy. It will help you reach your target audience if you consider a few things as you prepare to develop the policy and procedure.

Ask questions such as:

- What does this group react well to?
- What types of things are important for this group?
- Is there a good way to structure the policy and procedure that helps this group?
- What will this group need relative to this particular policy?
- Are there implementation strategies that will help the group incorporate the policy and procedure?

You want to write a policy with your targeted group of people in mind so they will understand the objective of the policy and the guidelines you are establishing. Pay close attention to how they will react to the policy when it's announced. You can make the entire process a much more pleasant experience when you anticipate the receptivity and needs of your target audience.

Let's run through a couple examples.

If your policy is directed toward managers only, structure the policy and procedures in a format that would help you understand and implement the yourself. Write it in a language that "speaks" to other managers, in management language, and at a level that gets a manager's attention.

For example, managers do not need all the detail in the world to follow a guideline. State your points in direct fashion and give them a contact to call if there are questions.

If you believe the managers will likely send the policy out to employees, take this into consideration when writing the policy. Nothing will reduce your effectiveness more than writing a document that has even a hint of disparaging against employees thinking that only managers will see the document.

There is no need to degrade employees so don't. You will be much more effective when you write policies that embrace "partners" and seek collaborative efforts. Keep your policy objective and straightforward as much as possible. A good rule to follow is that "any policy may be read by anyone in the company".

If your policy is being directed to all employees in all locations of the company, your guidelines may have to be more general in nature or more detailed depending upon the nature of the policy.

An example of a policy that needs to be fairly tight and specific would be one that discusses password security in the use of the company's business applications. In this case, the policy probably pertains to virtually all employees and needs to be very specific as to what you expect to be adhered to.

In the case of a Software Usage policy to address compliance issues related to the use of software products, the policy may need to take on more of a general guideline that has a more global directive.

What does this group react well to?
When writing a new policy, consider the types of things or "hot buttons" that help the targeted audience respond well. We all have individual needs. Groups have needs as well.

If the group is all employees, your message has to take into consideration that all employees are affected and the content needs to be written so that they can all understand the guideline and why it was written.

If the policy is for your "Programming Staff", you can take some "short cuts" and use terminology they understand. You can also make certain assumptions of their level of understanding of a topic when you start writing a new policy guideline for them.

Try to look into the minds of your targeted audience for each policy and identify things you can do that will get them to respond positively. Remember, change is not always welcome by people so take the time to think through what is going to work for each new policy you deliver.

Receptivity can be impacted by what you include in the policy, how the policy is written, or how the policy is presented to them. In fact, delivery may be as much to impact receptivity as anything. We devote the next chapter to this topic.

What types of things are important for this group?
Managers have different needs than Programmers who have different needs than the clerical workers of the Billing Department of a company. Take the time to outline the development of your new policy and procedure and take into consideration what's important to the type of people in the targeted audience as relates to this specific policy.

Is there a good way to structure the policy and procedure that helps this group?
Are there samples you can add that helps clarify the policy and procedure? Are there reference documents or supporting items that help you establish the objective and importance of the policy?

If so, include what you need to help the group understand and comply with the new guidelines.

What will this group need relative to this particular policy?
There may be specific steps that must be followed, forms to use, or prerequisite items to be completed in order for people to comply with the new policy. Be sure to include any relevant parts so you achieve full compliance.

Are there implementation strategies that will help the group incorporate the policy and procedure?
If there are certain strategies that will help stress the importance and gain "buy in" regarding the new policy, be sure you take them into consideration. This leads us to the next chapter where we discuss implementation tips.

VII. Implementation tips

The previous chapters have discussed several aspects of developing and introducing policies and procedures into your company. The thing that often makes or breaks the receptivity of a new policy is how it is implemented.

It's similar to delivering services to a client. More often than not, the level of client happiness and appreciation with your IT Support organization is in "how" you deliver your services and not necessarily "what" you deliver.

Sidebar: I've often stated and know it to be true that you can take two IT Organizations with different skills and achieve dramatically different results. One organization has excellent technical skill but poor project management, client service, and communication skills. The second organization knows how to deal with clients and has excellent "soft" skills but much weaker technical skill.

The second group will outperform the stronger technical group every time. Client support is about building professional relationships where the client thinks of you as a true "partner". When this happens, your IT Organization will have much more success than the technical organization and will be perceived as real value to the business as opposed to the IT Organization with their own "agenda".

When you prepare to develop a policy and procedure, think about how you need to deliver it to its intended audience early on. It may have a bearing on how you write the policy in both its structure and content.

Personal Note: One of the strongest senior executives I've worked for had some very insightful recommendations for me early into our management relationship. He was the President of our company and all departments of the company along with my IT Department reported to him.

As a new CIO, one of my responsibilities is to set the framework as to how we can best support the business and those departments that depend upon technology. Ultimately, that usually means introducing a policy or two on "how we need to do business".

I'll never forget one of our first discussions as he introduced me to the needs of the company and laid out the challenges and opportunities we had.

In this discussion, he stated very directly, "Mike, if you need to do something that helps the business but puts you or IT into a confrontational situation with Regional Operations, come to me and let's discuss it first. The company needs IT to be viewed as Operation's "advocate" and not an "adversary". If the issue is controversial but important and needs to be done, it may be better for me to deliver the bad news."

At first, I thought he was just protecting me but over time I saw clearly that many times a new policy that can be initially construed as a negative is better received when delivered by "your manager", and not another Department Manager, especially a Support Organization.

We introduced many challenging changes in that company and Operations always looked at them in a more objective light and a stronger willingness of endorsing them when introduced by the one person that could help them understand the importance and value of making such a difficult change. That person was their boss and my boss.

One specific policy I remember was that we started charging our internal operational departments for IT expense by allocating out the IT Department expense to each of the Regions based upon their revenue. The objective was twofold:

1. To maintain the IT Department as a zero cost based operation
2. To instill in Operations that there was a real cost for everything they were requesting from IT.

This was a very controversial issue as you might imagine. Over time, it actually became a normal part of Operation's budgeting process and a non-issue other than the fact that Operations now wanted me to reduce my expenses. That's actually a good thing.

Developing and delivering new policies and procedures can be "touchy" issues. In other words, they can be very controversial. It's important that you be able to "step back" (there I go with that phrase again) and take perspective of the "big picture".

Implementing a new policy is not really about the IT Department. It's about doing things in a way that supports the business in a positive way.

Be sure you understand this point.

Too many IT Managers and CIO's get "cross-wired" with the organizations they support by trying to "direct" behavior rather than facilitate steps that lead to behavior change.

In the Marine Corps, I learned a valuable lesson that you get a higher quality effort when Marines understand the purpose of orders than when they don't. Persuasive management styles can get more accomplished in the long run than will authoritative styles of management.

There are times in any IT Manager or CIO's life that you just want to order your clients and users to follow certain procedures that improve your quality of life at work. Announcing a ***policy directive*** may be the short path in getting the change started but it may be the long and painful path of actually getting it adhered to.

"You catch more flies with honey than with vinegar."

Let's discuss a few important points to consider as you implement new policies and procedures. There are several key points you should pay attention to such as:

A. Do your homework
B. Be consistent
C. Be "net" when writing the introduction
D. Why format is important
E. Communication methods
F. Validate before announcing

A. Do your homework

Make the effort to research the topic you plan to write a policy and procedure for. Consider the target audience as you determine the real objectives you have for introducing such a policy. When you develop the objective, analyze it to insure it makes sense and that a formal policy is actually the best means of achieving it.

When researching the topic, you may find considerable numbers of sample policies available that help you write your own. The research may spawn new ideas that you determine to be important.

The point is that by taking your time and reflecting about what you are trying to accomplish with a new policy and then making the effort to write a clear, crisp policy that makes sense will help you achieve the positive results you are looking for.

Take time to understand the intended audience. Knowing what their challenges are and their needs and desires can help you craft an appropriate delivery that gets their attention and helps them "buy in" to the objective of the policy being implemented.

B. Be consistent

This was mentioned earlier and worth repeating. Develop all of your policies consistently. You want those that read them to get the feeling that they were all written by the same company. Starting out with a set format and a consistent approach helps people recognize the documents as policies and that they are important guidelines.

You also need to be consistent in how you implement new policies and procedures. The official statement may be sent from different people in the company depending upon the policy, but the content of the announcement should be somewhat consistent for easy recognition of a new policy.

C. Be "net" when writing the introduction
Short, tight statements that create your desired policy message is best for a couple of reasons. It's easier to read and you will get more people to read through them. Long paragraphs with lots of discussion turn people off so keep it "net".

D. Why format is important
Format is important in many ways:

- Helps identify the document as a policy
- Creates familiarity when the format is consistent with other policies
- Establishes a structure to follow for people developing new policies
- Creates consistency
- Helps establish a simple outline for easy reading
- Can create "attention" and interest in the document

E. Communication methods
I have one rule of thumb in announcing new policies and procedures. Announce them from the highest management level in the company that is appropriate for the policy.

This can be somewhat of a gray area at times so when in doubt, opt for the higher level manager or executive.

The reason for this is that if the policy is truly important, the higher level position will create a stronger sense of importance with many employees.

Use good judgement here. For example, the company's vacation policy is important but it's also an annual routine for Human Resources to announce the dates holidays will be observed by the company. Although important, the VP of Human Resources is certainly an appropriate level to announce the policy as opposed to the President or CEO of your company.

If there is an internal IT "Programming Quality Assurance" policy the CIO and Programming Manager are introducing, you might announce it from either person or jointly from both of them so it carries the weight of importance you want with the programming staff.

When a new policy is important enough and addresses significant liability issues, you may want your targeted audience to sign a short form that says they have read and understand the policy. This could be important if you acquire a new company that has a history of installing and using software illegally.

There are many communication methods you may use. All can be effective but depending upon the policy some may be more effective than others. Evaluate the policy, its objective, the importance of the issue, complexity of the policy or procedure, and the targeted audience to determine which approach will be most effective.

The different delivery approaches you might consider include:

- Company announcement presentation
- Company memo
- Email notice
- Department and group meetings
- Company newsletter
- Intranet announcement
- Voice mail broadcast

F. Validate before announcing

When you complete the policy and procedure, you should have a few capable people review it for several reasons.

- Validate content for accuracy.
- Inspect for Human Resources compliance and appropriateness.
- Inspect for legal compliance and appropriateness.
- Proof for grammar and spelling.
- Collaborate to determine best possible means of "rolling the policy out".

You should sit down with key managers of the company who have a vested interest in effectively implementing the policy. Certain policies may need a full committee review prior to announcing the policy if there are highly sensitive ramifications of the policy.

There may be legal or Human resources implications that need to be signed off by your legal or HR Department. If so, be certain to include the appropriate representative from those areas as necessary. They may be needed in crafting the policy and procedure or simply to approve what you develop prior to announcing.

It is better to be safe than sorry.

You can lose lots of credibility by announcing a new policy that's "half baked" and not fully thought through. It can be viewed as very unprofessional when you have to withdraw a policy because it lacked significant content or potentially exposes the company to a legal action based on what it says or how it says it.

Everything you do either contributes to your professionalism or takes away from it. Approach the development and the implementation of policies and procedures so you are sure it enhances your IT Organization's image among company employees.

VIII. Sample IT Policies and Procedures

There are twenty-three sample policies and procedures included in this section. You may use them as you wish in helping you develop your own specific policies and procedures.

Disclaimer: *MDE Enterprises does not express or imply that any of the sample policies and procedures will meet your particular company needs nor should they be construed to limit liability or exposure to risk associated with any of your business issues.*

They are provided as samples only to give you a starting point in developing your own IT policies and procedures for use in your operation.

You should have your Human Resources group and possibly the company's legal counsel review any policy before implementing it to insure it complies to regulatory requirements and is supportable in a possible legal claim.

The samples to follow are not intended to be comprehensive policies to meet any and all company needs. There isn't such a thing.

The intent is to provide you with a development process that we have discussed in the preceding pages and samples that will give you a quick starting point. It's up to you to revise any policy you decide to use and add the 20 - 30% additional substance that makes it "your" policy and procedure that actually meets "your" specific needs.

You may also want to review the following chapter on **Policy and Procedure Resources** for other sources that can help you with your P&P initiative.

When it comes to developing your own policy and procedures, use all resources available to you. The important thing is to develop guidelines that achieve the objective you need and to create a positive reflection on your company and operation.

It's usually easier and faster to start with something that meets 80% of the need and enhance it rather than starting from scratch. That's where I hope you find the following twenty-three samples beneficial.

A few policies are company-wide in nature such as Expense Reporting. I have included these since many small companies do not have them and they can be helpful.

The 23 samples is by no means all the IT policies you may need, but it's a good start.

In the following samples, we have tried to make them as generic as possible. For example, instead of using our company name, MDE Enterprises, we use "the company". This allows you to use the policies and easily replace "the company" with your company name for a fast start in developing your own policies and procedures.

There are 23 examples in all that cover various aspects of managing an IT Organization. We hope you find them useful "starting points" for developing your own practical policies and procedures.

	Policy	Page
IT_01	Email and Instant Messaging	34
IT_02	Internet usage	37
IT_03	Password security	39
IT_04	Intranet usage	41
IT_05	Phone usage	44
IT_06	Building security and access	49
IT_07	Software usage	51
IT_08	PC software standards	54
IT_09	Travel and entertainment	58
IT_10	Employee conduct	67
IT_11	Employee non-compete	71
IT_12	Employee non-solicitation	73
IT_13	Performance plans and reviews	76
IT_14	Training and reimbursement	79
IT_15	Working from home	81
IT_16	Inventory and equipment	84
IT_17	PC standards	86
IT_18	Equipment requests (Adds, Changes, Deletes)	88
IT_19	New employee startup	91
IT_20	Information security	95
IT_21	Remote access	100
IT_22	Privacy	102
IT_23	Service level agreements	104

No: IT_01

Policy Name: Email and Instant Messaging

Objective:

Provide appropriate guidelines for productively utilizing the company's email system and instant messaging technology that protects the employee and company while benefiting our business.

Applies to:

All employees

Key guidelines:

The company has established this policy with regard to the acceptable use of company provided electronic messaging systems, including but not limited to email and instant messaging.

Email and instant messaging are important and sensitive business tools. This policy applies to any and all electronic messages composed, sent or received by any employee or by any person using company provided electronic messaging resources.

