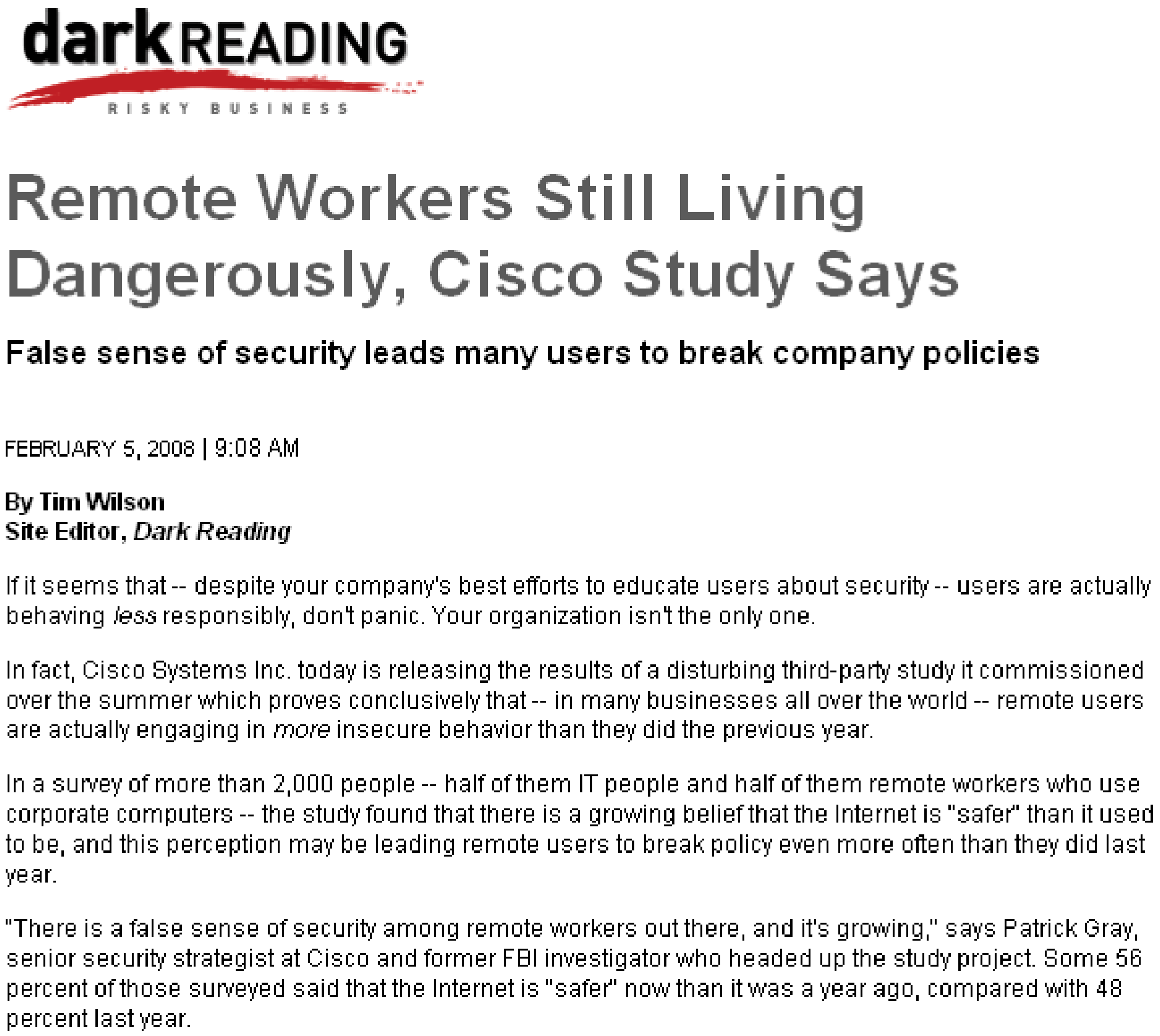
Ethical Hacking Countermeasures

Version 6

Module XLIX

Creating Security Policies

News



darkREADING

RISKY BUSINESS

Remote Workers Still Living Dangerously, Cisco Study Says

False sense of security leads many users to break company policies

FEBRUARY 5, 2008 | 9:08 AM

By Tim Wilson
Site Editor, *Dark Reading*

If it seems that -- despite your company's best efforts to educate users about security -- users are actually behaving *less* responsibly, don't panic. Your organization isn't the only one.

In fact, Cisco Systems Inc. today is releasing the results of a disturbing third-party study it commissioned over the summer which proves conclusively that -- in many businesses all over the world -- remote users are actually engaging in *more* insecure behavior than they did the previous year.

In a survey of more than 2,000 people -- half of them IT people and half of them remote workers who use corporate computers -- the study found that there is a growing belief that the Internet is "safer" than it used to be, and this perception may be leading remote users to break policy even more often than they did last year.

"There is a false sense of security among remote workers out there, and it's growing," says Patrick Gray, senior security strategist at Cisco and former FBI investigator who headed up the study project. Some 56 percent of those surveyed said that the Internet is "safer" now than it was a year ago, compared with 48 percent last year.

