The Twelve Steps To Designing A Strategic Security Process

By Rich Schiesser in conjunction with Harris Kern's Enterprise Computing Institute

Below are the 12 steps to developing a strategic security process:

1. Identify an executive sponsor – An executive sponsor needs to be identified to champion and support the strategic security program. This individual will provide management direction, will serve on the executive security review board and will select the security process owner.

2. Select a security process owner - The executive sponsor will need to select a security process owner who will manage the day-to-day activities of the process. This person will assemble and facilitate the cross-functional team that will brainstorm requirements, and will participate on the technical security review board that, among other things, will develop standards and implementation plans for various security policies. See Table 1 below for a prioritized list of characteristics of a security process owner.

Table 1 Prioritized Characteristics of a Security Process Owner

	Characteristic	**Priority**
1.	Knowledge of applications	High
2.	Knowledge of system software and components	High
3.	Knowledge of network software and components	High
4.	Ability to analyze metrics	High
5.	Ability to think and plan strategically	High
6.	Ability to work effectively with IT developers	Medium
7.	Knowledge of company's business model	Medium
8.	Ability to talk effectively with IT executives	Medium
9.	Knowledge of backup systems	Medium
10.	Knowledge of desktop hardware and software	Medium
11.	Knowledge of software configurations	Medium
12.	Knowledge of hardware configurations	Low
13.	Ability to meet effectively with IT customers	Low
14.	Ability to think and act tactically	Low

3. Define goals of strategic security – Executives should define and prioritize the specific goals of strategic security. Three characteristics that executives should consider in this regard are the availability, integrity and confidentiality of data. The scope of strategic security should also be defined to clarify which, if any, business units and remote sites will be included in the plan, and to what extent it will be enterprise-wide.

4. Establish review boards – The assessment and approval of security initiatives works best through a process of two separately chartered review boards. The first is an executive level review board chartered with providing direction, goals and policies concerning enterprise-wide security issues. Its membership should represent all key areas of IT and selected business units.

   The second board is comprised of senior analysts and specialists who are qualified to evaluate the technical feasibility of security policies and initiatives proposed by the executive board, and to set enforceable security standards and procedures. An example of such a procedure, password management, is shown in Figure 1.

Figure 1 Password Management Procedure (1 of 2)

Procedures for Selecting Secure Passwords

Passwords are used to safeguard the access to information to which you have been entrusted. Unfortunately, one of the simplest and most common means of violating this safeguard is to inadvertently allow another individual to learn your password. This could give an unauthorized person the capability to access and alter company information that you are responsible for protecting.
The following procedures are intended as guidelines for selecting passwords that greatly reduce the likelihood of a password being accidentally divulged or intentionally detected. If you have questions about the use of these procedures, please contact your security administrator.

I. General Guidelines

1. Never show, give, or tell, or send to anyone your password. This includes close friends, co-workers, repair technicians, and supervisors.
2. Never write your password down, nor leave it out on your desk, on a post-it note, on your desktop or laptop terminal, or in a desk drawer.
3. Change your password at least every 90 days, or whenever you have logged on remotely, or whenever you suspect someone may have accidentally or intentionally detected your password.
4. Logoff your desktop or laptop terminal whenever you leave it unattended for more than a few minutes.
5. Consider basing the complexity of, and the frequency of changing, your password on the level of access authority you have. Foe example, update capability may warrant a password more complex and frequently changed than simple inquiry access only.

II. What NOT to use in Selecting a Secure Password

1. Do not use any word, or any concatenation of a word, that can be found in any dictionary, including foreign and technical dictionaries.
2. Do not use any proper noun such as a city, a landmark, or bodies of water.
3. Do not use any proper names, be they from real life, literature, or the arts.
4. Do not use any words spelled backwards.
5. Do not use any common keyboard patterns such as “yuiop”.
6. Do not include “@” or “#” characters in your password since some machines interpret these as delimiter or eraser characters.
7. Do not use all upper case alphabetic characters.
8. Do not use all lower case alphabetic characters.
9. Do not use all numeric characters.
10. Do not use less than 6 characters in your password.
11. Do not use common number schemes such as birthdays, phone numbers or license plates, even though these may contain slashes, hyphens or blanks.