The company sets forth the following policies but reserves the right to modify them at any time in order to support our company:

General

- The company provides electronic messaging resources to assist in conducting company business.
- All messages composed and/or sent using company provided electronic messaging resources must comply with company policies regarding acceptable communication.
- The company prohibits discrimination based on age, race, gender, sexual orientation or religious or political beliefs. Use of electronic messaging resources to discriminate for any or all of these reasons is prohibited.
- Upon termination or separation from the company, the company will deny all access to electronic messaging resources, including the ability to download, forward, print or retrieve any message stored in the system, regardless of sender or recipient.
- Each employee will be assigned a unique email address that is to be used while conducting company business via email.

- Employees are prohibited from forwarding electronic messages sent through company provided systems to external messaging systems.
- Employees authorized to use instant messaging programs will be advised specifically on which instant message program(s) are permissible.
- Employees authorized to use instant messaging programs will be assigned a unique instant messaging identifier, also known as a buddy name, handle or nickname.
- Electronic messages are frequently inadequate in conveying mood and context. Carefully consider how the recipient might interpret a message before composing or sending it.
- Any employee who discovers a violation of these policies should immediately notify a manager or the Human Resources Department.
- Any employee in violation of these policies is subject to disciplinary action, including but not necessarily limited to, termination.

Ownership

- The email/electronic messaging systems are company property. All messages stored in company provided electronic messaging system(s) or composed, sent or received by any employee or non-employee are the property of the company. Electronic messages are NOT the property of any employee.
- The company reserves the right to intercept, monitor, review and/or disclose any and all messages composed, sent or received.
- The company reserves the right to alter, modify, re-route or block the delivery of messages as appropriate.
- The unique email addresses and/or instant messaging identifiers assigned to an employee are the property of the company. Employees may use these identifiers only while employed by the company.

Confidentiality

- Messages sent electronically can be intercepted inside or outside the company and as such there should never be an expectation of confidentiality. Do not disclose proprietary or confidential information through email or instant messages.
- Electronic messages can never be unconditionally and unequivocally deleted. The remote possibility of discovery always exists. Use caution and judgment in determining whether a message should be delivered electronically versus in person.
- Electronic messages are legally discoverable and permissible as evidence in a court of law. Messages should not be composed that you would not want to read out loud in a court of law.
- Employees are prohibited from unauthorized transmission of company trade secrets, confidential information, or privileged communications.
- Unauthorized copying and distribution of copyrighted materials is prohibited.

Security

- The company employs sophisticated anti-virus software. Employees are prohibited from disabling anti-virus software running on company provided computer equipment.
- Although the company employs anti-virus software, some virus infected messages can enter the company's messaging systems. Viruses, "worms" and other malicious code can spread quickly if appropriate precautions are not taken. Follow the precautions discussed below:
    - Be suspicious of messages sent by people not known by you.
    - **Do not open attachments** unless they were anticipated by you. If you are not sure, **always verify** the sender is someone you know and that he or she actually sent you the email attachment.
    - Disable features in electronic messaging programs that automatically preview messages before opening them.
    - Do not forward chain letters. Simply delete them.
- The company considers unsolicited commercial email (spam) a nuisance and a potential security threat. Do not attempt to remove yourself from future delivery of a message that you determine is spam. These "Remove Me" links are often used as a means to verify that you exist.
- Internet message boards are a fertile source from which mass junk e-mailers harvest email addresses and email domains. Do not use company provided email addresses when posting to message boards.

Inappropriate use

- Email or electronic messaging systems may not be used for transmitting messages containing pornography, profanity, derogatory, defamatory, sexual, racist, harassing, or offensive material.
- Company provided electronic messaging resources may not be used for the promotion or publication of one's political or religious views, the operation of a business or for any undertaking for personal gain.

Samples:

Not applicable

For questions, call:

For questions or comments, please call your IT Department at Ext. 5555.

Last revision date:

December 12, 2003

No: IT_02

Policy Name: Internet usage

Objective:

Provide appropriate guidelines for accessing and utilizing the Internet through the company's network.

Applies to:

All employees with authorized access to Internet services

Key guidelines:

Internet services are authorized to designated employees by their manager to enhance their job responsibility. The Internet is an excellent tool but also creates security implications that the company must guard against. For that reason, employees are granted access only as a means of providing support in fulfilling their job responsibility.

General

- Internet accounts are approved for designated employees by their immediate manager to provide tools that assist in their work.
- Each individual is responsible for the account issued to him/her.
- Sharing Internet accounts or User-ID's is prohibited.
- Organizational use of Internet services must reflect the mission of the company and support the company's goals and objectives.
- These services must support legitimate, mission related activities of the company and be consistent with prudent operational, security, and privacy considerations.
- The CIO led Internet Steering Committee will take responsibility for all web site content (i.e., "the company web site") and format presentation to reflect the company's mission and in supporting company and departmental objectives.
- The Company has no control over the information or content accessed from the Internet and cannot be held responsible for the content.
- Any software or files downloaded via the Internet into the company network become the property of the company. Any such files or software may be used only in ways that are consistent with their licenses or copyrights.

Inappropriate use

- The following uses of company provided Internet access are not permitted:
    - To access, upload, download, or distribute pornographic or sexually explicit material
    - Violate and state, local, or federal law
    - Vandalize or damage the property of any other individual or organization
    - To invade or abuse the privacy of others
    - Violate copyright or use intellectual material without permission
    - To use the network for financial or commercial gain
    - To degrade or disrupt network performance
- No employee may use company facilities knowingly to download or distribute pirated software or data. The use of file swapping software on company computers and company networks is prohibited.
- No employee may use the company's Internet facilities to deliberately propagate any virus, worm, Trojan horse, or trap-door program code.

Samples:

None

For questions, call:

For questions or comments, please call your IT Department at Ext. 5555.

Last revision date:

December 12, 2003

No: IT_03

Policy Name: Password security

Objective:

Provide guidelines in appropriate management of business passwords to maintain adequate security and integrity of all of the company's business systems.

Applies to:

All employees

Key guidelines:

Maintaining security of the company's business applications, software tools, email systems, network facilities, and voice mail are critical to providing data integrity and stability of our systems. Passwords are provided to limit access to these company assets on an as needed basis.

- The company provides access to network, electronic mail and voice mail resources to its employees in support of the company's mission. Passwords are assigned for access to each of these resources to authenticate a user's identity, to protect network users, and to provide security.
- It is the responsibility of each individual to protect and to keep private any and all passwords issued to him/her by the company.
- The IT Department will establish guidelines for issuing new passwords, deleting passwords as required, and allowing employees to change their passwords.
- Although the company strives to manage a secure computing and networking environment, the company cannot guarantee the confidentiality or security of network, e-mail or voice mail passwords from unauthorized disclosure.
- New employee passwords and changes must be requested by a Manager. This helps monitor and manage the importance of protecting passwords in their distribution and use in such a way that reinforces the integrity of users accessing company systems.
- A network manager must approve any password change requested by a user's supervisor. Confirmation will be sent to user when a password change is completed at the request of a supervisor.

- IT Customer Support will handle requests from company managers made in one of the following ways:
    - Requests may be made in person from 7:00am to 5:00pm Monday-Friday.
    - Requests may be faxed to (555) 555-5555.
    - Requests may be submitted via Intranet web form.
    - Password account requests must be verified by the employee's manager.
- The IT Department will delete all passwords of exiting employees upon notification from Human Resources.
- System administrators and users assume the following responsibilities:
    - System administrator must protect confidentiality of user's password.
    - User must manage passwords according to the Password Guidelines.
    - User is responsible for all actions and functions performed by his/her account.
    - Suspected password compromise must be reported to Customer Support immediately.

Password Guidelines

Select a Wise Password

To minimize password guessing:

- Do not use any part of the account identifier (username, login ID, etc.).
- Use 8 or more characters.
- Use mixed alpha and numeric characters.
- Use two or three short words that are unrelated.

Keep Your Password Safe

- Do not tell your password to anyone.
- Do not let anyone observe you entering your password.
- Do not display your password in your work area or any other highly visible place.
- Change your password periodically (every 3 months is recommended).
- Do not reuse old passwords.

Additional Security Practices

- Ensure your workstation is reasonably secure in your absence from your office. Consider using a password-protected screen saver, logging off or turning off your monitor when you leave the room.

Samples:

None

For questions, call:

For questions or comments, please call your IT Department at Ext. 5555.

Last revision date:

December 12, 2003

No: IT_04

Policy Name: Intranet usage

Objective:

Provide guidelines for the appropriate use of the company's Intranet to improve the productivity and effectiveness of our staff and company and to maintain security of our Intranet assets.

Applies to:

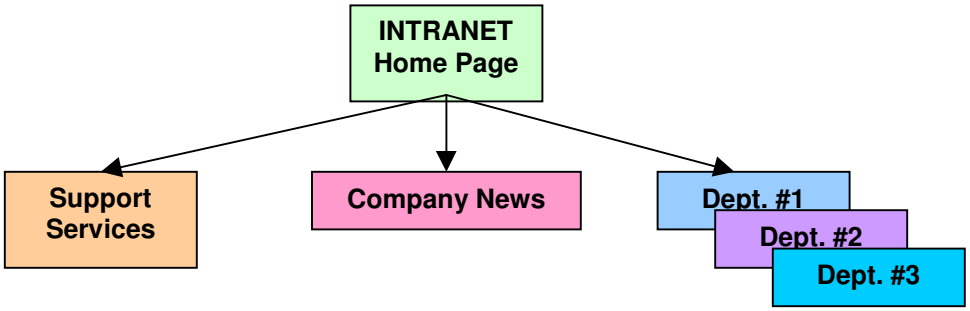
All employees

Key guidelines:

The company Intranet is a proprietary web based source of content, knowledge base, and process tool for our internal employees and managers. Security measures have been established to allow company employees and managers access to appropriate sections of the company's Intranet to assist in their efforts in conducting business for our company.

- All full time employees of the company are approved for access to the company Intranet. Part time employees and contracted resources must have management approval for Intranet access.
- Intranet security passwords are the responsibility of each individual authorized to access the Intranet. Passwords are not to be shared, swapped, or given out in any form. Keep passwords hidden from view and protect the integrity of your company's employee information.
- The CIO and Intranet Steering Committee are responsible for setting the goals and objectives for the company's Intranet, determining priorities for adding new content, and for maintaining the integrity of the Intranet site.
- The CIO and Intranet Steering Committee are also responsible for defining, creating, and maintaining consistent format for all web sites and pages developed for the Intranet regardless of original department source.
- Each of the company's operational and support departments will be represented in the Intranet Steering Committee to provide content and processes that enhance employee knowledge and productivity. Submit feedback and suggestions to your department representative.
- All content residing on the company's Intranet is the property of the company.
- Maintenance of the Intranet is an assigned role established by the CIO.

- The company will provide a central Home Page access that will be the employee's main entry point into the company's Intranet as follows:



- Departments may include links in department sites/pages for downloading documents and files in the following formats:
    - Microsoft Excel
    - Microsoft Word
    - Microsoft Access
    - Microsoft PowerPoint
    - Adobe PDF
    - Visio
    - Images and video files approved by the Steering Committee
- Downloaded files from the Intranet are considered proprietary information of the company and should be treated as such.
- Our company's Intranet represents an ongoing reflection of the company and organizations within the company. It is every employee's right and obligation to provide input that constantly improves the accuracy of all content and includes new material for consideration that enhances your experience with the company.

Guidelines for Establishing a Web Site on the Intranet

The following steps are general guidelines for adding new Intranet content:

1. Develop your idea to do an Intranet web site.
2. Review Intranet Guidelines and Policy.
3. Discuss your proposed web site project with your department's manager.
4. Determine if another effort already exists:
    - *IF YES*: Consider whether efforts should be combined.
    - *IF NO*: Proceed to the next step.
5. Gain submission approval from your department head.
6. Contact your department's Intranet Committee representative for guidance in any part of the web site process.
7. Determine if the Intranet is the best format for your purpose:
    - *IF NO*: Discontinue your plans for an Intranet web site and investigate alternative solutions.
    - *IF YES*: Continue to the next step.
8. Sketch out information and proposed organization of your web site.
9. Web Site Plan must be approved by function/business management including all associated costs and staffing.
10. Gain Department Head approval to fund the project.
11. Submit to Intranet Committee for approval.
12. If approved, assemble and develop content required for each web page.
13. Submit design to assigned Intranet development manager.
14. Define with Intranet development staff the project objectives, scope, and required participation from your department to develop, QA, and implement the new Intranet web site or functionality.
15. Participate as required in developing and implementing the new site.
16. Maintain content and hyperlinks of web site according to Intranet guidelines.

Samples:

None

For questions, call:

For questions or comments, please call your IT Department at Ext. 5555.

Last revision date:

December 12, 2003

No. IT_05

Policy Name: Phone usage

Objective:
Provide guidelines on appropriate use of the company's phone system to maintain high productivity and cost effectiveness in using this company asset

Applies to:
All employees

Key guidelines:
Included in this policy are guidelines for appropriate use of company phone systems and cell phones. The two types of phone services have very different issues and require unique guidelines for clarity.

Phone capabilities are integral parts of the company's assets to help conduct business effectively. Phone systems and equipment are provided to enhance employee capabilities and are not to be construed as assets available for personal use. The following guidelines should be read and understood by all employees.

I. Company phone system guidelines
- The phone systems of the company are assets to assist in conducting company business.
- Local phone carriers will be determined by the local Operations Manager along with the IT Manager responsible for supporting company PBX telephone systems.
- The company's 1-800 numbers are to be used for company business only.
- During business hours, all calls should be answered within three rings.
- Be courteous and considerate when representing yourself and our company when using company phone services.
- Voice mail greetings should be created to identify yourself, explain that you are away from your desk, and state that the caller should leave a message and you will return their call when you can.
- When out of town or on vacation, you should leave a voice mail greeting that states you are away for an extended amount of time and direct the caller to leave a message or call another number for one of your counterparts as appropriate.

- Voice mail messages should be responded to within a reasonable time of retrieving the voice message. Follow-up sets the professional tone of our company is regarded as an important company issue.
- Long distance calls can accumulate to significant costs. The company monitors long distance calls of every department as a means of managing phone expense of the company just as we do other company expenses.
- Personal phone calls made on company business telephones should be kept to a minimum and should be used only for local calls.
- Personal long distance calls are the responsibility of the employee. If the employee must make personal long distance calls, they may:
    1. call collect
    2. charge the call to their home phone
    3. charge the call to a personal calling card

II. Cell phone guidelines

New service and equipment: A signed request by the employee's department manager should be sent to the Cell Phone Contract Administrator located in the Purchasing Department of our corporate facility or faxed to extension 5555. Forms may be obtained from the Cell Phone Contract Administrator at extension 5554 or in the ***Samples*** section of this policy.

