

GLBA Can Be Simple

- ✓ **infotex** started in 2000. However, prior to our incorporation, we were the technology division of Bucheri McCarty & Metz LLP, who has been serving businesses for 25 years.
- ✓ We use CISSP's for all of our security consulting work.
- ✓ We carry additional E&O Insurance that covers IDS and other security consulting services that we provide. If necessary, we would be happy to provide the required certificates.
- ✓ Our financial statements look excellent, especially for a three-year-old company. We went "into the black" at the end of our second Fiscal Year.
- ✓ Our affiliation with **Purdue's CERIAS** allows us to fine-tune our instruments regularly. In fact, Matt Jonkman - our Security Engineer, is going to teach graduate level classes there next year.
- ✓ We are committed to security consulting and are positioned to continue these services well into the next decade!

Included in this informational banking packet you will find information on:

An Overview

Our Services

Our Security Team

Information Security Assessments

IT Policies

Confidentiality Notice:

The enclosed information is proprietary and confidential, and should not be disclosed to third parties without prior consent of **infotex**, with the exception of disclosure in the name of audits, regulations, and/or litigation.

Copyright © 2003 **infotex**. All rights reserved with the only exception being those listed above.



Ensuring an appropriate balance of Business, Technology, and People



Security is a maze of information, technology and regulations



Information Security is a dynamic Field that changes daily. Increasingly, many organizations find themselves overwhelmed with the rapidly changing technology. Our experienced team of security professionals offers proven assessment services based upon Best Practices, and regulations, including HIPAA and Gramm Leach Bliley.

The ISA, or Information Security Assessment, is another tool in the Information Architecture Process. It finds existing security vulnerabilities and helps you develop an action plan to meet a pre-determined level of security, depending on your unique needs. Like any IT Plan, the ISA defines where you are, where you want to be, and how you plan to get there.

The Information Security Assessment is a cost-effective way to develop an Information Security System, combining all of our Security Consulting Assessment Services. It considers people, processes, and technology so your Security System is aligned with your overall Information Technology Strategy and business goals.

The ISA reduces the risks to your organization’s valuable information, systems and networks by identifying what an authorized or unauthorized user could exploit from points both inside and outside the perimeter of your network. It also identifies policy, procedural, physical and technological weaknesses, details the severity, and recommends solutions.

A Complete Look at Our Security Services

Learn More About Our ISA



It takes everyone working together to make your business run smoothly



Bridge the gap between technology and people with policies and procedures



We utilize teams that include Certified Information System Security Professionals (CISSPs), CPAs, network engineers, and business consultants to ensure that your Security Gap Analysis considers your comprehensive Information System and the critical business process it supports.

Uncontrolled computer use at work diminishes overall corporate productivity by squandering precious company time as well as wasting bandwidth, slowing down the network, causing unnecessary bottlenecks, and exposing the organization to security and legal risks.

Our security consultants have certification from the International Information Systems Security Certification Consortium, Inc., also known as “ISC squared” (ISC)². This organization, named “Most Influential Non-vendor Association” by Information Security Week, governs the CISSP designation.

It is important to have a Computing Policy that informs all users that their Internet and Network usage is being monitored. It is also important to set guidelines that define what the company deems acceptable use of company computers and what could be deemed objectionable.

Meet Our Security Team

Additional Information About IT Policies



Analysis and Report: This includes the analysis of all compiled data and vulnerabilities, as well as confirmation and testing of issues. The analysis will include a background of the issue, explanation of the particular case, and recommendations. The report includes recommendations as to remediation, as well as a severity rating and suggested timeline for remediation.

Database Analysis (per DB): A normal Internal or External scan will include access attempts into any discovered database. This service is designed as a full analysis of a database, its schema, and access controls. The goals of the service are to provide recommendations geared toward better access control, better data integrity, and often performance enhancements. This is done in two phases: first, without granted access; second, with full access to analyze the system.