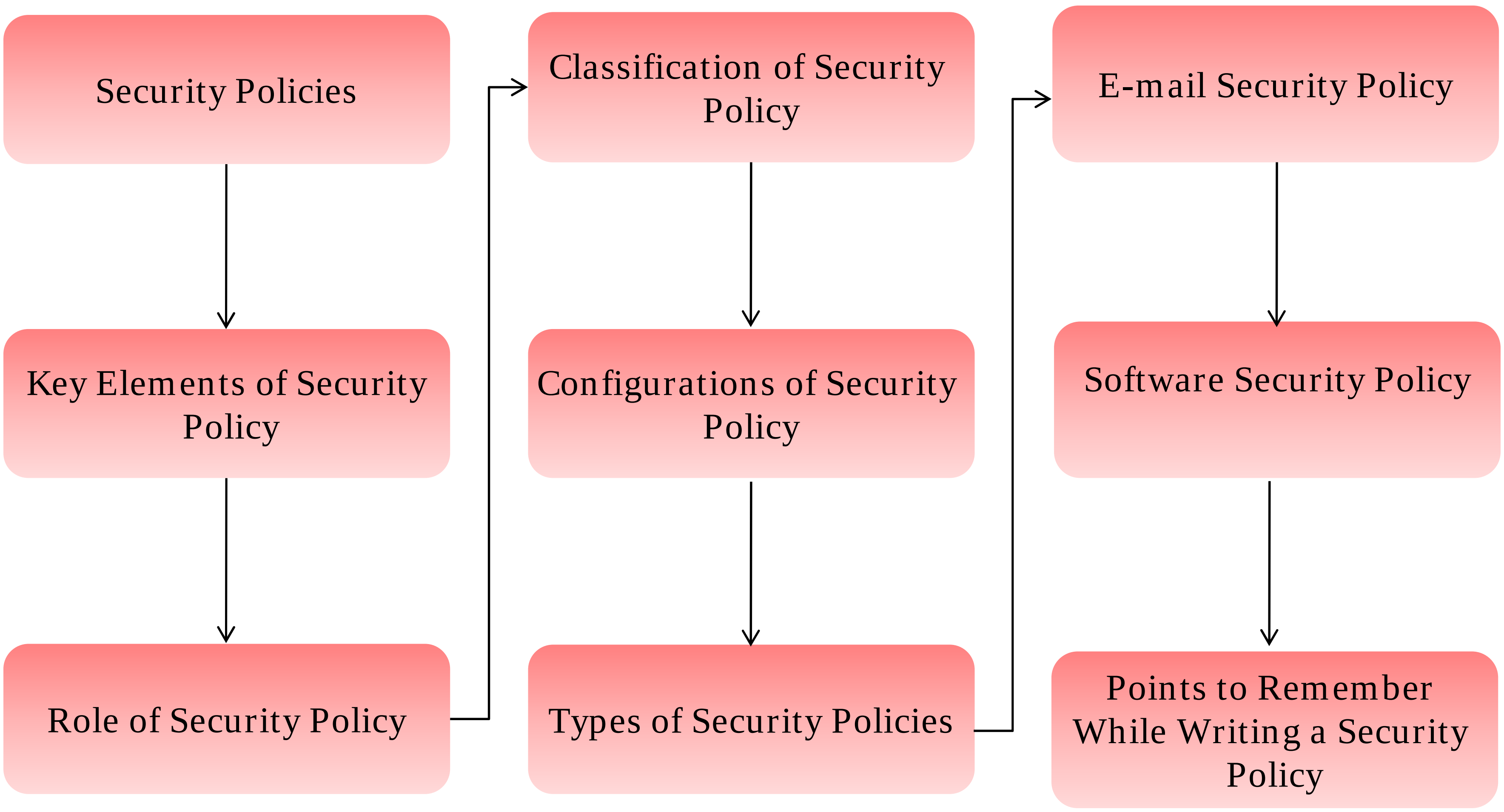
Source: *http://www.darkreading.com/*

Module Objective

This module will familiarizes you with:

- Security Policies
- Key Elements of Security Policy
- Role of Security Policy
- Classification of Security Policy
- Configurations of Security Policy
- Types of Security Policies
- E-mail Security Policy
- Software Security Policy
- Points to Remember While Writing a Security Policy

Module Flow



Security Policies

Key Elements of Security Policy

Role of Security Policy

Classification of Security Policy

Configurations of Security Policy

Types of Security Policies

E-mail Security Policy

Software Security Policy

Points to Remember While Writing a Security Policy

EC-Council

Security Policies

Security policies are the foundation of the security infrastructure

A security policy is a document or set of documents that describes the security controls that will be implemented in the company at a high level

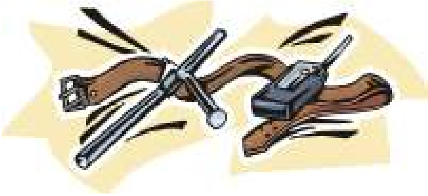
Without them, you cannot protect your company from possible lawsuits, lost revenue, bad publicity, and basic security attacks

Policies are not technology specific and do three things for a company:

- Reduce or eliminate legal liability to employees and third parties
- Protect confidential, proprietary information fromtheft, misuse, unauthorized disclosure, or modification
- Prevent waste of company computing resources

Key Elements of Security Policy

- Clear communication
- Brief and clear information
- Defined scope and applicability
- Enforceable by law
- Recognizes areas of responsibility
- Sufficient guidance
- Top management involvement



Defining the Purpose and Goals of Security Policy

Purpose of Security Policy

- To maintain an outlinefor the management and administration of network security
- To reduce risks caused by:
  - Illegal use of the system resource
  - Loss of sensitive, confidential data, and potential property
  - Differentiate the user's access rights

Goals of Security Policy

- Protection of organization's computing resources
- Elimination of strong legal liability from employees or third parties
- Ensuring customers' integrity and preventing unauthorized modifications of the data

Role of Security Policy

Suggests the safety measures to be followed in an organization

Provides set of protocols to the administrator on

- How the users work together with their systems?
- How those systems should be configured?
- How to react when the system is attacked?
- When susceptibilities are found?

Classification of Security Policy

User Policy

- Defines what kind of user is using the network
- Defines the limitations that are applied on users to secure the network
- Password Management Policy
  - Protects the user account with a secure password

IT Policy

- Designed for IT department to keep the network secure and stable
- Following are the three different IT policies:
  - Backup Policies
  - Server configuration, patch update, and modification policies
  - Firewall Policies

Classification of Security Policy (cont'd)

General Policies

- Defines the responsibility for general business purposes
- The following are different general policies:
  - High Level Program Policy
  - Business Continuity Plans
  - Crisis Management
  - Disaster Recovery

Partner Policy

- Policy that is defined among a group of partners

Classification of Security Policy (cont’d)

Issue Specific Policies

- Recognize specific areas of concern and describe the organization's status for top level management
- Involve revision and up gradation of policies from time to time, as changes in technology and related activities take place frequently

Components:

- Issue Statement
- Statement of the Organization's Position
- Applicability
- Roles and Responsibilities
- Points of Contact
- Physical security
- Personnel Security
- Communications Security
- Administrative Security
- Risk Management
- System Management

Design of Security Policy

Guidelines should cover the following points as policy structure:

- Detailed description of the policy issues
- Description about the status of the policy
- Applicability of the policy to the environment
- Functionalities of those affected by the policy
- Compatibility level of the policy is necessary
- End-consequences of non-compliance

EC-Council

Contents of Security Policy

High level Security Requirements

- This statement features the requirement of a system to implement security policies that include discipline security, safeguard security, procedural security, and assurance security

Policy Description based on requirement

- Focuses on security disciplines, safeguards, procedures, continuity of operations, and documentation

Security concept of operation

- Defines the roles, responsibilities, and functions of a security policy

Allocation of security enforcement to architecture elements

- Provides a computer system architecture allocation to each system of the program

EC-Council

Configurations of Security Policy

Role-Based Service Configuration

- Provides a way to configure services that are installed and available depending on the server's role and other features

Network Security

- Designed to configure inbound ports using Windows Firewall

Registry Settings

- Designed to configure protocols usedto communicate with computers on the network

Audit Policy

- Designed to configure the auditing of the server based on auditing objectives

Internet Information Service

- Designed to configure the security feature of Internet Information Services (IIS)

Implementing Security Policies

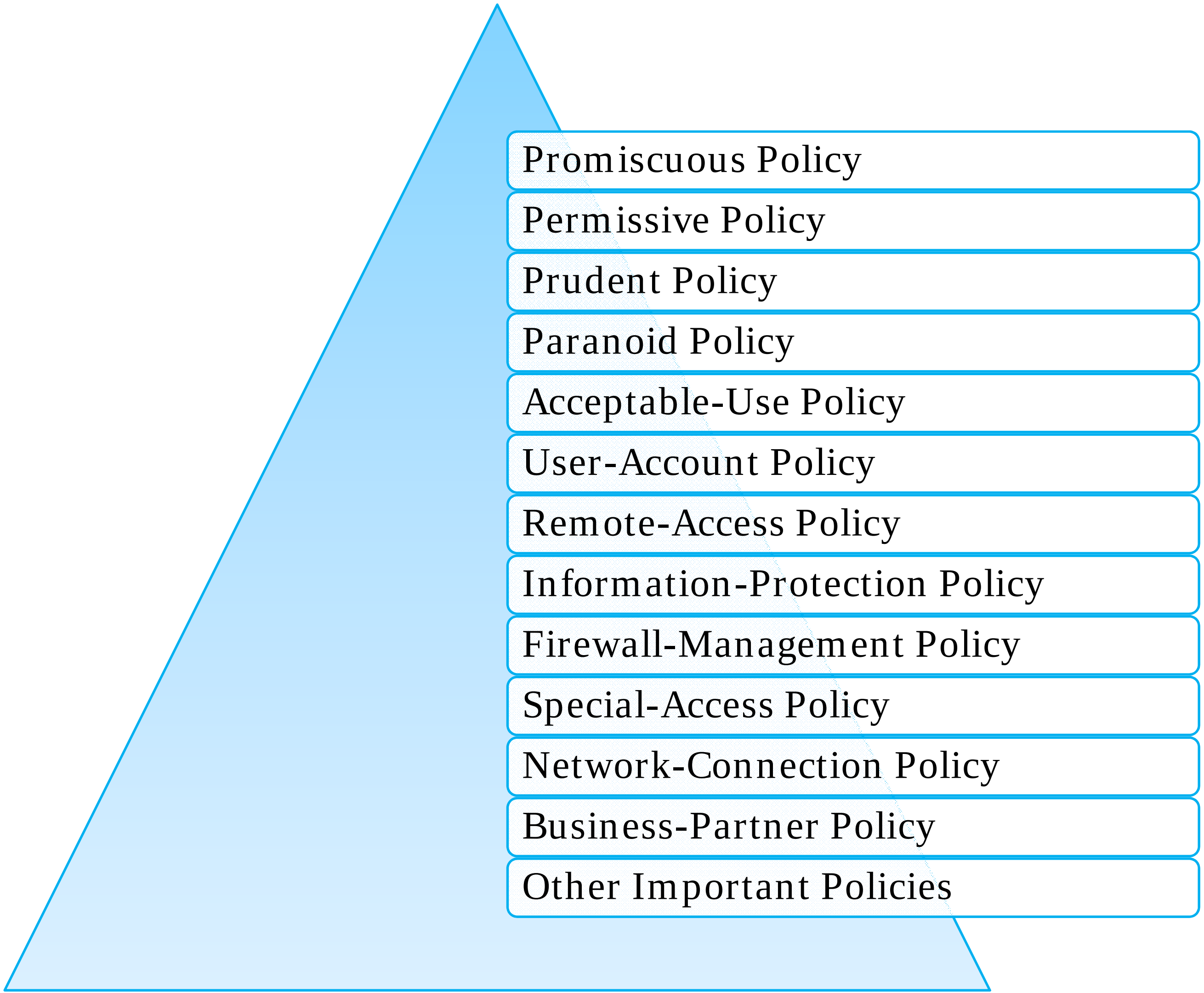
Implementation follows after building, revision, and updating of the security policy

Final version must be made available to all of the staff members in the organization

For effective implementation, there must be rotation of the job so that data must not be handled by few people

Proper security awareness program, cooperation, and coordination among employees is required

Types of Security Policies



- Promiscuous Policy
- Permissive Policy
- Prudent Policy
- Paranoid Policy
- Acceptable-Use Policy
- User-Account Policy
- Remote-Access Policy
- Information-Protection Policy
- Firewall-Management Policy
- Special-Access Policy
- Network-Connection Policy
- Business-Partner Policy
- Other Important Policies

Promiscuous Policy

No Restrictions on Internet/ Remote Access

- Good luck to your network administrator, you have our blessings...