Losses and repairs: The Cell Phone Contract Administrator must be notified immediately when a cell phone is lost or stolen so that appropriate action can be taken with the cell phone provider. All repairs to damaged cell phones are handled by the Cell Phone Contract Administrator.

Replacements: If the equipment is defective, the wireless provider will replace it at no cost to the user; however, if the equipment is damaged through negligence on the part of the user, then additional costs may be incurred. All replacement requests are processed in coordination with the Cell Phone Contract Administrator.

Responsibilities

The following responsibilities are helpful in managing cell phone usage in our company:

A. Requesting Department Manager:

- Submits completed wireless services equipment order form for all new wireless requests.
- Ensures cell phone users comply with company policies
- Informs Cell Phone Contract Administrator of user name changes.
- Submits e-mail requests for all changes to existing wireless service and additional accessory orders.
- Reviews monthly reports for cell phone usage charges via the electronic billing system used for all administrative phone charges, and takes corrective action when necessary.
- Ensures cell phone equipment is recovered from employees that are terminated or leave the company.
- Notifies the Cell Phone Contract Administrator immediately if a cell phone is lost, stolen, or damaged.
- Contacts the Cell Phone Contract Administrator for assistance at ext.5554.

B. Cell Phone Contract Administrator:

- Orders the cell phone equipment and accessories and will either distribute the equipment to the Cell Phone User or notify the ordering department when the items are available for pickup.
- Enters information for all cell phones into the telephone billing database, and maintains a master inventory of cell phone users, equipment, and vendor charges.
- Initiates all repairs, replacements, and changes to wireless service.
- Reviews cell phone bills monthly and makes recommendations to departments when necessary.

C. Cell Phone User

- Takes responsibility for sole use of the assigned company cell phone and will only use for company business.
- Takes responsibility for the wireless equipment and maintains it in good working order, protects from theft, and avoids placing the equipment in harmful environments.
- Returns all wireless equipment to the Cell Phone Contract Administrator upon leaving employment of the company.
- Contacts Cell Phone Contract Administrator for damaged equipment or loss.
- Cell phones can be distracting in an office setting. Each holder of a cell phone should be considerate of others and set the phone to vibrate or turn it 'off' during meetings unless job responsibility requires availability.

Samples:
A. Phone request form:

XYZ Company
Phone/fax/modem service request

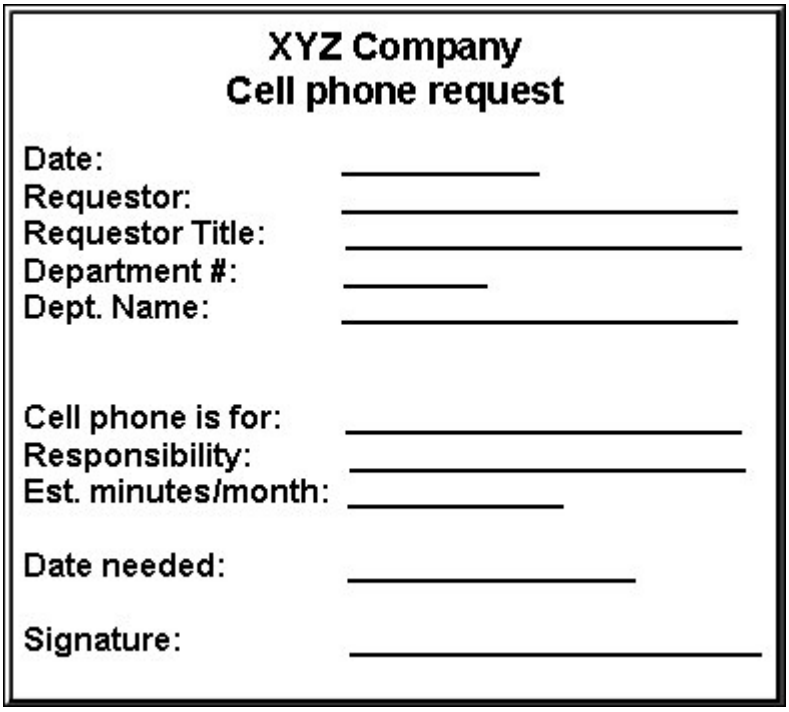
Date: _____
Requestor: _____
Requestor Title: _____
Department #: _____
Dept. Name: _____
Wall jack ID (if any): _____
Physical location: _____
Service required:
Phone: _____ Fax: _____ Modem: ____
Service is for (name):_____
Responsibility: _____
Special phone equipment needs:
1-line__ multi-line__ conference__ speaker__

_____
_____

Date needed: _____

Signature: _____

B. Cell phone request form:



XYZ Company
Cell phone request

Date: _____
Requestor: _____
Requestor Title: _____
Department #: _____
Dept. Name: _____

Cell phone is for: _____
Responsibility: _____
Est. minutes/month: _____

Date needed: _____

Signature: _____

For questions, call:

For questions or comments, please call your IT Department at Ext. 5555.

Last revision date:

December 12, 2003

No. IT_06

Policy Name: Building security and access

Objective:
Provide guidelines on maintaining the highest level of security for our physical office assets and employees

Applies to:
All employees

Key guidelines:
The company provides keys and password access for use by staff to maintain building and office security and allow access to designated areas for authorized personnel during normal business hours and after hours.

Physical security of company employees and assets is a primary objective of the company. This policy is intended to help provide a safe and secure work environment, prevent theft, and to provide a procedure for appropriate distribution and collection of keys and maintenance of accurate security access code logs.

- The official business hours of the company buildings are Monday through Friday, 8:00 A.M. to 5:00 P.M. (except for official holidays).
- Within reason and practical limits, employees having visitors must escort them when inside the building.
- Building Security Officers may issue special permission for individuals to be in the building without the presence of a staff member. Such cases will include announced meetings held in the company Conference Room such as Policy Board Meetings, designated vendor support calls, and consultants that work with the company from time to time.
- After business hours, visitors are subject to being challenged by staff members and required to identify themselves and their purpose in the building. Employees must share in the responsibility of questioning these unescorted visitors and reporting any unauthorized personnel to the Building Security Officer.
- Company keys are the property of the company.
- Managers may request building keys for authorized employees and will be responsible for collecting the key upon an employee separating from the company.

- Keys will be assigned by employee name. Each individual assumes responsibility for protecting the security of his/her key and will report losses or situations that possibly jeopardize building security to his/her manager.
- It is each Department Head's responsibility to insure that building keys are only given to those few employees that require after hours access to the building for business purposes.
- Lost keys must be reported to the issuing department within 24 hours of loss.
- The following actions are in violation of this policy:
    a. Loaning keys without authorization
    b. Duplicating keys
    c. Altering keys, locks, or mechanisms
    d. Admitting unauthorized persons into building
    e. Failure to return a key when requested by Security Services, authorizing department, or upon leaving the company.
- All company employees need to be concerned with building lock-up and ensure that when entering and leaving the building after normal business hours, the doors and office windows are locked.
- If an alarm system is present it is the responsibility of the last person leaving to set the alarm.
- Visitors are not allowed access to the IT Operations Center (computer room) without prior authorization. This advance authorization may be obtained by contacting the Manager of Operations.
- Any concerns, questions or comments regarding this policy or interpretation of this policy should be directed to a member of the management team.

Samples:

Key request form

For questions, call:

For questions or comments, please contact your Building Security Officer.

Last revision date:

December 12, 2003

XYZ Company
Key Request

Requestor: _____
Title: _____
Signature: _____
Key is for: _____
Responsibility: _____
Reason: _____

Key needed:
1. Building access ____
2. General office access ____
3. Interior office ____
4. Other secured areas (please describe)

_____
_____
_____
_____

No. IT_07

Policy Name: Software usage

Objective:
Provide guidelines on appropriate use of software products utilizing company equipment

Applies to:
All employees

Key guidelines:
This policy is intended to ensure that all company employees understand that no computer software may be loaded onto or used on any computer owned or leased by the company unless the software is the property of or has been licensed by the company.

General

- Software purchased by the company or residing on company owned computers is to be used only within the terms of the license agreement for that software title.
- Unless otherwise specifically provided for in the license agreement, any duplication of copyrighted software, except for archival purposes is a violation of copyright law and contrary to the company's **Software Usage Policy**.
- To purchase software, users must obtain the approval of their department manager who will follow the same procedures used for acquiring other company assets.
- All approved software will be purchased through the Purchasing Department.
- The CIO and designated members of the IT Department will be the sole governing body for defining appropriate software titles acceptable for use in the company.
- Under no circumstances will third party software applications be loaded onto company owned computer systems without the knowledge of and approval of the IT Department.
- Illegal reproduction of software is subject to civil and criminal penalties, including fines and imprisonment. Any company user who makes, acquires, or uses unauthorized copies of software will be disciplined as appropriate under the circumstances and may include termination of employment.
- The company does not condone the illegal duplication of software in any form.

Compliance

- We will use all software in accordance with its license agreements.
- Under no circumstances will software be used on company computing resources except as permitted in the company's **Software Usage Policy**.
- Legitimate software will be provided to all users who need it. Company users will not make unauthorized copies of software under any circumstances. Anyone found copying software other than for backup purposes is subject to termination.
- Each user of software purchased and licensed by the company must acquire and use that software only in accordance with the company's **Software Usage Policy** and the applicable Software License Agreement.
- All users acknowledge that software and its documentation are not owned by the company or an individual, but licensed from the software publisher.
- Employees of the company are prohibited from giving company acquired software to anyone who does not have a valid software license for that software title. This shall include but is not limited to clients, vendors, colleagues, and fellow employees.
- All software used by a company entity for company owned computing devices, or purchased with company funds, will be acquired through the appropriate procedures as stated in the company **Software Usage Policy**.
- Any user who determines that there may be a misuse of software within the organization will notify the software manager or department manager.

Registration of software

- Software licensed by the company will not be registered in the name of an individual.
- When software is delivered, it must first be properly registered with the software publisher via procedures appropriate to that publisher. Software must be registered in the name of the company with the job title or department name in which it is used.
- After the registration requirements above have been met, the software may be installed in accordance with the policies and procedures of the company. A copy of the license agreement will be filed and maintained by the IT Department's Software License Administrator.
- Once installed, the original installation media should be kept in a safe storage area designated by the IT Department.
- Shareware software is copyrighted software that is distributed freely through bulletin boards, online services, and the Internet. The company's policy is to pay shareware authors the fee they specify for use of their products if the software will be used at the company. Installation and registration of shareware products will be handled the same way as for commercial software products.

Software Audit

- IT will conduct periodic audits of all company owned PCs, including laptops, to insure the company is in compliance with all software licenses.
- Audits will be conducted using an auditing software product.
- Software for which there is no supporting registration, license, and/or original installation media will be removed immediately from the user's computer.
- During these audits, the software manager will search for computer viruses and eliminate any that are found.
- The full cooperation of all users is required during software audits.

Samples:

None

For questions, call:

For questions or comments, please call your IT Department at Ext. 5555.

Last revision date:

December 12, 2003

No. IT_08

Policy Name: PC software standards

Objective:
Provide guidelines for purchasing and installing software on company PC's

Applies to:
All employees

Key guidelines:
The purpose for this policy is to explain company software standards and to identify the levels of technical support available to the company employees from the IT Department.

Applicability

1. This policy applies to all employees of the company requesting the purchase of new computer software and who desire computing support for that application from the IT technical support team.
2. The following software standards have been established to ensure efficient and cost effective use of company computing assets:
    - To help ensure compatibility between applications and releases
    - To provide more effective system administration
    - To assist in the computer planning process and enable the realization of long term goals and the future computing vision
    - To ensure cost effective purchasing
    - To enable effective tracking of software licenses
    - To provide cost effective end user software training
    - To facilitate efficient and effective technical support effort

Technical Support

- Software support is provided at several levels and is based on whether the software is the company enterprise standard or department specific.
- The IT Department will not provide support for evaluation software, personally purchased software, illegal copies of software, screen savers, shareware, and non-network software that is not included in the standard software list.
- Software applications determined by IT technical staff to cause computer problems with the company's standard network software will be removed.

IT Department's Role In The Purchase of Hardware And Software

- Assist departments with evaluating new business software solution.
- Act as liaison for departments when dealing with computing vendors.
- Recommend and evaluate the tasks/jobs/functions to be accomplished via the new software product.
- Assist with hardware and system requirements.
- Install the software as needed.
- Enforce company hardware and software standards.

Standard PC Equipment and Software List

- Standard PC hardware and software configurations are posted on the company's Intranet web site in the IT Department section.
- Contact the Systems Support Manager of the IT Department for questions pertaining to company standards.

Requesting Standard PC Equipment and Software

- Equipment and software requests that are covered by the company's PC Equipment and Software Standards List will be provided quickly as long as appropriate approvals are granted.
- The steps that follow outlines the process for purchasing PC equipment and software:
  1. Complete the **PC Equipment and Software Request** form. (See example in SAMPLES section)
  2. Gain approval of the Department Manager
  3. Submit request to IT Department's Systems Support Manager.
  4. The IT Department will review the order and forward to Purchasing or will contact Requestor for clarification as needed.
  5. The IT Department or Purchasing Department are available for follow-up questions regarding your order as needed.

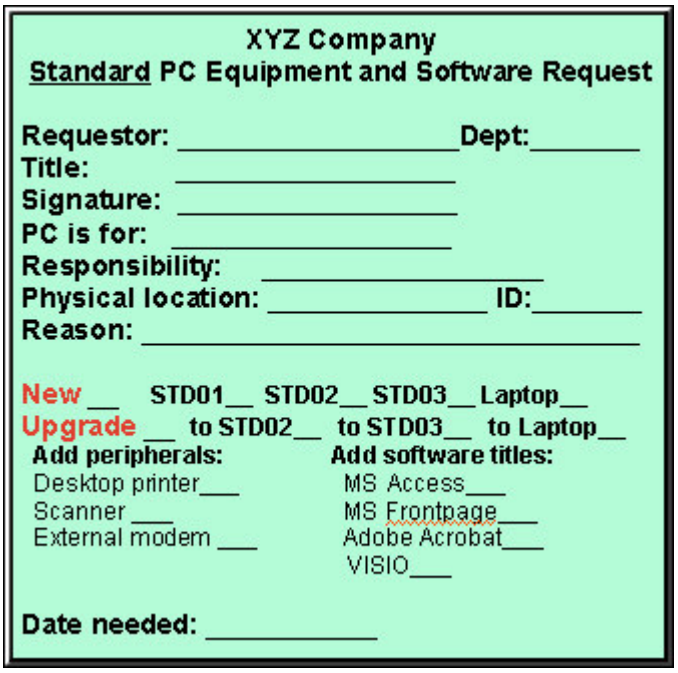
Request for a Variance from the PC Hardware or Software Standard

- Complete the "Request for a Variance from the PC Hardware and Software Standard" form.
- Practical and sufficient justification is a key part so be concise in building your case for deviating from the standard.
- Gain approval of the request from your Department Manager.
- Submit the request to the IT Department's Systems Support Manager for review.
- Your request is reviewed and either approved or declined based upon justified reasons presented and the IT Department's ability to support the new configuration within the company's network.