External Scans: External scans are performed with, but not limited to, generic hacker tools as well as a number of specific tools related to each service found open and some proprietary tools written in-house. The client must provide a range of addresses that are authorized for scanning, or must confirm a range discovered by our technicians prior to the beginning of scanning. A time frame to scan or leave systems alone should also be provided.

Internal Examination: An Internal Examination differs from an Internal Scan in that the testers go onsite, utilizing a conference room or office with a network connection, for 5-10 hours. The testers then map and attack the entire internal network. The client is encouraged to observe this examination. This is designed to raise awareness and understanding of the internal network, as well as emphasize the need for physical security of the network. An Internal Scan is part of this service. Therefore, only one Internal service need be purchased.

Internal Scans: Internal scans are performed with, but not limited to, the same tools as an External Scan. We take all possible measures to get an accurate and complete analysis and scan of the network while minimizing the impact to production systems in use. Internal scans can be performed either by onsite visit, delivered scanning machine with telephone line access, or through a VPN type connection to an internal machine.

Network Traffic Analysis: This service gives the client an idea of the types and state of traffic on their network. Generally, a sniffing machine will be placed at a key point of the network for a period of 1-3 weeks. The goal is to compile a picture of the data that travels the network, aimed at identifying clear text password and username streams, sensitive data that is not protected, unauthorized traffic or probing that may be present, and general network design and performance issues.

Password File Analysis: This is commonly known as Cracking the Password File. We can either attempt to capture a SAM or password file from chosen systems during other scans (most effective if performed against the Domain Controller or Master UNIX Systems) or have it provided by the client. The password file will be examined for easily compromised passwords. A report is provided on the passwords that have been compromised and the timeframe an average attacker would have been able to discover these after obtaining the password file, thus giving a picture of the strength of passwords in place.

Perimeter Ruleset Analysis: Periodic Analysis of firewall and router access lists and rulesets is a critical part of perimeter security. The client will either provide rulesets and access lists or give access to perimeter devices. Analysis will include rules that should be removed or altered, and improvements that may increase performance and reliability.

Physical Breach Attempts: This is an attempt to passively bypass physical security controls and access points. Generally, the goal of an attempt would be to make a phone call to the client from a phone extension within their datacenter or other designated sensitive area. Methods can include posing as repair personnel or simply walking past checkpoints to gauge the response of security personnel and equipment. Pricing is per method of attempt. These are for passive breach attempts only.

Social Engineering Attempts: These are attempts to convince employees and/or vendors to disclose sensitive information or grant access to an individual that does not have authorization to obtain this information or privilege. These are generally done via phone calls to help desks, secretaries, etc.

War-Dialing: This is the process of dialing a range of phone numbers searching for and penetrating modems configured to answer automatically, intelligent fax machines, phone systems, and environmental control systems. Pricing is based on a range of 50 numbers provided to dial and test.

Website/CGI Attempts: A normal external scan will include basic analysis of a website, if detected. This service is designed to dedicate more time toward analyzing and penetrating a website, e-commerce site, or web-based database service.

Wireless Network Discovery and Penetration: This includes visiting designated sites and discovering the wireless networks accessible from public locations around and inside the building. Discovered networks will be mapped and penetration attempted.

Purdue CERIAS Group:

We are very proud of our sponsorship of this center, which creates a great value in the services we can offer to our clients. We consider the CERIAS group to be a very important part of our consulting team!



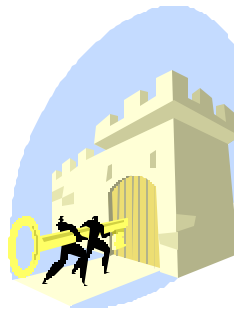


Policy Creation Policy Creation

Staying on the correct course of
Information Security Awareness and Practices

Security Awareness Workshop: This one to two hour interactive workshop utilizes educational materials created by the **Purdue CERIAS Group** in order to insure user understanding of your company's Information Technology Policy as well as an ongoing understanding of the "whys" and "exceptions."

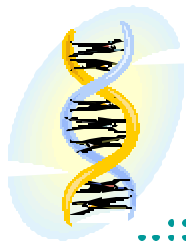
CERIAS Learning Tools: **infotex** is licensed to provide educational materials created by the **Purdue CERIAS Group** to our clients at discounted prices.