Permissive Policy

Known dangerous services/ attacks blocked

Policy begins wide open

Known holes plugged, known dangers stopped

Impossible to keep up with current exploits; administrators always play catch-up

Prudent Policy

Provides maximum security while allowing known but necessary dangers

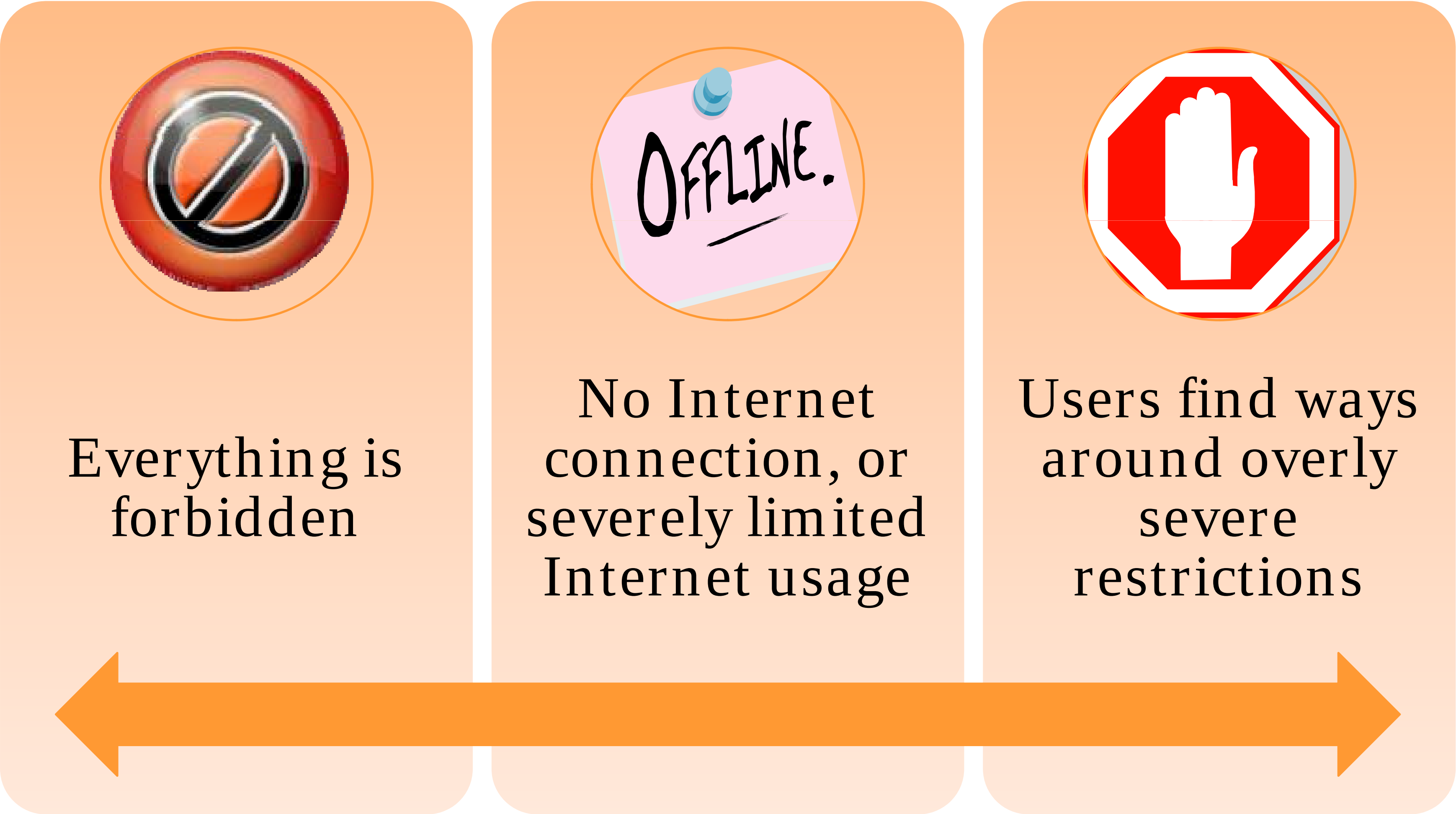
All services are blocked, nothing is allowed

Safe/ necessary services are enabled individually

Nonessential services/ procedures that cannot be made safe are not allowed

Everything is logged

Paranoid Policy



Everything is forbidden

No Internet connection, or severely limited Internet usage

Users find ways around overly severe restrictions

Acceptable-Use Policy

Should users read and copy files that are not their own but are accessible to them?

Should users modify files that they have write access to but are not their own?

Should users make copies of system configuration files (for example, /etc/passwd and SAM) for their own personal use or to provide to other people?

Should users be allowed to use .rhosts files? Which entries are acceptable?

Should users be allowed to share accounts?

Should users have the ability to make copies of copyrighted software?

User-Account Policy

Who has the authority to approve account requests?

Who (employees, spouses, children, company visitors, for instance) are allowed to use the computing resources?

May users have multiple accounts on a single system?

May users share accounts?

What are the users' rights and responsibilities?

When should an account be disabled and archived?

Remote-Access Policy

Who is allowed to have remote access?

What specific methods (such as cable modem/ DSL or dial-up) does the company support?

Are dial-out modems allowed on the internal network?

Are there any extra requirements, such as mandatory anti-virus and security software, on the remote system?

May other members of a household use the company network?

Do any restrictions exist on what data may be accessed remotely?

Information-Protection Policy

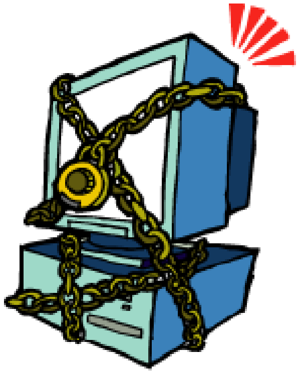
What are the sensitivity levels of information?

Who may have access to sensitive information?

How is sensitive information stored and transmitted?

What levels of sensitive information may be printed in public printers?

How should sensitive information be deleted from storage media (paper shredding, scrubbing hard drives, and degaussing disks)?



Firewall-Management Policy

Who has access to the firewall systems?

Who should receive requests to make a change to the firewall configuration?