Samples:

A. Standard PC Equipment and Software Request

This form should be used for most PC equipment and software orders. It assumes you have familiarized yourself with the standard configuration list for PC computers and software available from the company's Intranet site in the IT Department section.



XYZ Company
Standard PC Equipment and Software Request

Requestor: _____ Dept: _____
Title: _____
Signature: _____
PC is for: _____
Responsibility: _____
Physical location: _____ ID: _____
Reason: _____

New __ STD01__ STD02__ STD03__ Laptop__
Upgrade __ to STD02__ to STD03__ to Laptop__

Add peripherals:	Add software titles:
Desktop printer___	MS Access___
Scanner ___	MS Frontpage___
External modem ___	Adobe Acrobat___
	VISIO___

Date needed: _____

B. Request for a Variance from the PC Hardware or Software Standard
Requests for PC equipment or software not listed in the company's PC Standard Equipment and Software List must be reviewed and approved by the IT Department before purchasing and installing. The form below will highlight your request in order to expedite the review and response to your need.

Pay close attention to the ***Reason and justification*** section. Variances from the company's standards are reviewed closely for compatibility and justification of need.

XYZ Company
Request for a Variance
from the PC Hardware or Software Standard

Requestor: _____ **Dept:**_____
Title: _____ **Phone:**_____
Signature: _____
PC is for: _____
Responsibility: _____
Physical location: _____ **ID:**_____

Special PC equipment or software requested:
_____
_____
_____

Special vendor required: _____
Vendor contact: _____

Reason and justification (be specific):
_____
_____
_____
_____

Date needed: _____

For questions, call:
For questions or comments, please call your IT Department at Ext. 5555.

Last revision date:
December 12, 2003

No. IT_09

Policy Name: Travel and entertainment

Objective:

Provide guidelines pertaining to travel and entertainment when on company business.

Applies to:

All employees

Key guidelines:

IRS Compliance

- The Internal Revenue Service has issued publication 463, Travel, Entertainment, Gift and Car Expenses. This document is the basis for the company's Travel and Entertainment Guidelines.
- The IRS states that ordinary and necessary business related expenses are deductible and reimbursable.
- The IRS defines *ordinary* as “common in your field of trade, business or profession”; and *necessary* as “helpful and appropriate for your business”.
- The IRS states that meals, hotels and entertainment expenses cannot be “lavish or extravagant”.
- The IRS requires all businesses to reimburse employees for travel and entertainment expenses under "an accountable plan". For a plan to be deemed "accountable", it must meet the following guidelines:
    - must be a business reason for the expenses
    - the employee must substantiate the expenses
    - the employee must return to the employer any amount advanced in excess of the substantiated expenses on a timely basis
- To be in compliance with the IRS, the company has prepared the following accountable travel and entertainment plan guidelines. These guidelines apply to all company employees traveling on company business.

General

- The company's policy is to reimburse employees for ordinary and necessary travel and entertainment expenses incurred while on authorized company business.
- Costs included are for transportation, lodging, meals and communications.
- All travel and entertainment expenses are reviewed and approved by the employee's Department Manager and the company's Business Office before reimbursement.
- A Senior Executive must approve Department Manager's travel expenses.
- The intent of the travel policy is to reimburse employees for out-of-pocket expenses incurred while on company business that would not otherwise be incurred. Expenses that are of a personal nature, or expenses that would be incurred whether or not the employee was on company business, are not eligible for reimbursement.
- The company requires employees to document and request reimbursement for such expenses in accordance with the **Travel Expense Report** section of this policy.
- The company requires that employees on company business wear seat belts.
- The company discourages the use of cell phones while driving.
- Fees or fines incurred due to legal infractions (such as parking fines, speeding tickets, etc.) are the responsibility of the employee. The company will not reimburse such fees or fines.
- When several members of a department or many company employees are traveling to the same destination, the company recommends employees consider splitting the group to minimize exposure to the risks inherent in traveling.
- Discounts are often available through various organizations. The company cannot pay for personal memberships, but if these discounts are available to the employee they are encouraged to utilize them to minimize travel costs.
- Employees who travel frequently should request a company credit card from the Purchasing Department. Requests must be signed by a Department Manager.
- This is an evolving document. Updates will be made as regulatory (IRS) and industry standards change. Employees should review the Travel Guidelines at least annually to ensure they managing travel expenses consistent with company guidelines.

Travel agencies and ticketing fees

- The company does not have an "official" travel agent. Employees are free to choose a travel agent, deal directly with the airlines/hotels or book travel online.
- It is common practice for travel agencies to charge a fee for their service. Employees should be aware of this fee, as it can be quite high, and weigh the fee against the expense of doing the travel research on their own and other benefits provided by the travel agent.
- Managers should review the use of fees for appropriate benefit for the cost.
- When attending a conference or professional meeting, employees should check the group airfare rate negotiated by the event sponsor. Often, these group rates are quite a bit lower than normal fares.

Air transportation

- The company will reimburse the cost of airplane tickets in coach class only. All efforts should be made to obtain the lowest coach fare available. This usually requires booking 14 to 30 days in advance and a non-refundable ticket.
- In the event a non-refundable ticket has to be canceled, the airlines will charge a fee and issue a credit that has to be used by that employee within the year. Penalties can be quite high. The benefit of locking into a fare should be weighed against the risk of having to make changes in travel plans before purchasing a ticket. If a penalty is incurred due to cancellation, the Department Manager must approve the reimbursement amount.
- For electronic tickets, please request a receipt when obtaining boarding passes.
- When using a kiosk the machine will print one if requested. If that is not possible, submit the web page printout or confirmation letter that is e-mailed to the employee and the boarding passes for each leg of the trip with your Expense Report.
- For paper tickets, please provide the last page of the airline ticket (passenger receipt) as receipt for the trip. It is important that documentation is submitted that shows the name of the person traveling, the destination and the cost of the ticket.
- Most airlines strictly enforce rules regarding the number, size and weight of bags allowed for each passenger. Extra baggage charges and charges for personal items are not reimbursed by the company.

Spousal or companion travel

- The IRS requires a “bona fide business purpose” for the spouse to be on the business trip for the expenses to be reimbursable.
- A Senior Manager must approve any spousal travel at the company.
- Documentation of the spouse’s business purpose must be clearly documented on all travel forms.
- In the specific circumstance where non-business spousal travel is approved the cost will be treated as taxable income to the employee.
- In the event a spouse, companion, child, etc. travels with the employee, any increased costs must be paid by the employee (i.e. double vs. single occupancy, meal costs, etc.).

Business travel insurance

- Company authorized credit cards offer life insurance for tickets purchased on the card. For specific information regarding coverage, contact the Purchasing Office.
- Additional business travel insurance purchased by the employee is a personal expense and should not be charged to the company.

Frequent flyer miles

- Employees may retain frequent flyer miles earned while on company business. However, employees must always travel on the least expensive airline, not the airline with which they have a frequent flier relationship.
- Excess cost due to the use of an employee's preferred airline will not be reimbursed.
- It is inappropriate for the company to "buy" employee frequent flyer tickets.
- If an employee uses a frequent flyer ticket for business travel, they cannot be reimbursed for it in any way.

Saturday night stay

- The company encourages employees to make Saturday night stays when the total travel expense is less than by not staying over a Saturday night.
- Entertainment and other personal expenses incurred by the employee during this period will not be reimbursed.
- Please provide a worksheet showing the airfare with and without the Saturday night stay and the hotel/meal costs for the additional days to document the savings.

International travel

- The company will reimburse for the cost of coach transportation.
- In the rare circumstance where there is a health or business reason why an employee must upgrade to business class, such an upgrade must be approved by a Senior Manager and must be documented.

Currency exchange and ATM fees

- The company will reimburse employees for currency exchange fees.
- Employees are encouraged to pay for meals, hotels and purchases on their corporate or personal credit card as the cards often offer the safest and most economical currency exchange conversion.
- The company discourages employees from carrying large amounts of cash while traveling. In most cases, using an ATM machine will provide an excellent exchange rate and will reduce the amount of cash the employee has on his/her person.
- ATM fees for cash withdrawals will be reimbursed.

Rental car

- Employees should rent a car only when it is required for daily use at the business destination or there is no other less expensive means of transportation.
- If an employee rents a car for one week and uses the car partially for business and partially for personal use, the weekly cost of the car must be prorated.
- Rental cars should be appropriate size based on the number of employees traveling.
- Review the fuel policy of the rental agency to avoid excessive refueling charges.

Auto insurance - rental cars

- The company 's commercial automobile policy and the employee's personal auto insurance policy will provide sufficient automobile insurance coverage. Employees do not need to purchase additional insurance from the rental agency.
- Employees should be aware that only listed drivers are covered by insurance and there are additional charges for additional drivers to be eligible to drive rental cars. Employees must make sure that all potential drivers are listed and be aware that if those additional drivers are not employees the additional cost is not reimbursable.

Local transportation companies

- Employees should explore utilizing free airport/hotel shuttles when available.
- When airport/hotel shuttles are not available, the cost of a taxi will be reimbursed.
- There are several “limo” and taxi services available locally. Each service has a set fee to various destinations and the most economical service should be selected.
- The employee should ask for a signed invoice at the conclusion of the trip.
- Employees who choose to leave the driver a tip should so indicate that on the invoice. Tips should be *reasonable* (no more than 15%).
- Limos and other luxury vehicles will not be covered.

Lodging

- The company will reimburse the actual cost for average accommodations up to the single occupancy rate. The IRS states that expenditures for lodging cannot be lavish or extravagant.
- Movies and other entertainment charged to the room will not be reimbursed.
- Health Club charges, golf, mini-bar and other personal services will not be reimbursed.
- When traveling with a companion, the employee is responsible for any additional charges above single occupancy.
- The detailed itemized bill from the hotel must be submitted as supporting documentation for reimbursement. In addition, the detailed bill for any restaurant expenses charged to the room must be submitted.

Local (in town) meals

- A "business meal" is defined as a meeting that is held during mealtime where the main purpose of the meeting is business and a meal is served.
- In the case where employees must meet during the dining hour to discuss business, the cost of the meal will be reimbursed or may be charged to the company.
- Routine get togethers with associates are not considered business meals. Business meals must have a stated business purpose.
- Supervisors wishing to recognize an employee or a department with a lunch, or supervisors holding a meeting during the lunch hour, is an acceptable practice and will be reimbursed.

Meals while traveling

- Meals for employees while away on company business or while conducting company business will be reimbursed.
- Meal costs for business related participants will also be reimbursed. The location of the business meal does not change the reporting requirements.
- The same IRS rules apply to meals taken locally or out of town. The IRS states that expenditures for meals cannot be lavish or extravagant. Regardless of the cost of the meal, employees must provide documentation on
    - attendees
    - discussion topic(s)
    - cost
    - location (restaurant name, etc.)
    - date
- Receipts are requested for all meals.
- The company will reimburse the reasonable and actual cost of meals, including gratuities, while on business.
- The company will reimburse for breakfast, lunch and/or dinner when there is a business reason for the meal.

Alcohol

- Employees are expected to act responsibly in relation to alcohol consumption while on a business trip.
- The cost of a beverage with dinner will be reimbursed as part of the meal expense.
- Very expensive bottles of wine, drinks that are not associated with a meal, or drinks taken at a bar will not be reimbursed.

Gratuities

- Tips at the standard 15% (18% in major cities) on meals are reimbursable.
- Tips on meals should be included as part of the cost of the meal on the Travel Expense Report.
- Tips to bellhops, maids, etc. should be totaled and listed separately on the Travel Expense Report under the appropriate section.

Registration fees

- Registration fees will be paid directly to the sponsor organization. An accounts payable voucher with the appropriate manager approval and supporting documentation should be submitted for processing to Accounts Payable.
- Please allow enough time to process the accounts payable request and have your registration received by the deadline.
- If you must pay a registration fee directly and request reimbursement, a copy of your canceled check must accompany the request.

Telephone

- All business calls made while away from the office will be reimbursed.
- Reasonable calls to the employee's home will also be reimbursed (i.e. one call per day of reasonable length).
- Direct long distance calls from the hotel room are extremely expensive and should be avoided. Employees are encouraged to use a calling card, phone credit card or cell phone.
- If you travel extensively for business, consider requesting a corporate phone card or cell phone through the Purchasing Department (x5550).
- When an employee uses his/her personal phone calling card an accounts payable voucher should be submitted with a copy of the bill when received.

Cell phones

- Certain employees are issued a company cell phone for emergency contact and other business purposes. These cell phones are intended for job-related activities. Please refer to the company's Phone Usage policy for further information.

Internet access or remote access to company computers

- In some cases, it is critical for company employees to have access to the Internet while away on business. The company has procedures that must be followed to insure access in the most secure and economical way.
- Employees should consult with the appropriate person in their department or with the IT Department to acquire the necessary access numbers.
- Charges for Internet access outside of the company’s procedures may not be reimbursed.