Regulatory Assistance: Our CPAs have plenty of experience working with various government agencies. We have worked with the FDIC, the DFI, and the OCC related to Gramm Leach Bliley, as well as the Office for Civil Rights (OCR), and the agency charged with implementing and enforcing HIPAA. Not only can we produce a GAP analysis for HIPAA, we can also assist with remediation.

IT Management Policy: This service is recommended at least annually, but can be performed as needed. We help the client create an overall policy to address the maintenance of user and network policies, business continuity, outside services, and internal controls. Though the IT Management Policy addresses more than simply security, it is a critical element in Information Security Best Practices.

Information Technology Policy: This policy, also called a User Policy or a Computing Policy, is essential to insuring that security best practices are in place with all employees. The creation of this policy addresses legal as well as security issues, and is recommended annually. This service is usually accompanied by the Security Awareness Workshop.



Protection Services Protection Services

Insuring an organic approach to security.

Firewall Installation/Configuration

This service includes the building and hardening of a firewall device and its basic configuration. Once onsite, two hours of consulting are included to tailor the ruleset to fit the environment and tune traffic and throughput.

Firewall Log Monitoring/Management

Installed firewalls will be remotely monitored for configuration problems, network issues, and attackers. Generally, problems will be taken care of by the Operations Staff and notification of the change will be sent. Any change that could impact network traffic will be approved by local IT staff prior to implementation. IT staff will also be notified when issues are detected with local equipment, such as a misconfigured server or a user misusing or abusing network privileges. This service also provides some very basic IDS functionality, as many Trojans and worm-style viruses leave a very distinct footprint in firewall and network traffic. All changes required by IT staff will be performed and tested by Operations Staff. Testing and troubleshooting of changes, of up to one hour per change, are included.

Ongoing Internal and Perimeter Testing: For banks and larger networks, we recommend this service at least quarterly, but it can be performed at any interval, up to weekly, as desired. A full assessment must be performed at least once every year. Ongoing tests will be provided and analyzed to give an updated snapshot in time. The reports are based around the differences from the last analysis. These are an ideal way to detect problematic changes, track remediation, and detect issues with new services and hosts. Every scan will be performed with the most up to date vulnerability databases.

Ongoing Password File Analysis: To insure compliance with the password policy in the Information Technology Policy, we recommend this service be performed at least quarterly. The cracked passwords can be provided to the client or destroyed at the client's request.

IDS Installation/Configuration: Intrusion Detection System Installation and Configuration is the process of building and installing an IDS central database and sensors, and then configuring the network and sensors to see the appropriate traffic and report to the database. This process is very site specific depending on the size of the network, the types of networking equipment to interface with, and the desired level of coverage. We configure and tune the rulesets, as well as network and sensor configuration.

IDS Notification: With this service, installed IDS systems will be forward alerts to a member of the client's staff. All monitoring will be left to the client. The **infotex** Operations Staff will be available for assistance in response, but regular hourly consulting rates will apply. If a response is required by **infotex**, it will be billed at our standard hourly rate.

IDS Notification and Response: Installed IDS systems will be monitored by Operations Staff. Events deemed to be of concern will be automatically provided to local IT staff and immediate notification made via your chosen method. Operations Staff will then take appropriate action to investigate or contain an intrusion. Responses can be taken automatically in the event of delayed contact with local Staff, or can be taken after a customer defined contact wait period. This service also includes reasonable measures to complete investigation and gather evidence, as well as track attackers and provide an avenue and assistance to the customer to pursue prosecution.

Our Core Team

Where's the Geeks!

You will notice that our team consists of a wide variety of consultants. Though Information Architecture and Security involves technology, we help our clients realize that it's about the Information, not the Technology!

We work hard to hire ethical, creative people who strive for excellence. Then, we work even harder to keep them!

What is an Associate?

It is important to understand whom you are working with, especially in growing a system as organic and dynamic as your information system.