Who may approve requests to make a change to the firewall configuration?

Who may see the firewall configuration rules and access lists?

How often should the firewall configuration be reviewed?

Special-Access Policy

Who should receive requests for special access?

Who may approve requests for special access?

What are the password rules for special-access accounts?

How often are passwords changed?

What are the reasons or situations that would lead to revocation of special-access privileges?

Network-Connection Policy

Who may install new resources on the network?

Who must approve the installation of new devices?

Who must be notified that new devices are being added to the network?

Who should document network changes?

Are there any security requirements for the new devices being added to the network?

Business-Partner Policy

Is it mandatory for a company required to have a written security policy?

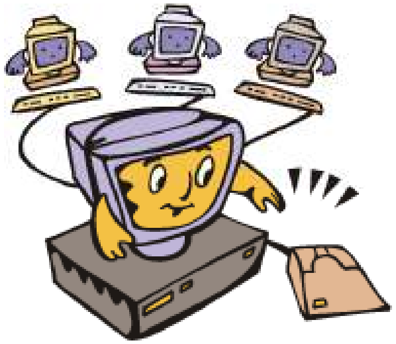
Should each company have a firewall or other perimeter security device?

How will one communicate (virtual private networking [VPN] over the Internet, leased line, and so forth)?

How will access to the partner's resources be requested?

Other Important Policies

A wireless network policy, which helps to secure wireless networks, includes which devices are allowed to be connected, what security measures should be followed, and so forth



A lab policy discusses how to protect the internal network from the insecurities of a test lab

The best option is to keep the test lab on a completely separate Internet connection and without connecting it in any way to the internal corporate network

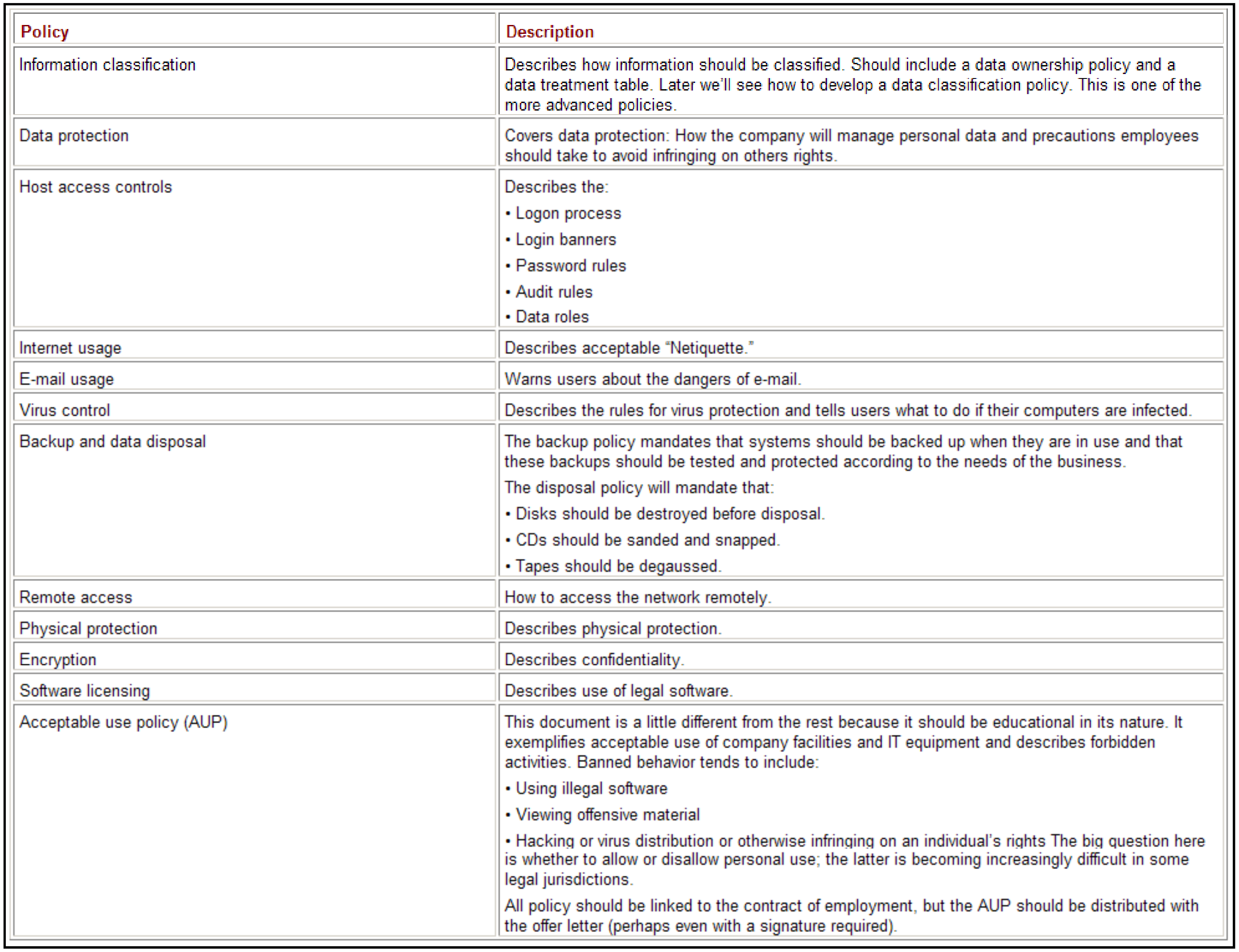
Policy Statements

The policy is really only as good as the policy statements that it contains. Policy statements must be written in a very clear and formal style

Good examples of policy statements are:

- All computers must have antivirus protection activated to provide real-time, continuous protection
- All servers must be configured with the minimum of services to perform their designated functions
- All access to data will be based on a valid business need and subject to a formal approval process
- All computer software must always be purchased by the IT department in accordance with the organization's procurement policy
- A copy of the backup and restoration media must be kept with the off-site backups
- While using the Internet, no person is allowed to abuse, defame, stalk, harass, or threaten any other person or violate local or international legal rights