Non-reimbursable expenses

The following items will **NOT** be reimbursed by the company:

- Fines for parking or moving violations
- Movies, health club fees, golf, or other personal entertainment
- Laundry services (if trip is less than five days)
- Lost or stolen personal property (including cash)
- Costs incurred at home, such as childcare, pet care or lawn/home maintenance
- Personal expenses such as haircut, toiletries, clothing, etc.
- Costs incurred due to unreasonable failures to cancel transportation or hotel reservations
- Companion expenses (including travel, meals and additional driver costs on rental cars)
- Life, flight or baggage insurance
- Excess baggage charges for personal items (i.e. golf clubs, skis)
- Unnecessarily excessive costs (i.e. very expensive restaurants or exclusive hotels) not warranted by the circumstances.
- Charitable or political contributions
- Mini-bar items
- Alcohol not associated with a meal
- Snacks, personal reading material

Note: *This list is not meant to be all-inclusive. Other items may be added to this list upon review.*

Travel expense report

- To obtain reimbursement for out of pocket travel expenses (those NOT charged to a company credit card or directly billed to the company), complete the Travel & Entertainment Expense Form on the Intranet.
- Travel reimbursement forms must be completed within 14 days of the return date of your trip and submitted with the required documentation to your manager for approval.
- Small receipts must be taped onto one page and clipped (no staples please) to the travel expense form. This eliminates the possibility of a lost receipt and reduces the cost of scanning supporting documentation.
- The completed form with appropriate approval signatures should be submitted to the Accounts Payable office.
- When a refund is due to the company a check must be attached to the travel form.
- When a refund is due to the employee a check will be generated within 14 days of receipt of the travel expense form.
- For departments with Petty Cash, travel reimbursements under $30 should be made from the petty cash fund.

Samples:

Company Travel and Expense reimbursement form:

MDE Enterprises
MDE_Expense Report.xls

Travel & Expense Report

Name:			Emp.#		Accounting Use Only						
Dept. to be charged:		Purpose of Trip:			Dept#						
Location:		Week Ending:			Dept#						
					Dept#						
Employee Signature:		Date:			Dept#						
					Dept#						
Approval Signature:		Date:					Total				

TRANSPORTATION/LODGING EXPENSES

		Auto			Travel Expenses		Hotel Expenses				
					Ground transportation,						
Date	Description	# miles @		Amount	Parking, Cabs, Rental	Airfare	Misc.	Phone	Room	Meals	Total
			0.345	0.00							0.00
			0.345	0.00							0.00
			0.345	0.00							0.00
			0.345	0.00							0.00
			0.345	0.00							0.00
			0.345	0.00							0.00
			0.345	0.00							0.00
		Sub-total		0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

ENTERTAINMENT EXPENSES:

Date	Description (Include purpose and people attending)	Total

MISCELLANEOUS EXPENSES:

Date	Description	Office Supplies	Misc.	Total		
				0.00	Total Expenses:	0.00
				0.00	Less expenses to Corp.Acct	0.00
				0.00	Less cash advance	0.00
				0.00		
				0.00	Tot. Reimbursable Expense	**0.00**

No. IT_10

Policy Name: Employee conduct

Objective:
Provide the company's policy regarding employee conduct, discipline, and termination.

Applies to:
All employees

Key guidelines:
This policy applies to all full-time and part-time employees of the company.

General

- Employees are expected to observe certain standards of job performance and appropriate conduct.
- When performance or conduct does not meet the company's standards, the company will endeavor, when it deems appropriate, to provide the employee a reasonable opportunity to correct the deficiency.
- If the employee fails to make the correction, they will be subject to discipline, up to and including termination.
- The guidelines set forth below are intended to provide employees with fair notice of what is expected of them.
- Such guidelines cannot identify every type of unacceptable conduct and performance. Therefore, employees should be aware that conduct not specifically listed below but which adversely affects the interests of the company or other employees may also result in corrective action or discipline.
- Nothing in this policy is intended to alter the "at will" status of employment with the company.
- The company reserves the right to terminate any employment relationship, to demote, or to otherwise discipline an employee without resort to these corrective action procedures.

Code of Ethics

- Employees are expected to conduct themselves in a manner that is consistent with the mission and values of the company.
- Employees must act with respect for the dignity of individual employees, managers, vendors, clients, and visitors reflecting a professional image of our company.
- When there is reason to believe that the conduct of an employee prevents or hampers other employees from performing their work or clients from receiving benefits or services from the company, the company may intercede.

Job Performance

Corrective action may be taken for poor job performance, including but not limited to:

- Unsatisfactory work quality or quantity
- Poor attitude (for example, rudeness or lack of cooperation)
- Failure to follow instructions of company policies or procedures
- Failure to follow established safety regulations.

Misconduct

Corrective action may be taken for misconduct, including but not limited to:

- Insubordination
- Dishonesty
- Theft
- Discourtesy
- Misusing or destroying company property or property of others on company premises
- Violating conflict of interest rules or policies
- Disclosing or using confidential or proprietary information without authorization
- Falsifying or altering company records, including the application for employment
- Interfering with the work performance of others
- Altercation
- Harassing, including sexually harassing, employees or others
- Being under the influence of, manufacturing, distributing, using, or possessing alcohol or controlled substances on company property or while conducting company business
- Gambling on company premises or while conducting company business
- Sleeping on the job or leaving the job without authorization
- Possessing a firearm or other dangerous weapon on company property or while conducting company business
- Being convicted of a crime that indicates unfitness for the job or raises a threat to the safety or well-being of the company, its employees or property

Attendance

Corrective action or discipline may be taken when employees fail to observe the following specific requirements relating to attendance:

- Reporting to work on time, observing the time limits for rest and meal periods, and obtaining approval to leave work early
- Notifying the supervisor in advance of anticipated tardiness or absence
- Employees who are frequently absent or tardy and/or absent without notifying their supervisors are subject to discipline.
- Employees who are absent for three consecutive working days, without notifying their supervisor are considered to have resigned their position.

Dress Code

Employees failing to comply with company's standards for dress are subject to corrective action or discipline.

- Discretion in style of dress and behavior is essential to the image and the safe and efficient operation of the company.
- Employees are expected to dress in a manner appropriate to the type of work performed.
- It is important that all employees project a professional image to the people with whom they interact internally and externally.
- Managers in consultation with the appropriate Vice President may enhance dress code requirements.
- Specific work days or work occasions may be deemed appropriate for business casual attire.
- The following are acceptable guidelines for business casual attire:
    - slacks and skirts
    - appropriate business casual does not include jeans, athletic attire (sweatshirts, sweatpants, gym shoes), T-shirts, spandex, casual sandals or shorts.
    - business casual attire is considered the minimum level of appropriate professional dress.
- Employees must abide by the safety policies and procedures of their department and wear protective clothing or safety equipment when required.
- Unique scheduled work activities may necessitate an exception to the Dress Code which will require approval of the supervisor and/or appropriate Vice President.

Procedures

- Dismissal or demotion for poor performance will ordinarily be preceded by an oral warning and followed by a written warning.
- The company reserves the right to proceed directly to a written warning, or demotion, or termination for misconduct of performance deficiency, without resort to prior disciplinary steps, when the company deems such action appropriate.
- Both oral and written warnings should cover:
    - The nature of the poor performance
    - What is required to correct the poor performance
    - How long the employee has to correct the poor performance
    - The consequences of failure to correct the poor performance (for example, more severe discipline, termination, etc.).
- A written memo of an oral warning should include the following and filed in the manager's employee file folder:
    - date
    - name of the employee
    - subject discussed
    - corrective action presented
    - summary of the discussion

- Documentation for a subsequent warning must be forwarded to Human Resources, along with documentation of the first warning kept in the employee's personnel file.
- All written warnings must be approved by Human Resources and should detail the issue(s), refer to previous oral warnings and include expectations and deadlines for achieving acceptable performance.
- Written warnings will clearly state that failure to achieve the expectations and deadlines will result in further action up to and including termination.
- Both the employee and the supervisor should sign written warnings. If the employee refuses to sign the warning, the supervisor shall request another supervisor or a representative from Human Resources to sign the document, in the presence of the employee, as a witness that the warning was received by the employee.
- The employee may submit a written response to the written warning for the personnel file.
- If, subsequent to receiving a first warning, an employee works 18 months without receiving another warning, the first warning shall not be counted against the employee as a first offense.

Responsibility

- The Director of Human Resources is principally responsible for the implementation of this policy throughout the company.
- Any company manager or supervisor is responsible for the implementation of and compliance with this policy for employees under their supervision.

Samples:

None

For questions, call:

For questions or comments, please call your IT Department at Ext. 5555.

Last revision date:

December 12, 2003

No. IT_11

Policy Name: Employee non-compete

Objective:

Provide guidelines regarding employee "non-compete" issues that protect company assets and promote goodwill with former employees

Applies to:

All employees

Key guidelines:

Employees of the company are our most valuable assets. As such, we require every new employee to sign a "non-compete" agreement. These steps are taken to improve our competitive edge and protect the investment we make in our employees.

- The Employee Non-Compete Agreement is signed by new employees. If the employee later leaves the company, this agreement prevents him/her from competing against the company, recruiting other employees, or misusing confidential information.

Justification for the policy

- The agreement provides the company protection in four key areas:
    1. Prohibits a former employee from working with a competitor.
    2. Prohibits a former employee from soliciting current employees to be employed in his or her new company.
    3. Prohibits a former employee from disclosing confidential information learned in the course of employment with our company.
    4. Protects the investments made in the company's employees.

Samples:

Employee Non-Compete agreement

EMPLOYEE NON-COMPETE AGREEMENT

For good consideration and as an inducement for_____ (Company) to employ _____ (Employee), the undersigned Employee hereby agrees not to directly or indirectly compete with the business of the Company and its successors and assigns during the period of employment and for a period of _____ years following termination of employment and notwithstanding the cause or reason for termination.

The term "not compete" as used herein shall mean that the Employee shall not own, manage, operate, consult or to be employed in a business substantially similar to, or competitive with, the present business of the Company or such other business activity in which the Company may substantially engage during the term of employment.

The Employee acknowledges that the Company shall or may in reliance of this agreement provide Employee access to trade secrets, customers and other confidential data and good will. Employee agrees to retain said information as confidential and not to use said information on his or her won behalf or disclose same to any third party.

This non-compete agreement shall extend only for a radius of_____ miles from the present location of the Company and shall be in full force and effect for_____ years, commencing with the date of employment termination.

This agreement shall be binding upon and inure to the benefit of the parties, their successors, assigns, and personal representatives.

Signed this _____ day of _____ 20____.

_____
Company

_____
Employee

For questions, call:

For questions or comments, please call your Human Resources Department at Ext. 5559.

Last revision date:

December 12, 2003

No. IT_12

Policy Name: Employee non-solicitation

Objective:

Provide guidelines intended to prevent former employee solicitation of clients or other employees or in sharing confidential information with competitive organizations

Applies to:

All employees

Key guidelines:

This policy has been established to protect and retain key assets of the company including clients, employees, and confidential information.

- The Employee Non-solicitation Agreement policy is intended to protect the company's interests by preventing former employees from:
    - soliciting clients
    - soliciting current employees
    - sharing confidential and proprietary company information outside of our company.
- Employees are provided knowledge of company confidential information such as client lists, employee lists, pricing strategies, marketing and sales strategies, trademark or copyright information, and other insight that managed inappropriately can create significant damage to the company. It is the responsibility of each employee to maintain strict confidence with any and all information which the company deems proprietary and confidential in nature.
- All new employees are expected to read, understand, and sign the company's Employee Non-solicitation Agreement on or before their first day of employment.
- It is each manager's responsibility to insure the Employee Non-solicitation Agreement is signed by new employees on or before their first day of employment.
- Any employee who becomes aware of a breach in the agreement by a former employee should notify the Director of Human Resources.

Samples:

EMPLOYEE NON-SOLICITATION AGREEMENT

This Non-Solicitation Agreement dated {Date} is made between:

_____ (Employee) and _____ (Company)

WHEREAS {Company} has offered to employ {Employee} in its {Location} office;
AND WHEREAS {Company} will be revealing to employee confidential information such as existing pricing structures to customers, marketing strategies, overall pricing and service strategies for new business and existing business, and putting employee in contact with {Company}'s existing customers in order to develop {Company}'s goodwill and customer relations so that the employee can promote {Company}'s interests and objectives;

NOW THEREFORE in consideration of the mutual benefits and premises made herein, the hiring of the employee by {Company}, as well as the salary paid from time to time for the employee's services, {Company} and the employee agree with each other as follows:

1. The employee understands that {Company} is a profit corporation which must work in a competitive environment and is entitled to limit reasonably an employee's unfair competition following the end of the employee's employment. As a result, the employee agrees as follows:
    a. Employee agrees that for a period of {Months' Non-Solicitation} months after resignation or termination with or without cause that he/she will not directly or indirectly solicit business from any client or customer of {Company} , whether potential or otherwise, with whom he/she had dealings during his/her employment with {Company};
    b. The employee agrees that for a period of {Months' Non-Solicitation} months after resignation or termination with or without cause that he/she will not directly or indirectly entice, encourage or otherwise ask current {Company} employees to leave their current employment to work with or for another business that competes with {Company};
    c. Employee agrees that for a period of {Months' Non-Solicitation} months after resignation or termination of employment with or without cause that he/she will not be employed or associated with any competitive business or enterprise which has a former employee of {Company} who is subject to a similar restriction which has not expired where he/she being so employed or associated with that person may cause substantial damage to the business interests of {Company} This clause does not prevent the employee from working with a competitor of {Company} except in the circumstances described;
2. The employee acknowledges and confirms the scope of this undertaking in respect of its area, time and subject matter is no more than what is reasonably required to protect {Company}; and
3. This agreement in no way relieves the employee of any fiduciary obligations the employee owes to {Company}.
4. This agreement shall be governed by the laws of the United States and the state of {State}.
5. Any claim or dispute arising out of or related to this agreement or its interpretation shall be brought in a court of competent jurisdiction sitting within the State of {State}.
6. The employee acknowledges that he/she has been invited to obtain independent legal advice as to the terms of this agreement.
7. The terms of this agreement are separable. The invalidity of one clause does not invalidate the agreement.

Signed this ____ day of _____, 20_____.

_____ _____
Company Representative Employee

For questions, call:

For questions or comments, please call your Human Resources Department at x5550.

Last revision date:

December 12, 2003

No. IT_13

Policy Name: Performance plans and reviews

Objective:

Provide management guidelines regarding the implementation of Employee Performance Plans and Reviews

Applies to:

Managers

Key guidelines:

It is important for each manager of the company to proactively manage the development and performance of his/her employees. Performance plans and reviews are possibly the best tools to help your department achieve higher levels of performance from your staff.

Performance planning

- Managers will develop and deliver annual performance plans for all employees under his/her responsibility.
- New employees should receive a performance plan with an expectation to be reviewed after 90 days of working with the company.
- An employee's performance plan should include, but is not limited to, the following areas of performance:
    - Technical knowledge and productivity
    - Client service
    - Communication
    - Teamwork and leadership
    - Education and training
    - Process and standards
- Performance plans offer the manager an excellent means of defining exactly what you expect of each employee. In that regard, plans are expected to be unique for each individual.
- Emphasize major areas of importance by placing higher "weighting factors" on elements of the performance plan.