We couldn't possibly afford to hire all the expertise we bring to the table. But there are many types of services that we find for our clients again and again. A good example of this would be security consulting. Our clients don't need to hire a full-time CISSP when they can outsource this type of service. We need them maybe 20 to 25 hours per week. So, in order to be able to provide these services in a cost-effective manner, with the quality control that comes with working with the same consultant consistently, we have made arrangements with professionals that we use on a contract basis. The services performed by these associates will be billed through **infotex** (unlike our subcontractors, who invoice our clients directly).

The benefit to our clients is a much quicker deployment, lower costs, and a higher level of quality control. Feel free to ask us for more information about our associates.

Greg McCarty, BS, MBA, CPA

Greg began his public accounting career in 1976 as an auditor with a national CPA firm in Dallas, Texas. Greg is primarily responsible for all audit and accounting policies at Bucheri McCarty & Metz LLP and has developed expertise in MIS.

Chuck Bucheri, CPA

Chuck began his accounting experience in public accounting with a regional firm upon graduation. After three years, he was founding partner of Bucheri McCarty & Metz LLP. Since becoming a partner in 1978, Chuck has been responsible for managing a wide range of accounting and consulting services. As a management consultant, Chuck is very concerned with the use of Information.

Ron Metz, BS, CPA

Ron began practicing in accounting in 1980. He spent the first five years of his career with a large, regional CPA firm, primarily in their tax department. He moved to Kokomo in 1984, and joined the Partnership in 1987. Ron spearheaded the opening of our satellite office in Wabash, Indiana. Given that we are now in the Information Age, Ron recognizes the value of Information in a business.



It takes everyone working together
to make your business run smoothly.

Matt Jonkman, CISSP, Security Engineer

Matt has been involved in Information Technology since the mid-1980's. He has a strong background in telecom security, banking security, network security, network engineering, server design, and UNIX and NT Systems. His certification as CISSP, one of the highest levels of security certification currently available, brings a diverse perspective to the group. Matt obviously brings the technology perspective to the table. Matt is also A+ Certified, CCSE (Checkpoint Certified Systems Engineer), CCSA (Checkpoint Certified Systems Administrator), and FAA Radar Certified.

Roy Chenoweth, CISSP, CISA, Security Consultant

Roy has over three decades of experience in Information Technology, starting at SBC/Ameritech where his assignments included mainframe, midrange, and desktop/server environments. He worked as a staffer and later supervisor in two Network Control Centers. He helped manage and control the corporate Standard Operating Environment, which led to a position as a Senior Security Analyst in Corporate Information Security. He has extensive experience with C/C++, Unix, Cisco, and RSA/SecurID and holds CISSP and CISA professional designations. He is also a WatchGuard Certified Firewall Professional.

Enoch Laudie, CISSP, Security Engineer

Enoch is a CISSP with over ten years of Network Engineering and Telecommunications experience. He has helped develop the engineering procedures, network architecture, and business practices for several networking and telecom startup companies. He also spent time working for IBM as a C and C++ programmer. Enoch's ability to combine all of his experience gives our customers a full range of information security scrutiny, including penetration testing, security forensics, and security best-practices.

Julie Tracy, BA, MCP, Information Architect

Julie started her career in the technology field while in biomedical research doing statistical programming. From there, she became a network administrator for both Novell and Windows NT environments. Julie has been involved in supporting NT networks since 1996 and is familiar with the progression of the network operating system. Julie has also held an appointment as an adjunct faculty teaching computer software and operating systems. Julie's training skills, coupled with her network and technology experience, makes her an excellent member of our team!

Our Core Team

Garrett Honeycutt, Unix Engineer

Garrett comes to us with a background as a system administrator at Purdue University. In this capacity, he learned to resolve a wide range of issues arising from the needs of students and faculty. He has worked with clusters, data conversion, samba, OS, RS6000, IBM SP2 (supercomputer), DEC Alphas, SGI, and Sun Hardware. Garrett is an associate.