Basic Document Set of Information Security Policies



Policy	Description
Information classification	Describes how information should be classified. Should include a data ownership policy and a data treatment table. Later we'll see how to develop a data classification policy. This is one of the more advanced policies.
Data protection	Covers data protection: How the company will manage personal data and precautions employees should take to avoid infringing on others rights.
Host access controls	Describes the: • Logon process • Login banners • Password rules • Audit rules • Data roles
Internet usage	Describes acceptable "Netiquette."
E-mail usage	Warns users about the dangers of e-mail.
Virus control	Describes the rules for virus protection and tells users what to do if their computers are infected.
Backup and data disposal	The backup policy mandates that systems should be backed up when they are in use and that these backups should be tested and protected according to the needs of the business. The disposal policy will mandate that: • Disks should be destroyed before disposal. • CDs should be sanded and snapped. • Tapes should be degaussed.
Remote access	How to access the network remotely.
Physical protection	Describes physical protection.
Encryption	Describes confidentiality.
Software licensing	Describes use of legal software.
Acceptable use policy (AUP)	This document is a little different from the rest because it should be educational in its nature. It exemplifies acceptable use of company facilities and IT equipment and describes forbidden activities. Banned behavior tends to include: • Using illegal software • Viewing offensive material • Hacking or virus distribution or otherwise infringing on an individual's rights The big question here is whether to allow or disallow personal use; the latter is becoming increasingly difficult in some legal jurisdictions. All policy should be linked to the contract of employment, but the AUP should be distributed with the offer letter (perhaps even with a signature required).

E-mail Security Policy

An e-mail security policy is created to govern the proper usage of corporate e-mail

Things that should be in an email security policy:

- Define prohibited use
- If personal use is allowed, it needs to be defined
- Employees should know if their emails are reviewed and/or archived
- What types of email should be kept and how long
- When to encrypt email
- Consequences of violating email security policy

EC-Council

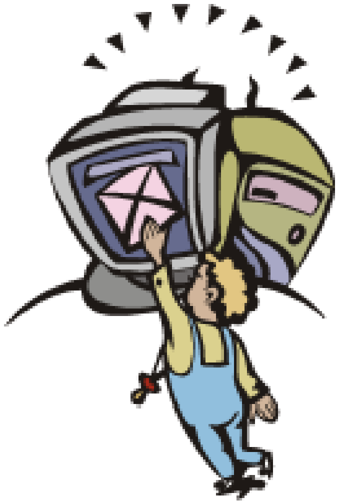
Best Practices for Creating E-mail Security Policies

Employees should know the rights granted to them by organization in respect of privacy in personal e-mails transmitted across the organization's system and network

Employees should not open an e-mail or attached files without ensuring that the content appears to be genuine

Conditional and sensitive information should not be transmitted by e-mail, unless it is secured by encryption or any other secure techniques

Employees should be familiar with general good e-mail policies such as, the need to save, store file e-mail with business contents same as storage of letters, and other traditional e-mails



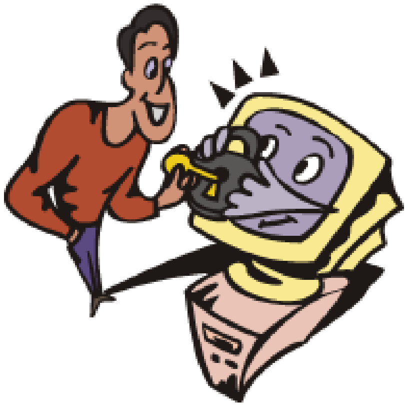
User Identification and Passwords Policy

Each user is allocated an individual user name and password

Requests for new computer accounts and for termination of existing computer accounts must be formally authorized to the IT Help Desk/ relevant IT resource by the relevant manager

Staff must notify the IT Help Desk/ relevant IT resource when moving to a new position or location within "Company Name“

Line management must notify staff about changes, that might affect security



EC-Council

User Identification and Passwords Policy (cont’d)

All user accounts should have the following password settings:

- Minimum password length of 8 characters
- A combination of alpha, numeric, and punctuation should be used
- Users are forced to change their passwords every (insert number) days
- Users cannot repeat passwords
- Accounts are locked after (insert number) incorrect login attempts

CEH™ Certified Ethical Hacker

Software Security Policy

Software must not be copied, removed, or transferred to any third party or non- organizational equipment

Only software that has been authorized by the IT Department must be used on PCs and notebook computers connected to the "Company Name" IT network

Downloading of any executable files (.exe) or software from the Internet must be prohibited without written authorization from the IT Department/ relevant IT resource

Regular reviews of desktop software should be undertaken and the presence of unauthorized software should be investigated

Software Licence Policy

Copyright stipulations governing vendor-supplied software must be observed at all times

Software that is acquired on a trial basis must be used in accordance with the vendor's copyright instructions

All software developed within Company is the property of the Company and must not be copied or distributed without prior written authorization from the IT Department

Points to Remember While Writing a Security Policy

Designing the best possible Security Policy for the network

Stakeholders of the organization must aid the security professional in steering policy development

Policy development must be devised and processed entirely by the security professional and it should be expanded only with the stakeholders' input

EC-Council

Sample Policies

Remote Access Policy

- Do you restrict remote access to the enterprise to just authorized users (probably—i.e., not employee's family members)?
- Is wireless access permitted? (See Wireless AUP.) Is access from Internet cafés permitted? If so, under what circumstances and with what safeguards?
- What software and hardware combinations and configurations are required for remote access?
- May users access the enterprise network from devices your IT department has not issued, or has not authorized?
- How will you authenticate (confirm the identity of) the person accessing the network?
- How is access controlled? By passwords, security tokens, VPNs, or what?
- Is remote access granted to all employees, or must they apply for it? How do they apply?
- What activities are prohibited? What activities are permitted?
- Is account activity monitored? If so, how will you notify employees of this fact?
- In what ways must a user protect the remote access account?