Figure 1 Password Management Procedure (2 of 2)

III. What Your Password SHOULD Contain

1. Your password should contain at least 6 characters.
2. Your password should contain at least one uppercase alphabetic character.
3. Your password should contain at least one lowercase alphabetic character.
4. Your password should contain at least one numeric character.
5. Consider including one special or non-alphanumeric character in your password.
6. A single occurrence of an uppercase, lowercase, or special character should not be at the beginning or end of your password.
7. Consider using a personal acronym to help you remember highly unique passwords, such as:

we Bought his/her towels 4 us. (wBh/ht4u)
or
good Passwords are Not 2 hard 2 find. (gPaN2h2f)

5. Identify, categorize and prioritize requirements – Representatives from each of the two review boards, along with other appropriate Subject Matter Experts (SMEs) should meet to identify security requirements, categorize them according to key areas for security issues as shown in Table 2, and then prioritized.

Table 2 Key Areas for Categorizing Security Issues

Key Area	**Security Issues**
Client/Server	Anti-virus
	Desktop software
	E-mail
Network/Internet	Firewalls
	Intrusion/Detection
	Remote Access
	Encryption
Data Center	Physical access
	Databases
	Application software
	Operating systems
Security Policies	Executive proposals
	Technical evaluation
	Approval and implementation
	Communication and enforcement

6. Inventory current state of security – This step involves taking a thorough inventory of all current security-related items to determine what you already have in-house and what may need to be developed or purchased. These items should include:
    - security policies approved, adhered to, and enforced;
    - security policies approved, but not adhered to or enforced;
    - security policies drafted but not yet approved;
    - existing software security tools with the ability to be used for enforcement;
    - existing hardware security tools with the ability to be used for enforcement;
    - current security metrics available to analyze:
        - virus attacks;
        - password resets;
        - multiple sign-ons;
        - trouble tickets.

7. Establish security organization – Based on input from the two review boards, on the list of requirements, and on the inventory of current security policies, tools and metrics, establish a centralized security organization to be headed up by a security manager. The location of the security organization and the responsibilities and authorities of the security manager will be jointly determined by the two security review boards and other appropriate areas of management.

8. Develop Policy Statements – Based on the inventory of existing security policies, eliminate obsolete or ineffective policies, modify those policies requiring changes, and develop necessary new policies. Figure 1 is shows a sample corporate security policy and Figure 1-4 shows a sample security policy on the use of the Internet.