Joe Cychosz, BSEE, MSE, E-Commerce Strategist

Joe began his career twenty years ago as a Systems Analyst for Control Data Corporation. His clients have included Bendix, Caterpillar, Indiana State, Fermilab, Aeritalia, Purdue University, and various government locations. Joe has over fifteen years of experience in product development and integration of UNIX-based systems. He has been the manager of the Purdue University Computer Aided Design and Graphics Lab's infrastructure since 1986 and has participated in state-of-the-art computer graphics research projects since 1981. He has published several articles on computer graphics and has authored contributions in the Graphics Gems series. Joe is co-founder of WorldServer, a web-hosting services and database solutions company, and is CTO of Imart Corporation, a provider of e-commerce solutions. Joe is an associate.

Jeff Brambora, BS, MS, MA, Quality Systems Consultant

With degrees in chemistry, biochemistry and theology, Jeff has one of the most diverse backgrounds of all our associates. Jeff's experience includes service to both the not-for-profit sector as well as the for-profit business community. During his eleven years working for not-for-profit organizations, Jeff developed systems of simple standard operating procedures that integrated his organizations' observed best practices. Today, Jeff works in the pharmaceutical industry where he specializes in developing and implementing compliance quality systems using software out of the box and simple control strategies. Jeff is an associate.

Tammy Durr, MCP, Network Engineer

Tammy started her IS career in 1997 as a NT Network Administrator for a local school corporation. She has worked as a consultant for a large company in Indianapolis providing both network and software support to several major Fortune 100 businesses, as a LAN/WAN administrator for a large financial organization, and as a Network Administrator in city government. Her strengths include network design, implementation, and administration for Novell, NT 4.0 as well as Windows 2000 environments. Tammy's certifications include Microsoft (NT and Exchange). Tammy is an associate.

Scott Lavengood, CCNA, Network Engineer

Scott just began working with us this past summer. He just received his CCNA, after studying Cisco Systems hardware and networking protocols for two years. He worked with one of our clients during the summer to help "fine tune" their IT plan. Scott is currently studying Computer Technology at Purdue University, while helping us with clients in Lafayette as we continue to grow towards that area.

Dale Sears, Senior Consultant

Dale Sears is a proven professional with nearly 14 years of demonstrated consulting expertise. He has worked with all levels of personnel in achieving outstanding results for numerous companies in a variety of industries ranging from Fortune 100 to entrepreneurial. Dale has demonstrated skills in areas including leadership development, behavioral assessments, hiring recommendations, team building and executive and personal coaching; meeting facilitation, strategic planning, implementation and execution, and performance management systems; sales development, e-commerce, business technology integration, and career marketing and development. Dale was Consultant of the Year two years in a row for a national firm. Dale is an associate!

David Brinson, Network Engineer

David's career began with several years in the Marine Corps – first as a Radio Technician and later as a Small Computer Systems Specialist. David's IT experience began over a decade ago supporting a small Banyan Token-ring. Subsequently, David has worked the past few years as a Network/IT manager while earning Cisco (CCNP & CCDP), Citrix (CCA), Microsoft (MCSE), Lotus (CLP) and CompTIA (A+) certifications.

Bobbette R. Fagel, CPS, IT Deployment Specialist

Bobbette has worked with Bucheri McCarty & Metz LLP since 1989, with primary responsibilities in collections, systems diagramming, web site maintenance, and administrative responsibilities. She has extensive training and experience in various software programs, including word processing, database, web development and graphics software. Bobbette's ability to utilize Information Technology tools and, more importantly, train others brings a great value to our clients!

Blake Matheny, SCSA, MCP, Unix Engineer

Blake managed a network of over 50 machines when he was 17 years old. When he was 19, he started working as a Unix Consultant, worked for Sprint to help secure their global network, and now works freelance on various consulting jobs. Besides his skills with networking in the Microsoft, Novell, and Unix platforms, Blake has extensive experience in application development using C, SQL, Perl, C++, and many other languages. If it can be done on a Unix machine, Blake can do it! Blake is an associate.