Performance reviews

- Employees should be reviewed at least once every twelve months.
- New employees should be reviewed at the end of their first 90 days employment.
- Managers should use a rating system that allows you to rate employee performance in terms of:
    - Outstanding
    - Exceeds requirements
    - Meets requirements
    - Needs improvement
    - Unacceptable
- Interim reviews and coaching sessions are appropriate to help employees perform better and to make them aware of improvements needed. There should be no real surprises at the annual review session if managers are communicating effectively and providing appropriate feedback.
- Performance reviews should be signed and dated by both the employee and manager conducting the review.
- Performance plans should be filed in the manager's employee file and a copy sent to Human Resources to be filed in the employee file.
- Salary increases do not necessarily follow a performance review. Timing of salary increases should be appropriate to the responsibility, experience, and performance of the individual.

Samples:

Sample Performance Plan template

Employee Performance Plan

Name: _____ **Position:** _____ **Date:**_____

I. Technical Knowledge & Productivity

A.
B.
C.

II. Client Service

A.
B.
C.

III. Teamwork/Leadership

A.
B.
C.

IV. Processes & Standards

A.
B.
C.

V. Communication

A.
B.
C.

VI. Education/Training

A.
B.
C.

VII. Miscellaneous

A.
B.
C.

Weighting factors are: 1 - high; 2 - medium; 3 - low
Grading Scale: 1– Outstanding; 2– Exceeds; 3- Meets; 4- Needs Improvement; 5 - Unacceptable

Manager Signature: _____ **Date:** _____

Employee Signature: _____ ***Date:*** _____

For questions, call:

For questions or comments, please call your IT Department at Ext. 5555.

Last revision date:

December 12, 2003

No. IT_14

Policy Name: Training and reimbursement

Objective:
Provide guidelines regarding the company's training and reimbursement policy

Applies to:
All employees

Key guidelines:
The company encourages the investment of training and education in all levels of our employee base to increase employee skill, performance, and opportunity. The following guidelines will help manage the use of training and education in the company.

General

- Training and education requests should be for training that enhances the skills of the employee to do a better job in his/her position or that positions the employee for a new responsibility within the company.
- All training requests must be approved by the employee's manager.
- The company provides in-house training for certain skilled positions and in developing employee professional skills such as communication, client service, etc. Employees are encouraged to sign up for these classes as available and upon approval from their manager.
- Training and education programs should be budgeted for. Each manager is responsible for operating within operating budget commitments.
- Managers are encouraged to include in each employee's annual performance plan specific training and education programs that improve the employee's skill and help the organization achieve more success.

Internal company education

- All employees are eligible for internal education classes provided by the company.
- Selected classes should be appropriate in developing skills to improve the employee's skills for current responsibility or that positions him/her for future responsibilities agreed upon by management.
- Management approval is required for all education.
- Available classes are posted on the company Intranet.

External education

- External classes that enhance employee skills or help an employee stay current with technology or industry trends are encouraged.
- External classes must be approved by management and fall within operational budget commitments.
- External classes must pertain to the employee's current or future responsibilities.
- External classes and associated travel expenses are reimbursed fully.

College level education

- Qualified employees (full time with more than 6 months service) are eligible for college courses that lead to certifications or degrees upon meeting certain guidelines:
    - The course must lead to a degree or certification that is consistent with the employee's current responsibility or positions the employee for a new responsibility agreed upon by management.
    - All courses must be approved by the employee's manager.
    - Employee must receive a grade of B or above for reimbursement.
- The company will reimburse 75% of college level education courses upon meeting requirements.

Samples:

None

For questions, call:

For questions or comments, please call your Human resources Department.

Last revision date:

December 12, 2003

No. IT_15

Policy Name: Working from home

Objective:
Provide management guidelines on managing "Work at home" employees.

Applies to:
All Managers

Key guidelines:
The company encourages a work at home policy for departments that are available to take advantage of home workers and can manage them in such a way that improved productivity and cost effectiveness can be validated.

General

- Work at home capability is not a universal benefit for all employees of the company. It is not available for every job or for every employee in an approved department.
- Work at home is encouraged for departments to use when the results are beneficial in improving productivity and/or cost effectiveness of the department.
- All work at home approvals are made by a Department Manager.
- Only eligible employees may apply for a work at home position.

Eligibility criteria

- Employees satisfying the following criteria may apply for a work at home status:
    - No pending personnel related disciplinary action
    - Portable job duties (the job is an approved work at home position)
    - Availability of a work site suitable for telecommuting
- Eligibility is approved at the sole discretion of the department.
- The department reserves the right to waive any of the above criteria if it is in the best interest of the department.
- Employee has been a full time employee for six months or more.

Selection criteria

- Selection is the sole discretion of the department manager.
- The criteria used for selection includes, but is not limited to the following:
    - Employee meets eligibility criteria
    - Supervisor agreement and approval
    - Nature of the work to be accomplished
    - Job duties with clearly defined deliverables that are measurable and results oriented
    - Willingness to participate in telecommuting training
    - Successful performance of current duties for at least 6 months
    - Achieves the business needs of the department
    - Ability of the employee to adapt to a telecommuting environment
    - Current and past performance reviews meet or exceed requirements
    - Availability of computers and other telecommuting equipment

Position suitability

- Some positions are more suitable than others for work at home employees.
- The Department Head will make the final determination for which positions are acceptable for work at home employees.
- The Department must be able to:
    - Define specific job functions
    - Define process by which performance can be monitored and measured to insure the position is productive when worked from home
    - Define specific measurement criteria that measures:
        - Results
        - Capacity of work completed
        - Quality of work
        - Cost effectiveness

Participant suitability

- Characteristics of appropriate participants include:
    - Dependable
    - Self motivated and responsible
    - Knowledgeable about the department policies and procedures
    - Independent worker needing minimal supervision
    - Possesses good organizational skills
    - Effective communicator
    - Adaptable
    - Results oriented

Monitoring work at home participants

- Department Managers are responsible for defining the means of monitoring each work at home position deployed in the department.
- Specific measurements should be established and approved by Senior Management that measures:
    - Activity
    - Productivity
    - Results
    - Quality
    - Responsiveness to issues
    - Cost effectiveness

Home conditions

- It is the responsibility of the work at home individual to set up an appropriate work space in his/her home that is conducive to an effective work environment.
- Specific requirements as to equipment, computer and software, file information, etc. will be defined by the Department manager in conjunction with the IT Department.

Termination

- The employee or the Department Manager may terminate the work at home situation for the employee at any time.

Samples:

None

For questions, call:

For questions or comments, please call your IT Department at Ext. 5555.

Last revision date:

December 12, 2003

No. IT_16

Policy Name: Inventory and equipment

Objective:
Provide management guidelines for managing the use and security of company inventory and equipment

Applies to:
Managers

Key guidelines:
PC's, equipment, and supplies are purchased for company employee use and productivity. It is the responsibility of all employees and managers to manage the security of company equipment and supplies in order to cost effectively manage the company's expense in these areas.

Allocating equipment to employees

- Equipment is assigned to employees based upon their job function.
- Managers should maintain a list of equipment allocated to each of his/her employees. (See sample Employee Inventory Allocation log)
- Specific equipment should be tracked by employee includes, but is not limited to:
    - PC's (both desktop and laptop)
    - PC peripherals (scanners, printers, modems, etc.)
    - Faxes
    - Pagers
    - Cell phones
    - Building access keys and access cards

Employee termination

- One of the responsibilities of the manager is to collect all allocated equipment issued to an employee who leaves the company. Maintaining the Employee Inventory Allocation Log makes it a simple process.
- Employees not able to return allocated equipment are responsible for reimbursing the company for the fair market value of the item.

Technology assets

- The IT Department will maintain an accurate inventory of all networked technology assets, laptops, and tangible technology equipment valued at over $250.00 of the company to include the following information:
    - Item
    - Company ID#
    - Serial #
    - Basic configuration (i.e., Dell PC Desktop -1GB RAM, 100GB FD, CD-RW)
    - Physical location
    - Operating system release level
    - Date placed in service
    - Original cost
- Technology equipment will be tagged for easy identification.
- Periodic inventory audits will be conducted to validate the inventory and to identify maintenance issues needed for employee productivity.

Samples:

Department Employee Inventory Allocation log

_____ Dept. Employee Inventory Allocations						
Employee	PC	PC Peripheral	Cell phone	Pager	Keys	Other
Bob Example	DT Laptop	HP820 HP scanner	1		Bldg A Data Ctr.	Fax
Totals	1– DT 1-Laptop	1-HP820 1-HP scanner	1	0	1-Bldg A 1-Data Ctr.	1-Fax

For questions, call:

For questions or comments, please call your IT Department at Ext. 5555.

Last revision date:

December 12, 2003

No. IT_17

Policy Name: PC standards

Objective:

Provide guidelines for maintaining a standard PC image for the company that addresses the needs of company employees

Applies to:

All employees

Key guidelines:

The company will maintain standard configurations of PC's and laptops in order to enhance employee productivity and supportability of the company's network.

General

- The IT Department will establish the standard configuration of PC hardware and software to be run on company PC's and laptops.
- Multiple configurations are maintained to provide stronger capabilities for employees that need more PC capabilities for their work. These users are called "Power users" and are determined to need the more capable PC's by their manager.
- On an exception only basis, a PC may be requested that does not meet the standards configuration. To request a non-standard PC, see **the PC Software Standards** policy for the *Requesting a Variance from the Standard* request form.

Network access

- All PC's are network enabled to access the company's network.
- It is the employee's responsibility to maintain appropriate security measures when accessing the network as defined in the company's **Password Security** policy.

PC Support

- The IT Department will maintain all PC's of the company or will direct you to appropriate measures for maintaining your PC.
- Standard configurations are defined to assist in providing responsive support and to assist in troubleshooting your issue or problem. Deviations from the standards are not permitted except in appropriately reviewed and approved situations.
- For assistance with your PC or peripheral equipment, contact the IT Help Desk.

Employee training

- Basic training for new employees on the use of PC's, accessing the network, and using applications software is held every week by the IT Department. Published schedules are available on the IT Department's Intranet site.
- Training not listed on the IT Department's schedule may be requested or taken outside the company.

Backup procedures

- Network data and programs are backed up daily and archived off site in case of emergency.
- Data and software on your PC is not backed up. If you want to protect data and files used on your PC, you should take one of the following measures:
    1. Save the data onto diskettes or CD drive if you have a RW (Read-Write) CD drive.
    2. Copy the data to the appropriate network server and store it within your personal file folder specifically set up for this purpose. This will insure your important data is saved and archived daily in our normal backup process.
- Large amounts of data (over 10MB) should be discussed with the IT Department before uploading to a network server.

Virus software

- The company maintains network virus software that will automatically scan your PC for possible viruses each time you log onto the network.
- Downloading or copying data files from external systems and the Internet are prohibited without the IT Department's review and approval in order to protect the integrity of the company network.

Applications software

- Standard software is maintained on all PC's and laptops. See the **PC Software Standards** policy for more information.
- Under no circumstances are additional software programs allowed to be loaded onto a PC without the review and approval of the IT Department. This is a protective measure to avoid network problems due to viruses and incompatibility issues.

Samples:

See IT Department section of the company Intranet for current PC standards.

For questions, call:

For questions or comments, please call your IT Department at Ext. 5555.

Last revision date:

December 12, 2003

No. IT_18

Policy Name: Equipment requests (Adds, Changes, Deletes)

Objective:

Provide management guidelines on the proper steps and requirements for requesting equipment (adds, deletes, changes)

Applies to:

Managers

Key guidelines:

Guidelines for ordering new technology equipment or making changes to existing equipment are provided to streamline the order process and to assist the IT Department in fulfilling the request.

General

- Capital equipment items (over $500.00) must be budgeted and approved for purchase.
- All technology capital requests are reviewed and approved by the IT Department and Corporate Purchasing and Accounting Departments for appropriate need even when budgeted in the company's annual Capital Budget.
- Only Department Managers may submit equipment requests.
- Other forms are available for keys, phones, etc. The Equipment Request Form may also be used for these items, especially to assist in using one master form when ordering equipment for new employees.
- Published response times for various new equipment installations, changes, etc. are posted on the IT Department's Intranet site.
- Appropriate lead time of at least three work days should be taken into consideration when ordering new equipment, upgrades, equipment relocations, etc.
- The IT Department will maintain a small inventory of standard PC's and other heavily used equipment to minimize the delay in fulfilling critical orders.
- It is the manager's responsibility to provide enough lead time for new orders and change requests in managing his/her department effectively.

Procedures

1. Complete the **Equipment Request Form** (see Sample) for the equipment or service you need.
2. Have the Department Manager review and approve the request.
3. Submit the request to the IT Systems Support organization for review and follow-up.
4. The IT Systems Support organization will review the request for appropriateness based upon standards and capital equipment purchasing guidelines of the company. The IT organization will follow-up in one of the following ways:
    A. Forward the request to the Purchasing Department to order the equipment.
    B. Fill the order if equipment is available in inventory.
    C. Contact the requesting department for clarification.
    D. Decline the request and forward the request form along with an explanation back to the originating department.