Source: *http://www.watchguard.com/*

Wireless Security Policy

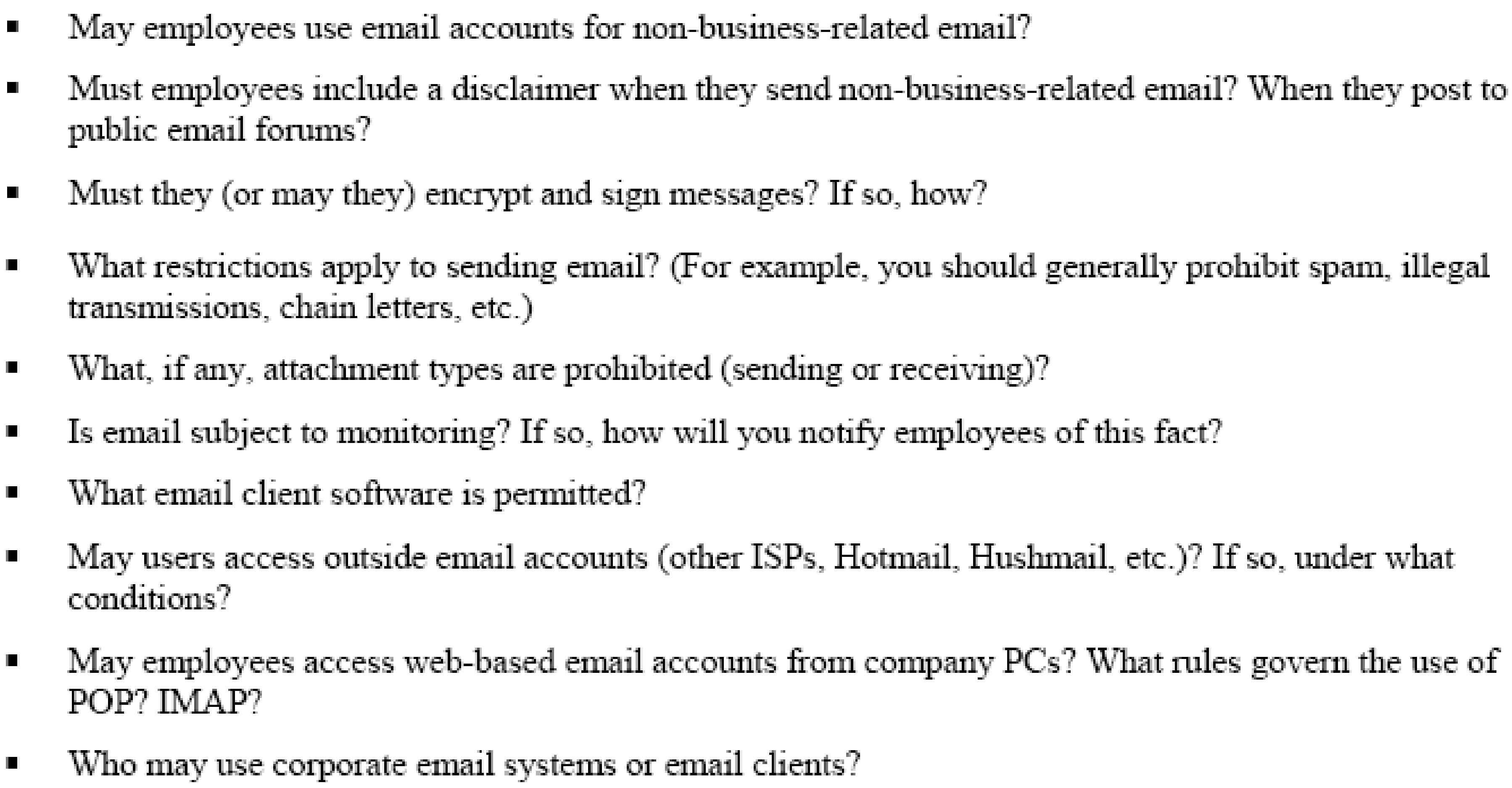
- Is wireless access to your network allowed?
- Are any kinds of data or communication prohibited over wireless?
- What protection must be in place before wireless communication is authorized?
- How must the user protect the wireless device (physically and logically)?
- For wireless data, what hardware is approved, permitted, and/or required?

Wireless Security Policy (cont'd)

- For wireless data, what software is approved, permitted, and/or required?
- What rules govern wireless access points? Must they be deployed, configured, and installed by IT, or are other employees permitted such activities?
- What are the configuration requirements for wireless access points? (For example, "The password and username must be changed from the manufacturer's default.")
- Is VPN software required? Which or what kind? Who must or may install it?
- Where must wireless connections terminate on the network? In the DMZ? On a segregated VLAN?
- How must wireless connections authenticate and encrypt?
- Is wireless permitted for remote users connecting to the Internet with enterprise equipment?
- Is wireless access permitted for mobile users connecting into the enterprise network from outside the enterprise?
- What security devices and controls must be in place on authorized wireless devices?
- What configuration rules must users follow when connecting home wireless networks to enterprise assets?

