Technology Policy and Procedures: Protecting Client and Program Data

In recent years the news has been peppered with stories of computer data breaches where millions of records of personally identifiable information for customer and clients has been leaked or released. In many instances, the actual victims of these breaches have been the last to know just how much damage has been done, discovering only too late that their bank accounts have been pilfered by identity thieves in possession of financial records more comprehensive than the victim would have ever guessed. The companies responsible for the breaches have seen their reputations crater and customer faith evaporate.

Most of these breaches were not, as would be expected, the work of shadowy and super-funded criminal syndicates, but rather, were the result of simple lapses of oversight on the part of the companies affected. Lost laptops and USB keys containing client data, improperly wiped and discarded hard drives, databases or network equipment with default, and widely available, passwords enabled, an employee who e-mails a username and password to a colleague are all examples of breaches where no overt criminal activity has occurred. Unfortunately, however, each of these examples could prove disastrous to a company that sees the lost or shared information fall into the wrong hands.

Regardless of their nature, however, data breaches such as the above could have been prevented, or at the very least, mitigated, by the presence of a simple set of policies, procedures or guidelines that define how to store and protect program and client information in a manner that secures not only the client's peace of mind, but that of the company as well.

What Are Policies?

Policies are not, as some might expect, strictly defined as a set of rules and regulations that dictate employee behavior. Their sole purpose is to act as a protective tool for the company which, like it or not, is ultimately responsible for dealing with, or cleaning up, any messes that may occur. Companies create and deploy policies not just to ensure that client or program information remains private, but also to ensure that all employees are on the same operational page and aware of the dangers that could arise should a breach occur.

Types of Policies

There are three separate types of policies common to modern business: Point Specific Policies, Operational Standards, and Guidelines. Point Specific Policies typically cover single areas of concern such as "Building Key Management" or "Internet Acceptable Use", and most often take the form of rules and regulations that have been coupled with implementation and enforcement clauses. Operational Standards are collections of of system-specific or procedural-specific requirements that most often come into play during the construction of end user workstations or servers. Here an administrator may define exactly how to assemble a machine, what software to purchase, how to configure it, and how to keep it up to date. Operational standards exists to ensure that a designated ideal can be repeated as religiously as possible in order to reduce complexity, comply with licensing terms, and preserve system security. Guidelines are "Best

Practices", and are generally defined as optional, yet strongly recommended variations on the theme of maintaining "intelligent behavior". A good example of a guideline would be the recommendation to restrict, wherever possible, the e-mail exchange of system passwords

Preparation and Planning

When it comes to crafting policies, there are really no formal guidelines for deciding what to protect, and how. These decisions depend entirely upon the nature of the program or company developing the policy, and what it is the company considers worthy of attention. The first stage of any policy development should be a comprehensive review of every aspect of a program's technological operations, with an eye towards identifying any key areas of concern. The best way to approach this is to first assemble a core committee, consisting of a broad swath of employees with varying operational responsibilities (i.e., Directors, Secretaries, I.T., Attorneys, Accountants or others). Each job title has its own perspective on how the program approaches certain tasks, events or issues, and each can offer valuable insight that might be overlooked by a more exclusive group. Decisions that appear black and white to a CEO may be visible in multiple shades of grey visible to a practicing attorney.

This initial committee should first acknowledge the fact that it will become a political body, whether it intends to or not. Policies affect all staff, in more ways than some will initially be prepared to accept. First and foremost, they must apply to all **staff**, from the Executive Director to the part-time volunteer. Some policies may be require monitoring or enforcement clauses that can be coupled with disciplinary actions. While its important to remember that the company's need must always come before the political peace of mind of its employees, the committee should never lose sight of the fact that their decisions will carry great weight.

Policy Elements

Once the committee has identified it s priorities for policy development, the next stage becomes the actual drafting of the document itself. As with any document, there are several key elements that should be present in any finished policy statement: Scope, Definitions, Declarations of Responsibility, and, if applicable, details concerning enforcement.

A policy's scope is simply the definition of what it is the policy is intended to address and why. For example, a policy mandating acceptable behavior should state what types of behavior it applies to (interpersonal, business use of equipment, netiquette), and why certain behaviors are either prohibited (offensive) or encouraged (best practice).

Definitions within the policy help employees understand what exactly the policy is addressing in terms they can easily understand. Technology policies in particular demand extremely clear language that simplifies terminology that an average employee may be unfamiliar with. For example, it may not be enough to say that electronic files should be archived every thirty days. An end user may assume that the policy only applies to documents, and ignore a need to archive e-mail as well. A good definition will present an employee with a precise list of what constitutes an "electronic file" (documents, scans, e-mail, faxes, instant messages, web postings, voice mail, recorded telephone calls, etc.).