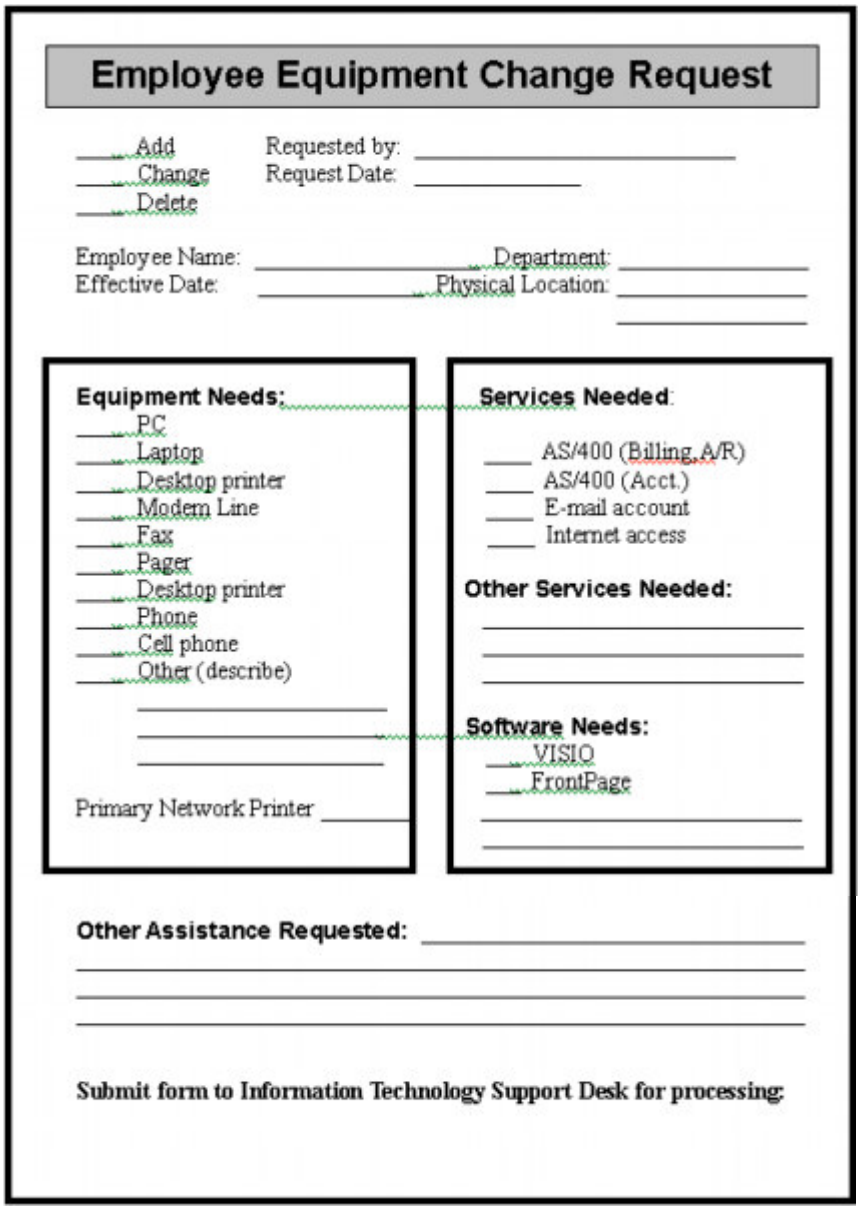
Approved equipment

1. If the equipment exists in inventory, the equipment is prepped as needed and installed for the requesting department.
2. If the equipment is ordered through Purchasing, the IT Department will either be notified of receipt at the requesting department or the equipment will be sent directly to the IT Department for prep, staging, and installation.

Support

For normal support of non-working technology equipment, contact your IT Support Help Desk at x5554.

Samples:
Equipment change request form



Employee Equipment Change Request

___ Add
___ Change
___ Delete

Requested by: _____
Request Date: _____

Employee Name: _____ Department: _____
Effective Date: _____ Physical Location: _____
_____

Equipment Needs:
___ PC
___ Laptop
___ Desktop printer
___ Modem Line
___ Fax
___ Pager
___ Desktop printer
___ Phone
___ Cell phone
___ Other (describe)
_____
_____
_____

Primary Network Printer _____

Services Needed:
___ AS/400 (Billing, A/R)
___ AS/400 (Acct.)
___ E-mail account
___ Internet access

Other Services Needed:
_____
_____
_____

Software Needs:
___ VISIO
___ FrontPage
_____
_____

Other Assistance Requested: _____
_____
_____
_____

Submit form to Information Technology Support Desk for processing.

For questions, call:
For questions or comments, please call your IT Department at Ext. 5555.

Last revision date:
December 12, 2003

No. IT_19

Policy Name: New employee startup

Objective:
Provide Managers guidelines to use when starting a new employee with the company.

Applies to:
Managers

Key guidelines:
Getting new employees off to a fast and productive start is important for the employee and for our company and sets the tone of professionalism we strive for.

General

The purpose of the New Employee Startup policy is to help the new employee:

- Feel at ease and welcome at our company.
- Obtain a good grasp of our company's organizational history, mission and values.
- Understand the functions of different units, divisions and departments.
- Understand what the organization expects in terms of work and behavior.
- Learn what is necessary to start performing his/her job.
- Know who and where to go to for help with work matters.
- Know the policies and procedures of the company and of the new employee's department.
- Feel a part of our company.
- Feel a sense of belonging to a professional and organized department and company.

Prior to first day

- Send offer/welcome letter and include job description.
- Notify unit personnel/payroll/benefits representative of the new hire.
- Prepare new employee packet, including:
    - Agenda for the first week
    - Company Mission
    - Company Organizational Chart
    - Employee handbook
    - Departmental Organizational Chart
    - Departmental mission, vision, and values
    - Departmental phone/e-mail directory
    - Emergency Procedures
- Notify IT Department Help Desk of new hire.
    - Order list of required software/hardware and other technology equipment.
    - Request network setup with assignment of primary network printer.
    - Request email setup.
    - Notify departmental telecommunications contact of hire.
    - Request phone hookup and voicemail setup.
- Prepare employee work area, including:
    - Order any needed desk supplies & furniture
    - Order a nameplate
    - Assign keys and keypad codes
- Make lunch plans for employee's first day.
- Identify employee(s) with similar responsibilities to function as the new employee's coach/mentor for work-related processes & procedures.
- Add employee to department and/or unit organizational contact and routing lists.
    - Prepare new hire paperwork (payroll & benefits information).
    - Prepare parking permit information/paperwork (if applicable).
    - Set up timesheet(s) or time reporting process (if applicable).
    - Confirm PC and network connectivity is activated with appropriate PC software installed.
    - Confirm e-mail account is active and send welcome email message.
    - Confirm phone and voice mail is active.

First day

- Send welcome e-mail to staff announcing the new employee's arrival, function and location.
- Warm welcome ideas:
    - Welcome signs/banner at desk
    - Coffee/donuts staff get together
    - Introduce employee to co-workers and buddy
    - Give brief tour of department
- Meet with personnel/payroll/benefits representative to complete new hire paperwork and to receive introduction to employee benefits.
- Obtain company Employee ID.
- Schedule attendance at New Employee orientation programs.
- Order business cards.
- Introduce employee to work area and office facilities, including:
    - Ergonomic Review – (Arrange for/make any needed adjustments.)
    - Use of phones
    - Departmental purchasing policies
    - Computer orientation – common programs, network access, etc.
    - Review & set up standard meetings
    - Benefit Representative or Disability Management Services
    - Coffee room
    - Restrooms
    - Photocopy machines
    - Fax machines
    - Supplies
    - Transportation
    - Break rooms
    - Conference rooms
    - Training facilities
    - Vending machines
    - Location of first aid and emergency supplies
    - Mail services
- Review departmental new employee packet, including:
    - Company Mission
    - Employee Handbook
    - Company Organizational Chart
    - Departmental Organizational Chart
    - Problem Resolution Channels
    - Departmental mission, vision, and values and the connection to the company's mission and values
    - Departmental phone/e-mail directory

- Review departmental policies and procedures concerning:
    - Probationary period
    - Timesheets or time reporting (if applicable)
    - Vacation and sick leave accrual and use
    - Dress Code
    - Hours of Work
    - Work Rules
    - Attendance Policy
    - Phone etiquette
    - Personal phone usage policy
    - Personal computer usage policy
    - Performance plan and appraisal process
    - Merit/salary increase timeline
- Introduce employee to job:
    - Review Job Description
    - Discuss supervisor's style and expectations
    - Review performance goals and expectations
    - Identify the "key players" connected to the position; make appointments with "key players" for brief orientation or responsibilities
    - Identify the "customers" served by this position; define customer service
    - Discuss employee safety
    - Review standard meetings the employee needs to attend
    - Identify training and development activities that will be needed in the next six months. Sign up for the appropriate classes.
- Meet weekly to complete orientation to work-related tasks and to ask/answer questions.
- Set performance expectations and discuss how and when the employee will be evaluated.
- Meet Department Head and other Senior managers as appropriate.

After 90 days

- Prepare formal 90-day employee evaluation.
- Celebrate completion of probationary period.

Samples:

None

For questions, call:

For questions or comments, please call your IT Department at Ext. 5555.

Last revision date:

December 12, 2003

No. IT_20

Policy Name: Information security

Objective:

Provide guidelines that protect the data integrity and proprietary nature of the company's information systems.

Applies to:

All employees

Key guidelines:

- By information security we mean protection of the company's data, applications, networks, and computer systems from unauthorized access, alteration, or destruction.
- The purpose of the information security policy is:
  - To establish a company-wide approach to information security.
  - To prescribe mechanisms that help identify and prevent the compromise of information security and the misuse of company data, applications, networks and computer systems.
  - To define mechanisms that protect the reputation of the company and allow the company to satisfy its legal and ethical responsibilities with regard to its networks' and computer systems' connectivity to worldwide networks.
  - To prescribe an effective mechanism for responding to external complaints and queries about real or perceived non-compliance with this policy.
- The company will use a layered approach of overlapping controls, monitoring and authentication to ensure overall security of the company's data, network and system resources.
- Security reviews of servers, firewalls, routers and monitoring platforms must be conducted on a regular basis. These reviews will include monitoring access logs and results of intrusion detection software.
- The IT Organization must see to it that:
  - The information security policy is updated on a regular basis and published as appropriate.
  - Appropriate training is provided to data owners, data custodians, network and system administrators, and users.
  - Each department must appoint a person responsible for security, incident response, periodic user access reviews, and education of information security policies for the department.

- Vulnerability and risk assessment tests of external network connections should be conducted on a regular basis.
- Education should be implemented to ensure that users understand data sensitivity issues, levels of confidentiality, and the mechanisms to protect the data.
- Violation of the Information Security Policy may result in disciplinary actions as authorized by the company.

Data classification

- It is essential that all company data be protected. Different types of data require different levels of security. All data should be reviewed on a periodic basis and classified according to its use, sensitivity, and importance.
- The company classifies data in the following three classes:
  High Risk - Information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure.

    - Data covered by federal and state legislation, such as FERPA, HIPAA or the Data Protection Act, are in this class.
    - Payroll, personnel, and financial information are also in this class because of privacy requirements.
    - The company recognizes that other data may need to be treated as high risk because it would cause severe damage to the company if disclosed or modified.
    - The data owner should make this determination. It is the data owner's responsibility to implement the necessary security requirements.

  Confidential – Data that would not expose the company to loss if disclosed, but that the data owner feels should be protected to prevent unauthorized disclosure. It is the data owner's responsibility to implement the necessary security requirements.

  Public - Information that may be freely disseminated.

- All information resources should be categorized and protected according to the requirements set for each classification. The data classification and its corresponding level of protection should be consistent when the data is replicated and as it flows through the company.
    - Data owners must determine the data classification and must ensure that the data custodian is protecting the data in a manner appropriate to its classification level.
    - No company owned system or network can have a connection to the Internet without the means to protect the information on those systems consistent with its confidentiality classification.
    - Data custodians are responsible for creating data repositories and data transfer procedures that protect data in the manner appropriate to its classification.
    - High risk and confidential data must be encrypted during transmission over insecure channels.
- All appropriate data should be backed up, and the backups tested periodically, as part of a documented, regular process.
- Backups of data must be handled with the same security precautions as the data itself. When systems are disposed of, or re-purposed, data must be certified deleted or disks destroyed consistent with industry best practices for the security level of the data.

Access control

- Data must have sufficient granularity to allow the appropriate authorized access.
- There is a delicate balance between protecting the data and permitting access to those who need to use the data for authorized purposes. This balance should be recognized and addressed appropriately.
- Where possible and financially feasible, more than one person must have full rights to any company owned server storing or transmitting high risk data.
- The company will have a standard policy that applies to user access rights. This will suffice for most instances.
- Data owners or custodians may enact more restrictive policies for end-user access to their data.
- Access to the network and servers and systems will be achieved by individual and unique logins, and will require authentication. Authentication includes the use of passwords, smart cards, biometrics, or other recognized forms of authentication.
- As stated in the Appropriate Use Policy, users must not share usernames and passwords, nor should they be written down or recorded in unencrypted electronic files or documents. All users must secure their username or account, password, and system from unauthorized use.
- All users of systems that contain high risk or confidential data must have a strong password, the definition of which will be established and documented by the IT Organization.

- Empowered accounts, such as administrator, root or supervisor accounts, must be changed frequently, consistent with guidelines established by the IT Department.
- Passwords must not be placed in emails unless they have been encrypted.
- Default passwords on all systems must be changed after installation. All administrator or root accounts must be given a password that conforms to the password selection criteria when a system is installed, rebuilt, or reconfigured.
- Logins and passwords should not be coded into programs or queries unless they are encrypted or otherwise secure.
- Users are responsible for safe handling and storage of all company authentication devices. Authentication tokens (such as a SecureID card) should not be stored with a computer that will be used to access the company's network or system resources.
- If an authentication device is lost or stolen, the loss must be immediately reported to the appropriate individual in the issuing unit so that the device can be disabled.
- Terminated employee access must be reviewed and adjusted as found necessary. Terminated employees should have their accounts disabled upon transfer or termination.
- Since there could be delays in reporting changes in user responsibilities, periodic user access reviews should be conducted by the unit security person.
- Transferred employee access must be reviewed and adjusted as found necessary.
- Monitoring must be implemented on all systems including recording logon attempts and failures, successful logons and date and time of logon and logoff.
- Personnel who have administrative system access should use other less powerful accounts for performing non-administrative tasks.
- There should be a documented procedure for reviewing system logs.

Virus prevention

- The willful introduction of computer viruses or disruptive/destructive programs into the company environment is prohibited, and violators may be subject to prosecution.
- All desktop systems that connect to the network must be protected with an approved, licensed anti-virus software product that it is kept updated according to the vendor's recommendations.
- All servers and workstations that connect to the network and that are vulnerable to virus or worm attack must be protected with an approved, licensed anti-virus software product that is kept updated according to the vendor's recommendations.
- Where feasible, system or network administrators should inform users when a virus has been detected.
- Virus scanning logs must be maintained whenever email is centrally scanned for viruses.

Intrusion detection

- Intruder detection must be implemented on all servers and workstations containing data classified as high or confidential risk.
- Operating system and application software logging processes must be enabled on all host and server systems. Where possible, alarm and alert functions, as well as logging and monitoring systems must be enabled.
- Server, firewall, and critical system logs should be reviewed frequently. Where possible, automated review should be enabled and alerts should be transmitted to the administrator when a serious security intrusion is detected.
- Intrusion tools should be installed where appropriate and checked on a regular basis.

Samples:

None

For questions, call:

For questions or comments, please call your IT Department at Ext. 5555.