Dan Hadaway, BA, Architecture, President

After graduating with a degree in Architecture in 1982, Dan helped start one of the premier regional video store chains which, when sold in 1995, was ranked in the Top 10 of Video Store Magazine's Top 100 Report four times. Much of this success is attributed to the intense focus the company had on the customer, via the use of Information.

Purdue CERIAS Group: We are very proud of our sponsorship of this center, which creates a great value in the services we can offer to our clients. We consider the CERIAS group to be a very important part of our consulting team!





Security is a maze of information, technology and regulations!

Just what we need, another acronym!

The ISA, or Information Security Assessment, is another tool in the Information Architecture Process. It finds existing security vulnerabilities and helps you develop an action plan to meet a pre-determined level of security, depending on your unique needs. Like any IT Plan, the ISA defines where you are, where you want to be, and how you plan to get there.

Who needs an ISA?

Regulations (HIPAA and Gramm/Leach/Bliley) will eventually require any entity that electronically stores medical and/or financial records to conduct an ISA. This will be used to create a GAP Analysis to address security vulnerabilities according to a set of “security best practices.”

Beyond that, any business that depends upon information stored on a network with a 24/7 direct connection to the Internet will need to address security. We find the ISA to be the most cost-effective way to initiate this process.

Who does this?

Because of our affiliation with the Indiana CPA Society, we offer an assessment process that provides a uniformity that is sorely absent from most technology services. Our CISSPs team up with CPAs to conduct a three-pronged assessment of your external perimeter, your internal information system, and your policies and procedures.

Are there other options?

- ◇ If your company is not subject to new Federal Regulations and Laws regarding Security and Privacy, you could conduct an internal assessment. However, an objective third party can catch oversights in even the best networks.
- ◇ Network Integrators are starting to offer their own version of the ISA. They tend to concentrate on external threats while disregarding internal threats. Security is a habit and a discipline, and the best firewall in the world won't stop an employee from innocently breaching security best practices.
- ◇ You could just sit back, relax, and take the “It won't happen to me!” approach. After all, who would want to hack into your office? However, we don't recommend it.

According to a recent survey by the FBI, 80% of US Corporations had monetary losses from security breaches just last year. 67% of the attacks were from insiders!

- ◇ **Remember:** technology does not equal security!!



Do I need an ISA in my company?

As with most questions related to Information Systems, the answer is a set of questions:

- What industry are you in?
- Does your industry require you to comply with applicable laws and regulations regarding information security?

If so, then you must conduct an ISA to insure compliance. Even if you are not required to do so, you should still think about the Value of Information while trying to answer these questions:

- Have you analyzed the risks associated with the loss or theft of Information?
- Do you have a written security policy?
- Do you know what security vulnerabilities a disgruntled employee, an external hacker, or even simply an untrained employee could exploit?
- Are systems really being backed up on schedule?
- Whose advice are you relying on to insure that your system is secure? What credentials does this person or business have related to security?

What does the Assessment Process do?

The ISA reviews your Information System from both the non-technical and technical viewpoints. From the non-technical side, we review your infrastructure, policies and physical/procedural controls to identify any weaknesses that could result in a security breach or loss of service. We then conduct a technical review, which includes internal scans of your network, seeking to identify vulnerable ports, services and configurations that could be exploited. Finally, we conduct what is called a Penetration Test, or external scan of your network. We mimic the latest attack methods and identify potential threats from hackers. Using the Information Architecture approach, this unbiased third-party assessment insures that your Information Systems Security is in line with your overall business strategies.

And why is this all necessary?

The ISA reduces the risks to your organization's valuable information, systems and networks by identifying what an authorized or unauthorized user could exploit from points both inside and outside the perimeter of your network. It also identifies policy, procedural, physical and technological weaknesses, details the severity, and recommends solutions.

infotex employs professionals who have been working in security consulting for national firms. We use Certified Information Systems Security Professionals (CISSP).

Purdue CERIAS Group:

We are very proud of our sponsorship of this center, which creates a great value in the services we can offer to our clients. We consider the CERIAS group to be a very important part of our consulting team!