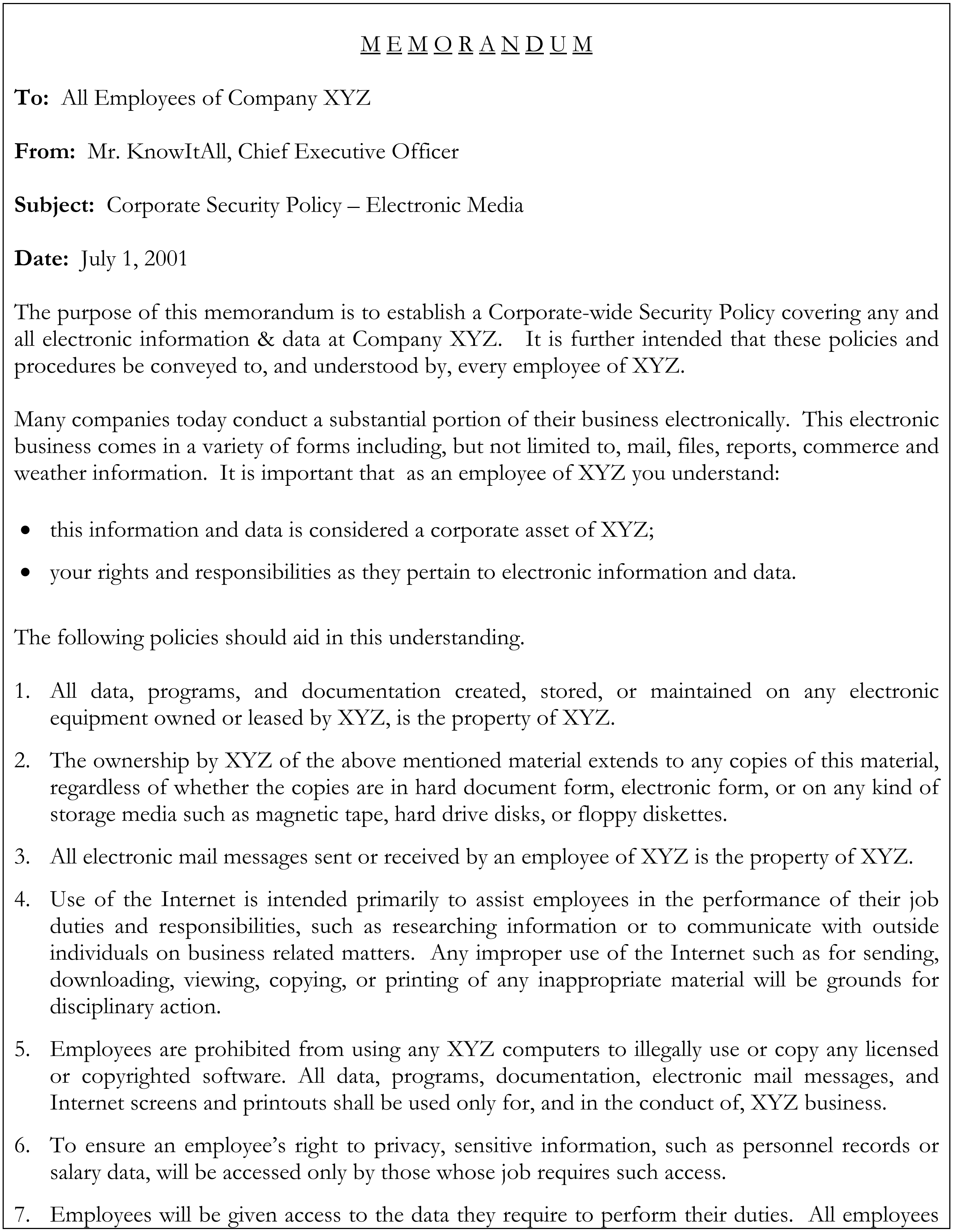
9. Assemble planning teams – Cross-functional teams should be assembled to develop implementation plans for new policies, procedures, initiatives and tools proposed by the either of the two security review boards.

10. Review and approve plans – The executive security review board should review the implementation plans from a standpoint of policy, budget, schedule and priority.

11. Evaluate technical feasibility of plans – The technical security review board should evaluate the implementation plans from a standpoint of technical feasibility and adherence to standards.

12. Assign, schedule and execute the implementation of plans – Individuals or teams should be assigned responsibilities and schedules for executing the implementation plans.

Figure 3 Sample Corporate Security Policy (1 of 2)



M E M O R A N D U M

To: All Employees of Company XYZ

From: Mr. KnowItAll, Chief Executive Officer

Subject: Corporate Security Policy – Electronic Media

Date: July 1, 2001

The purpose of this memorandum is to establish a Corporate-wide Security Policy covering any and all electronic information & data at Company XYZ. It is further intended that these policies and procedures be conveyed to, and understood by, every employee of XYZ.

Many companies today conduct a substantial portion of their business electronically. This electronic business comes in a variety of forms including, but not limited to, mail, files, reports, commerce and weather information. It is important that as an employee of XYZ you understand:

- this information and data is considered a corporate asset of XYZ;
- your rights and responsibilities as they pertain to electronic information and data.

The following policies should aid in this understanding.