Last revision date:

December 12, 2003

No. IT_21

Policy Name: Remote access

Objective:

Provide guidelines on appropriate use of remote access capabilities to the company's network, business applications, and systems

Applies to:

All employees

Key guidelines:

- The purpose of this policy is to define standards for connecting to the company network from a remote location outside the company.
- These standards are designed to minimize the potential exposure to the company from damages that may result from unauthorized use of the company resources. Damages include the loss of sensitive or confidential company data, intellectual property, damage to critical company internal systems, etc.
- This policy applies to all the company employees, contractors, vendors and agents with a company owned or personally owned computer or workstation used to connect to the company network.
- This policy applies to remote access connections used to do work on behalf of the company, including reading or sending email and viewing Intranet web resources.
- Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, cable modems, etc.
- It is the responsibility of the company employees, contractors, vendors and agents with remote access privileges to the company's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to the company network.

Remote connection

- Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong password phrases.
- At no time should any company employee provide his/her login or email password to anyone, not even family members.
- Company employees and contractors with remote access privileges must ensure that their company owned or personal computer or workstation, which is remotely connected to the company's corporate network, is not connected to any other network at the same time.
- The company employees and contractors with remote access privileges to the company's corporate network must not use non company email accounts (i.e., Yahoo, AOL), or other external resources to conduct the company business, thereby ensuring that official business is never confused with personal business.
- Routers for dedicated ISDN lines configured for access to the company network must meet minimum authentication requirements established by the IT Department.
- Frame Relay must meet minimum authentication requirements of DLCI standards.
- All hosts that are connected to the company internal networks via remote access technologies must use the most up-to-date anti-virus software.
- Third party connections must comply with requirements defined by the IT Department.
- Personal equipment that is used to connect to the company's networks must meet the requirements of the company-owned equipment for remote access.
- Organizations or individuals who wish to implement non-standard Remote Access solutions to the company production network must obtain prior approval from the IT Department.

Enforcement

- Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.
- The IT Department is responsible for monitoring remote access and addressing inappropriate use of remote access priviliges.

Samples:

None

For questions, call:

For questions or comments, please call your IT Department at Ext. 5555.

Last revision date:

December 12, 2003

No. IT_22

Policy Name: Privacy

Objective:
Provide guidelines on appropriate management of employee and client privacy

Applies to:
All employees

Key guidelines:
- This document describes the company's policy regarding the collection, use, storage, disclosure of and access to personal information in relation to the personal privacy of past and present staff, clients, and vendors of the company.

Handling personal information
- The following policy principles apply to the collection, use, storage, disclosure of and access to personal information:
    - The collection and use of personal information must relate directly to legitimate purposes of the company.
    - Individuals must be informed of the purpose for which personal information is obtained.
    - The company will take all reasonable measures to ensure that the personal information it receives and holds is up to date.
    - The company will take all reasonable measures to store personal information securely.
    - Individuals are entitled to have access to their own records, unless unlawful.
    - Third party access to personal information may only be granted in accordance with the procedures made pursuant to this policy.
    - The company will observe the principles defined in the ***US Privacy Act***.
- This Policy does not apply to personal information that is:
    - In a publication available to the public
    - Kept in a library, art gallery or museum for reference, study or exhibition
    - A public record under the control of the Keeper of Public Records that is available for public inspection
- The Privacy Officer shall be responsible for ensuring compliance with the policy
- This policy applies to all organizational areas and is binding on all employees.

Personal Information

- Information obtained by the company which pertains to an individual's characteristics or affairs.
    - The personal information can be recorded in any format - for example, in writing, online, digitally or by electronic means.

Privacy Officer

- A member of the company appointed to monitor compliance with this policy and to hear and determine complaints arising under the policy.
- The Privacy Officer's responsibilities will include:
    - Receiving and investigating complaints
    - Ongoing review of the company's practices and procedures to ensure that it complies with this Policy, current legislation and best practice
    - Educating company employees on their responsibilities under this policy and the ***Information Privacy Act*.**
    - The Privacy Officer is _____.

Complaints

- Any person, whether or not an employee of the company, who on reasonable grounds believes that a breach of this policy has occurred within the company, may complain to the company's Privacy Officer.
- The Privacy Officer shall investigate complaints as expeditiously as practicable and shall provide a written copy of the findings of fact and recommendations made to both the company and to the individual filing the complaint.
- The Vice President of Human Resources or nominee will determine what action will be taken on any recommendation contained in the findings of the Privacy Officer.

Samples:

None

For questions, call:

For questions or comments, please call your IT Department at Ext. 5555.

Last revision date:

December 12, 2003

No. IT_23

Policy Name: Service level agreements

Objective:

Provide guidelines for the IT Organization's commitment in providing Service Level Agreements.

Applies to:

Managers

Key guidelines:

- Service Level Agreements will be maintained between the IT Department of the company and its main users and includes data suppliers and output users
- These Service Level Agreements will be reviewed on a regular basis in order to provide flexibility in the light of changing needs.

Background

- The products and services offered by the IT Department need to be clearly defined and agreed upon with the major user departments, particularly funding partners and larger suppliers of data, in order to moderate potential demand.
- Demand for the IT Department's products and services is likely to increase over time and there should be clear agreement over the extent and type of information to be provided and over services to be carried out in respect to supporting the User.
- Part of the function of a Service Level Agreement is to manage expectations of both sides of the agreement.

Activities Supporting Service Level Agreements

- The IT Department will establish a basis upon which supplied services can be provided that will be agreed upon by its principal users and the company's IT management team.
- An approach is taken based upon the relative capacity and other work of the IT Department considered to be the best way of defining the basis for a Service Level Agreement.

- Within this framework, the IT Department and its users, will agree on:
    - the level of response considered acceptable
    - parameters by which that response is considered unacceptable
    - the kind of response expected by differing parties to the Service Level Agreement which can be defined in terms of products or by the duration of time needed to deliver a product.
- The Service Level Agreement will stipulate any limits applicable to the geographical extent of service and the nature of any level of responses, or kinds of products, which are outside the terms of the agreement.
- The agreement may stipulate the basis upon which such extra service(s) or product(s) might be made available.
- The Service Level Agreement will specify any cost of services that the IT Department may be charging for the agreed upon services or products.
- Service Level Agreements will specify any limitations in terms of duration of time to be spent, or kinds of products which will be made available, within such a service.
- Service Level Agreements will stipulate timeframes for their review specific to the products and services involved
- When required, the IT Department staff will operate a time-recording system to monitor the apportionment of time to specific areas of work under a Service Level Agreement, and will make use of this time record to inform both the recipient of services and the IT Department.
- When a work request under an existing Service Level Agreement is deemed by the IT Department manager to be impossible to meet, the requesting organization will be informed in writing not more than five days from receipt of the work request.
- Work requests under Service Level Agreements should be of reasonable operation (i.e. not all initiated within the last few days of an Service Level Agreement period).

Samples:
None

For questions, call:
For questions or comments, please call your IT Department at Ext. 5555.

Last revision date:
December 12, 2003

IX. Enforcing your Policies

Once you implement new policies you want to insure they are followed. You might think that this is a lot easier said than done and in some cases you will be correct. There are steps you can take to enforce your policies in a positive way and encourages employees to embrace new guidelines.

Here are a few things you should consider:

Provide training - Education and training is a very effective way to encourage employees to follow new policies. The better they understand why the policy exists in the first place and the benefits it provides the company the better. Employees tend to resist change but the resistance can be minimized by explaining what, why, and how.

Take prompt action - When non-compliance to company policies are discovered, it is important that there be an appropriate response that addresses the situation. An appropriate response might be a one-on-one coaching session or it might even mean that the employee should be fired.

Obviously, responding by terminating someone is a strong response and should only be a course of last resort or for the most flagrant violations, but if the policy helps to protect the safety of other employees and the company, you need to take it seriously.

If management takes a lighthearted approach, you can be certain that your employees will do the same.

My preferred response is always to provide education, coaching, and constructive feedback first. Everyone is entitled to a mistake and unless you are absolutely certain there could not possibly be any misunderstanding of the policy and consequences in disregarding it, you should err on the side of the employee.

Monitor - There are always means by which you can inspect to verify that your policies are being followed. Individual policies may offer different methods of monitoring them so take approaches that are cost effective and do not make your employees feel as though "big brother" is always watching over their shoulder.

Encouragement in doing the right thing and complying to company policies is always a better approach than using a "heavy hand" to try to force your employees to comply.

In flagrant situations you may need to install technology monitoring systems or equipment such as facility cameras, phone long distance monitors, email filters or other technology to manage the security of your business and monitor activities of employees.

X. Policy and Procedure Resources

There are many resources available that you might want to look into when preparing to develop policies and procedures for your company. Listed below are a few resources available as of this writing that you may want to check out.

IT Professional's Guide to Policies and Procedures
TechRepublic www.techrepublic.com
A collection of policies and procedures from various contributors.

Establishing a System of Policies and Procedures
Achieving 100% Compliance of Policies and Procedures
7 Steps to Better Written Policies and Procedures
Best Practices in Policies and Procedures
Author: Stephen Page http://www.companymanuals.com/index.htm
Four titles from a professional policy and procedure writer

Writing Effective Policies and Procedures: A Step-By-Step Resource for Clear Communication
Author: Nancy Campbell

Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management
Author: Thomas R. Peltier

How to Write Policies, Procedures & Task Outlines: Sending Clear Signals in Written Directions
Authors: Larry Peabody, John Gear

Information Systems Policies and Procedures Manual
Author: George Jenkins

Policy and Procedure Manual
www.policyandproceduremanual.com
A software approach to developing policies and procedures. Includes samples.

IT Policies and Procedures: Tools and Techniques that Work
Author: George Jenkins, Michael Wallace

Business and Legal Resources
Lots of policies and procedurs available for an annual subscription fee.
http://www1.hrnext.com/Article_List.cfm/Nav/2.5.0.0

Internet
Research policies and procedures through the search engines such as Yahoo, Google, MSN, etc. You will find lots of resources and examples.

Your industry
Check out companies and professional organizations in your industry.

Your Human Resources Department
If HR doesn't already have what you need, they may know where to find it.

XI. Conclusion

Developing and implementing policies and procedures is not one of the more fun parts of managing an IT Organization. In fact, it can be boring and something you just don't want to work on.

On the other side of the coin, they can help protect your company from significant risk and liability so they are needed. They can also be effective in channeling employee behavior in a manner that improves productivity, reduces error, improves quality, and provides real value to your business.

Don't overlook the potential benefit that can be derived by inserting just the right amount of policies and procedures for your company. Take the time and make the effort to write them in a clear and concise manner and the results can be very positive.

Implement them in a way that embraces the value for the business and reinforces department "partners" and you have a winning formula.

There are many resources available to help you get the job done. Take advantage of them to your best benefit and develop policies and procedures for your company that have a positive impact.

Best of success.

Mike Sisco

MDE Enterprises
mike@mde.net

APPENDIX A - DEFINITIONS

Accountability Holding people responsible for their actions.

Building Security Officer Each building will designate a senior resident manager as Building Security Officer who takes ultimate responsibility for building security.

Cable Modem Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.

Company information Information or data which relates to, and belongs to your company. Information which is created and shared in the company's interest.

Content Provider The person who supplies information to be posted on an Internet service. The content provider may provide the information directly to the system owner or indirectly through the webmaster.

DLCI Data Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network, and has local significance only to that channel.

Dial-in Modem A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.

Dual Homing Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the Corporate network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP). Being on a company provided Remote Access home network, and connecting to another network, such as a spouse's remote access.

DSL Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).

Electronic data interchange Includes electronically sharing of data related to such things as orders, invoices, paychecks, payments, inventory management records, etc.

Encrypted Date that is coded so as to ensure that unapproved, unauthorized individuals can't access confidential information.

Firewall A combination of software and hardware that maintains security of a network from the external Internet. It keeps people outside of your Intranet from accessing information on your network.

Frame Relay A method of communication that incrementally can go from the speed of an ISDN to the speed of a T1 line. Frame Relay has a flat-rate billing charge instead of a per time usage. Frame Relay connects via the telephone company's network.

Internet A global public network of independent hosts and communications facilities, which connect users to those hosts. The term "Internet" also may refer to the content presented on the hosts or transmitted through the network.

Internet Protocol (IP) The standards by which computers talk to other computers via the Internet.

IP Address A number that identifies a computer that is linked to the Internet. When displayed, an IP address is typically written as four numbers separated by periods (e.g., 24.12.33.56).

Internet Services Service offered to the public for exchanging information. These services include but are not limited to web pages, file transfer, remote log-in access, web sites, and established electronic discussion groups available to employees, contractor support personnel, consultants, etc., using computing or network resources.

Intranet Services Your company's own internal Internet. The Intranet links your organization and your employees together and is the primary source of company information for company employees.

Intrusion Any external unauthorized access to your network.

Personal Information Information which is not created for the benefit of your company. For example, personal e-mail messages to children, family and friends.

Personally initiated or motivated home pages Web sites which are set up strictly for personal reasons. They are not permitted.

Privacy Review A review conducted by the manager of the content provider to ensure information provided to an Internet service is not regulated by the Privacy Act. This review must be conducted prior to providing information through an Internet service.

Registration An approval process that must be conducted on each existing Internet service to continue operation. New Internet service must be registered prior to going online.

Remote Access Any access to the company's corporate network through a non-company controlled network, device, or medium.

Restricted sites Sites which represent no value to your company and which the company has deemed "off-limits" (for example, pornographic content).

Security Audit An audit of the security configuration on the Internet service. The audit assesses the Internet service's compliance with its Security Practice Agreement.

Security risk Any activity or behavior which could result in your company's information being compromised.

Server A computer system that provides network service such as disk storage and file transfer or the program that provides such a service for the requestor.

System An assembly of computer hardware, software, or firmware configured for the purpose of classifying, sorting, calculating, computing, summarizing, transmitting and receiving, sorting, or controlling information with a minimum of human intervention.

System Owner The manager responsible for the organization that sets policy, direction, and manages funds for an information system; i.e., owns the system. Systems under development are owned by the developing organization until accepted and authorized by the operating organization. The system owner provides a system to host applications on.

Uniform Resource Locator (URL) The path descriptor to a specific network resource and the protocol used to access it (i.e., www.mde.net). The global address of documents and other resources on the Internet.

Value The benefit using this technology contributes to the company compared to other communications access mechanisms based on cost, effectiveness, efficiency.

Web page A hypertext markup language document containing information that can be seen on the Internet and is identified by a unique URL address.

Website A group of web pages under the control of a single organization or individual that have been developed together to present information on a specific subject.

Webmaster An individual who manages a website.