Bridge the gap between technology and people with policies and procedures.

“Organizations lose an estimated \$50 billion dollars a year in productivity due to employees web-surfing out of personal interest at the workplace.”
- Sacramento Bee

What is an Effective IT Policy?

Uncontrolled computer use at work diminishes overall corporate productivity by squandering precious company time as well as wasting bandwidth, slowing down the network, causing unnecessary bottlenecks, and exposing the organization to security and legal risks.

infotex can help you develop a responsible computing policy to:

- Increase productivity and save time
- Block crucial information loss
- Decrease the possibility of lawsuits
- Reduce the threat of virus attacks, and deal appropriately with viruses when they do show up
- Optimize bandwidth and improve network speed
- Eliminate unauthorized access by outside hackers as well as internal personnel
- Eliminate unlicensed software on your network
- Promote a comfortable work environment

Creating a Computing Policy

It is important to have a Computing Policy that informs all users that their Internet and Network usage is being monitored. It is also important to set guidelines that define what the company deems acceptable use of company computers.

Data Storage Policies

First and foremost, your policy should strongly state that all user data is to be stored on the network (not on the workstations.) Mapping drives for convenience is the best way to enforce appropriate file storage. Second, your policy should state that all software and/or data found on company computers is owned by the company, and that employees are not allowed to download software and/or data without permission. Likewise, the policy should clarify the procedure for installing new software programs on the network to avoid licensing problems as well as viruses. Guidelines should be explicit regarding data transfers. Try to establish what data can and can't go home, be shared with customers or friends, etc.

Offensive Sites and/or E-mail Messages

Employees visiting pornographic or other offensive sites hurt office morale. Equally as important, such activities put users and the company at risk of harassment lawsuits.

Virus Attacks from E-mail and Data Transfers

E-mail, floppy disks, and zip disks all potentially contain viruses. Employees must follow stringent policies to avoid the possibility of destroying data. Do they know what those guidelines are? Do you? Don't wait until after your system crashes to fix this problem!

Internet / E-mail Policies

Define acceptable use of your company's Internet connection for personal reasons. Do you want to allow employees to access the Internet for personal use during lunch-break and before or after official work hours? Is personal e-mail allowed? How about e-mail mailing lists? Your policy should answer these questions in a way that sets guidelines on "gray areas." Give some examples of what you consider unacceptable – such as surfing out of personal interest during work hours; visits to sexually explicit, racist or other "offensive" sites whether during work hours or not, downloading of objectionable material, etc.

Policy Abuses

It is important to specify the penalties that apply for breach of computing policies. To provide flexibility and the ability to handle each instance individually, avoid absolutes, such as "doing this will result in termination." Instead, use language such as "doing this may result, upon review, in dismissal." This is very important in computing policies because of the unpredictable nature of computer usage. For example, what will happen to employees who visit an unacceptable web site by accident simply by clicking on a seemingly relevant link during a work-related search? For this reason, your policy should also have a methodology for reporting accidental violations to an authorized person.

Introducing Your Policy

Prior to "finalizing" your policy, distribute a copy of the policy with the word "draft" in plain site to your company's department heads and/or supervisors. Be sure to explain the importance of the policy. Feel free to attach this newsletter. Communicate that you are open to feedback about the policy, but also state an effective date to inspire your department heads quickly read and comment on the policy.

Then, prior to the effective date, give a hard copy of the final policy to every employee. Send an e-mail explaining that there is a new computing policy and the effective date. Explain that your policy is not only meant to help your company but also to provide a more pleasant and safe work environment. Send an e-mail reminder on the effective date.

It's the Information Age!

It's very important to always remember this when developing a computing policy. Your goal is to remove the risk of sharing information, but you are still trying to increase the ability of your people to USE information. Because it is the Information Age, the computing policy is one of those policies that must be reviewed annually!



Purdue CERIAS Group:

We are very proud of our sponsorship of this center, which creates a great value in the services we can offer to our clients. We consider the CERIAS group to be a very important part of our consulting team!