1. All data, programs, and documentation created, stored, or maintained on any electronic equipment owned or leased by XYZ, is the property of XYZ.
2. The ownership by XYZ of the above mentioned material extends to any copies of this material, regardless of whether the copies are in hard document form, electronic form, or on any kind of storage media such as magnetic tape, hard drive disks, or floppy diskettes.
3. All electronic mail messages sent or received by an employee of XYZ is the property of XYZ.
4. Use of the Internet is intended primarily to assist employees in the performance of their job duties and responsibilities, such as researching information or to communicate with outside individuals on business related matters. Any improper use of the Internet such as for sending, downloading, viewing, copying, or printing of any inappropriate material will be grounds for disciplinary action.
5. Employees are prohibited from using any XYZ computers to illegally use or copy any licensed or copyrighted software. All data, programs, documentation, electronic mail messages, and Internet screens and printouts shall be used only for, and in the conduct of, XYZ business.
6. To ensure an employee's right to privacy, sensitive information, such as personnel records or salary data, will be accessed only by those whose job requires such access.
7. Employees will be given access to the data they require to perform their duties. All employees

will be held personally accountable for the information entrusted to them to ensure there is no unauthorized disclosure, misuse, modification, or destruction.

8. Authorizing documents and passwords will be used to manage and control access to data, programs, and networks.

9. All data, programs, and documentation deemed to be of a production nature are under the custodianship of the Chief Information Officer. This custodianship requires that all reasonable measures be taken to safeguard the use and integrity of this material, including a documented disaster recovery plan.

10. All XYZ managers are responsible for ensuring that every new employee and contractor reporting to them who has access to electronic programs and data understand these policies and procedures.

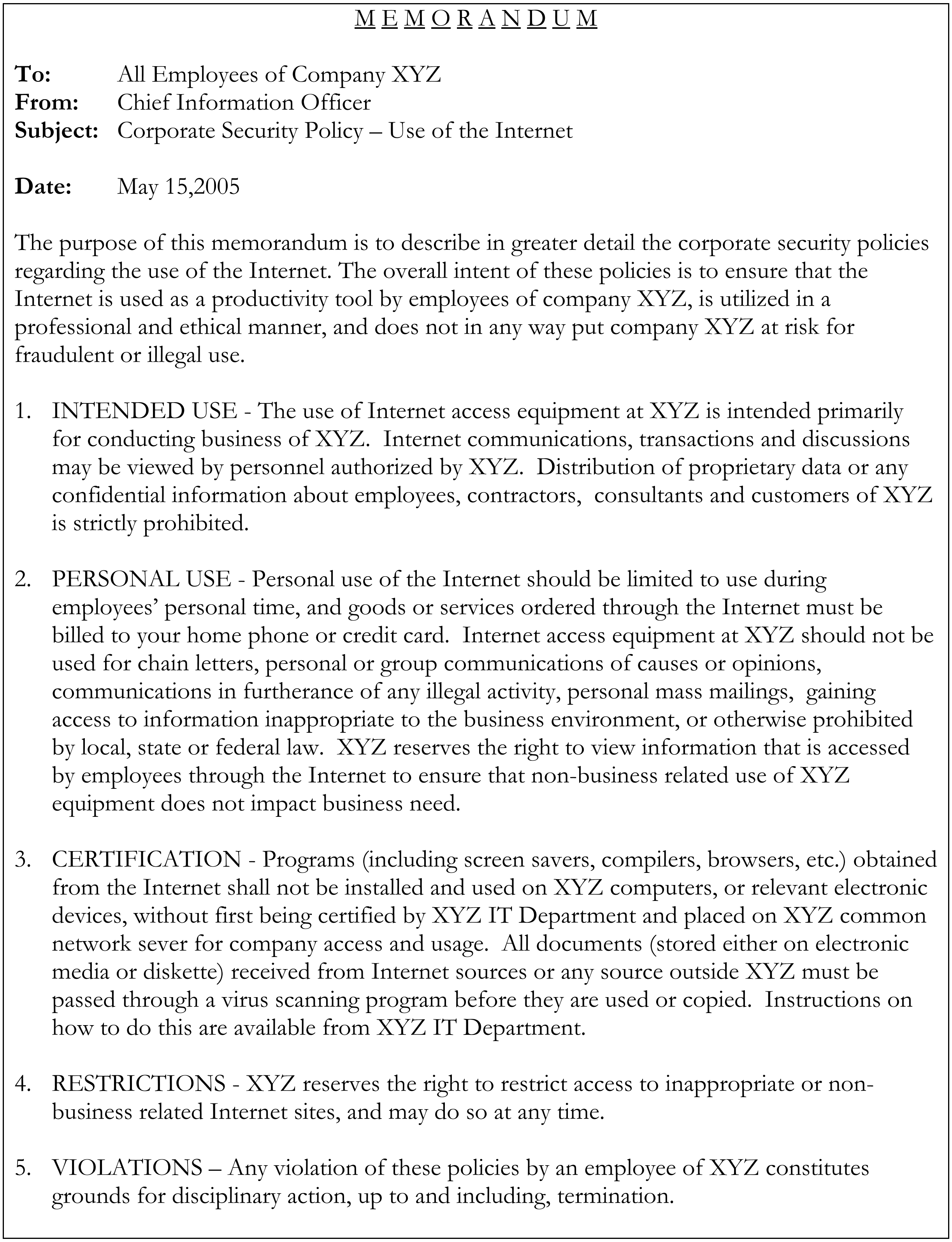
11. All XYZ managers are responsible for ensuring that any terminating employee reporting to them have all passwords and electronic accesses removed at the time of termination.