Declarations of responsibility inform employees of how the policy is applied within the chain of command of an organization. Most often associated with enforcement, declarations of responsibility clearly delineate who will be doing what in the event of a breach of protocol or security, and will marry a policy to a program's disciplinary procedures. Additionally, in the case of policies that define acceptable behavior, they will outline what steps the program is taking to make the sure behaviors are monitored and reported. Nobody, least of all attorneys, like to be told they can't do something, and for every "thou shalt not" defined, you will invariably discover instances wherein the policy cannot be rigidly applied. For example, one law firm may implement a strict "no pornography" policy, only to take on a family law case wherein one of the parties is accused of posting compromising pictures of a spouse on a web site. As proof of such actions would be critical for evidentiary purposes, there must be some mechanism present that allows for an administrative "override" around the restriction.

Special Note - Confidentiality and Data Aggregators

One key element of any program's operational manual should be a Declaration of Confidentiality Guidelines. The key to protecting confidential data lay in defining exactly what it is the program considers confidential. Social Security numbers by themselves are a powerful tool when it comes to identifying an individual, but other data that may appear benign on the surface can often be used to negative effect should it fall into the wrong hands. A good example of this would be street address information within domestic violence cases, which can be used to place family members in a very real physical danger.

Once you have defined the types of data that will be treated as "confidential", the next stage is to develop and put in place a series of controls governing how that data will be protected. Utilizing mechanisms such as encryption to scramble critical bits of data will make it far harder for breaches to yield criminally usable results and may serve to limit liability. Decide whether it is necessary to store full Social Security numbers, or whether your organization can get by with partials (i.e., the last four or five digits), or replacing them outright. Establish a solid set of controls governing information exchange within and without the organization in order to further reduce the risk of data leaks.

Finally, it is not enough to say that "client information" is going to be confidential, if you are willing to turn around and hand that very information off to other sources without question. When exchanging any kind of client information with an external source, be sure to make an effort at negotiating protective guidelines for its use, handling and further dissemination. One often overlooked side-effect of our current culture of information exchange is the capacity for data aggregators to assemble massive amounts of disparate and seemingly disconnected pieces of information into detailed profiles that go far beyond the data a program's initial confidentiality guidelines could have anticipated.

Implementation - Duration: 10 minutes to remainder of session

On a general level, most policies can be implemented with little fanfare beyond an announcement to all staff, and incorporation into the program's operational manual. It is strongly recommended that all staff be required to sign an acknowledgement of receipt of any

policies, particularly if they contain any disciplinary clauses. Technical policies might require a little more preparation before their "go live" date, as many of their conditions may be dependent on the technology being present, or brought under control. Policies addressing topics as complex as the new Federal E-Discovery rules can require a significant amount of time and expense preparing technologies to assist in meeting document retention requirements, automatic archiving, and preservation of communications.

Once implemented, however, the work is far from over. Policies are living documents, and should be subject to review and periodic modification and/or enhancement as need requires or circumstances dictate. Program operations and the technologies that assist will continually evolve, and new developments will invariably present scenarios that no longer fall comfortably within the frameworks of policies past. Programs should establish a program of annual review, wherein the same group of original stakeholders meet to discuss existing policies, sharing employee feedback on their overall effectiveness and acceptance, and any new developments worthy of attention that may have emerged during the course of the year.

Because policies are subject to change, it is critical that staff receive ongoing training to not only reinforce their existing knowledge, but to keep them aware of new developments. Remember that a policy is only effective if employees are aware of both its content and intent. Ongoing training can consist of something as simple as regular e-mail reminders or announcement at staff meetings, or as formal as becoming a staple of the new hire orientation and training sessions.

Suggestions and Sources

Acceptable Encryption Policy	Information Sensitivity Policy
Acceptable Use Policy	Information System Audit Logging Requirements
Analog/ISDN Line Policy	Internal Lab Security Policy
Anti-Virus Process	Internet DMZ Equipment Policy
Application Service Provider Policy	Lab Anti-Virus Policy
Application Service Provider Standards	Password Protection Policy
Acquisition Assessment Policy	Personal Communication Device
Audit Vulnerability Scanning Policy	Remote Access Policy

Automatically Forwarded Email Policy	Removable Media Policy
Bluetooth Device Security Policy	Mobile Computing and Storage Devices
Database Credentials Coding Policy	Risk Assessment Policy
Dial-in Access Policy	Router Security Policy
DMZ Lab Security Policy	Server Security Policy
E-mail Policy	Server Malware Protection Policy
E-mail Retention	The Third Party Network Connection Agreement
E-Discovery	VPN Security Policy
Ethics Policy	Wireless Communication Policy
Extranet Policy	Wireless Communication Standard

Resources:

The SANS Security Policy Project: http://www.sans.org/security-resources/policies/