12. These policies constitute the majority, but not necessarily all, of the key security issues involving electronic media. The rapidly changing nature of information technology may periodically obsolete some policies and require the inclusion of new ones. In any event, all XYZ employees are expected to conduct themselves at all times in a professional, ethical and legal manner regarding their use of XYZ information resources.

13. Any violation by an employee of these policies constitutes grounds for disciplinary action, up to and including termination.

14. A copy of these policies and procedures will be kept on file by the XYZ for review by any regulating agency.

Figure 4 Sample Internet Security Policy



M E M O R A N D U M

To: All Employees of Company XYZ
From: Chief Information Officer
Subject: Corporate Security Policy – Use of the Internet

Date: May 15,2005

The purpose of this memorandum is to describe in greater detail the corporate security policies regarding the use of the Internet. The overall intent of these policies is to ensure that the Internet is used as a productivity tool by employees of company XYZ, is utilized in a professional and ethical manner, and does not in any way put company XYZ at risk for fraudulent or illegal use.

1. INTENDED USE - The use of Internet access equipment at XYZ is intended primarily for conducting business of XYZ. Internet communications, transactions and discussions may be viewed by personnel authorized by XYZ. Distribution of proprietary data or any confidential information about employees, contractors, consultants and customers of XYZ is strictly prohibited.

2. PERSONAL USE - Personal use of the Internet should be limited to use during employees' personal time, and goods or services ordered through the Internet must be billed to your home phone or credit card. Internet access equipment at XYZ should not be used for chain letters, personal or group communications of causes or opinions, communications in furtherance of any illegal activity, personal mass mailings, gaining access to information inappropriate to the business environment, or otherwise prohibited by local, state or federal law. XYZ reserves the right to view information that is accessed by employees through the Internet to ensure that non-business related use of XYZ equipment does not impact business need.

3. CERTIFICATION - Programs (including screen savers, compilers, browsers, etc.) obtained from the Internet shall not be installed and used on XYZ computers, or relevant electronic devices, without first being certified by XYZ IT Department and placed on XYZ common network sever for company access and usage. All documents (stored either on electronic media or diskette) received from Internet sources or any source outside XYZ must be passed through a virus scanning program before they are used or copied. Instructions on how to do this are available from XYZ IT Department.

4. RESTRICTIONS - XYZ reserves the right to restrict access to inappropriate or non-business related Internet sites, and may do so at any time.

5. VIOLATIONS – Any violation of these policies by an employee of XYZ constitutes grounds for disciplinary action, up to and including, termination.