Source: *http://www.watchguard.com/*

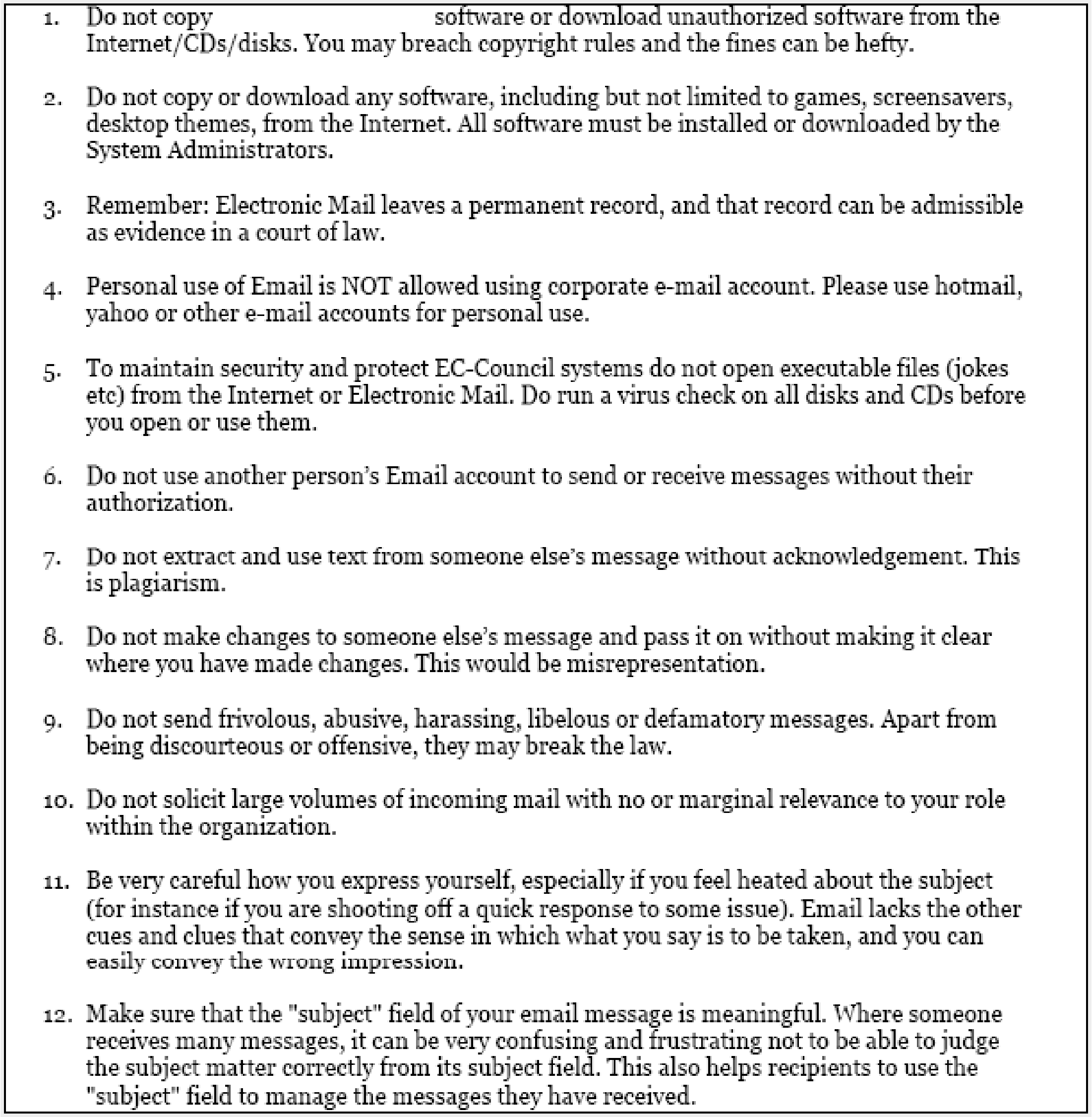
E-mail Security Policy



- May employees use email accounts for non-business-related email?
- Must employees include a disclaimer when they send non-business-related email? When they post to public email forums?
- Must they (or may they) encrypt and sign messages? If so, how?
- What restrictions apply to sending email? (For example, you should generally prohibit spam, illegal transmissions, chain letters, etc.)
- What, if any, attachment types are prohibited (sending or receiving)?
- Is email subject to monitoring? If so, how will you notify employees of this fact?
- What email client software is permitted?
- May users access outside email accounts (other ISPs, Hotmail, Hushmail, etc.)? If so, under what conditions?
- May employees access web-based email accounts from company PCs? What rules govern the use of POP? IMAP?
- Who may use corporate email systems or email clients?

Source: *http://www.watchguard.com/*

E-mail and Internet Usage Policies



1. Do not copy software or download unauthorized software from the Internet/CDs/disks. You may breach copyright rules and the fines can be hefty.

2. Do not copy or download any software, including but not limited to games, screensavers, desktop themes, from the Internet. All software must be installed or downloaded by the System Administrators.

3. Remember: Electronic Mail leaves a permanent record, and that record can be admissible as evidence in a court of law.

4. Personal use of Email is NOT allowed using corporate e-mail account. Please use hotmail, yahoo or other e-mail accounts for personal use.

5. To maintain security and protect EC-Council systems do not open executable files (jokes etc) from the Internet or Electronic Mail. Do run a virus check on all disks and CDs before you open or use them.

6. Do not use another person's Email account to send or receive messages without their authorization.

7. Do not extract and use text from someone else's message without acknowledgement. This is plagiarism.

8. Do not make changes to someone else's message and pass it on without making it clear where you have made changes. This would be misrepresentation.

9. Do not send frivolous, abusive, harassing, libelous or defamatory messages. Apart from being discourteous or offensive, they may break the law.

10. Do not solicit large volumes of incoming mail with no or marginal relevance to your role within the organization.

11. Be very careful how you express yourself, especially if you feel heated about the subject (for instance if you are shooting off a quick response to some issue). Email lacks the other cues and clues that convey the sense in which what you say is to be taken, and you can easily convey the wrong impression.

12. Make sure that the "subject" field of your email message is meaningful. Where someone receives many messages, it can be very confusing and frustrating not to be able to judge the subject matter correctly from its subject field. This also helps recipients to use the "subject" field to manage the messages they have received.

Personal Computer Acceptable Use Policy

- Who owns the PC? (Most of the time it's the company, but you'll need the policy to also address, for example, the home PC of a telecommuter.)
- Are there any restrictions on non-business use? (For example, may a company computer be used for games, or personal email?)
- Who is authorized to use the PC? Only the employee to whom it is issued? Any employee of the company? An employee's immediate family?
- How should the user protect the computer data? (For example, must the user encrypt files?)
- How should the user protect the computer from unauthorized access? (Passwords? Password-protected screensaver? How many minutes before the screen saver times out?)
- What software must be running on the PC? (Examples: Antivirus? Personal firewall? A spyware detector? What versions? etc.)
- Are there restrictions on software installation? (For example, is the user permitted to install anything downloaded from the Internet?)
- What special protection is required for mobile computers?
- What activities or classes of activities are prohibited?
- Will you monitor keystrokes or communications? If so, how will you notify employees of this?
- Who is responsible to back up computer data?
- How must the user protect or mark personal information on a company-owned computer?

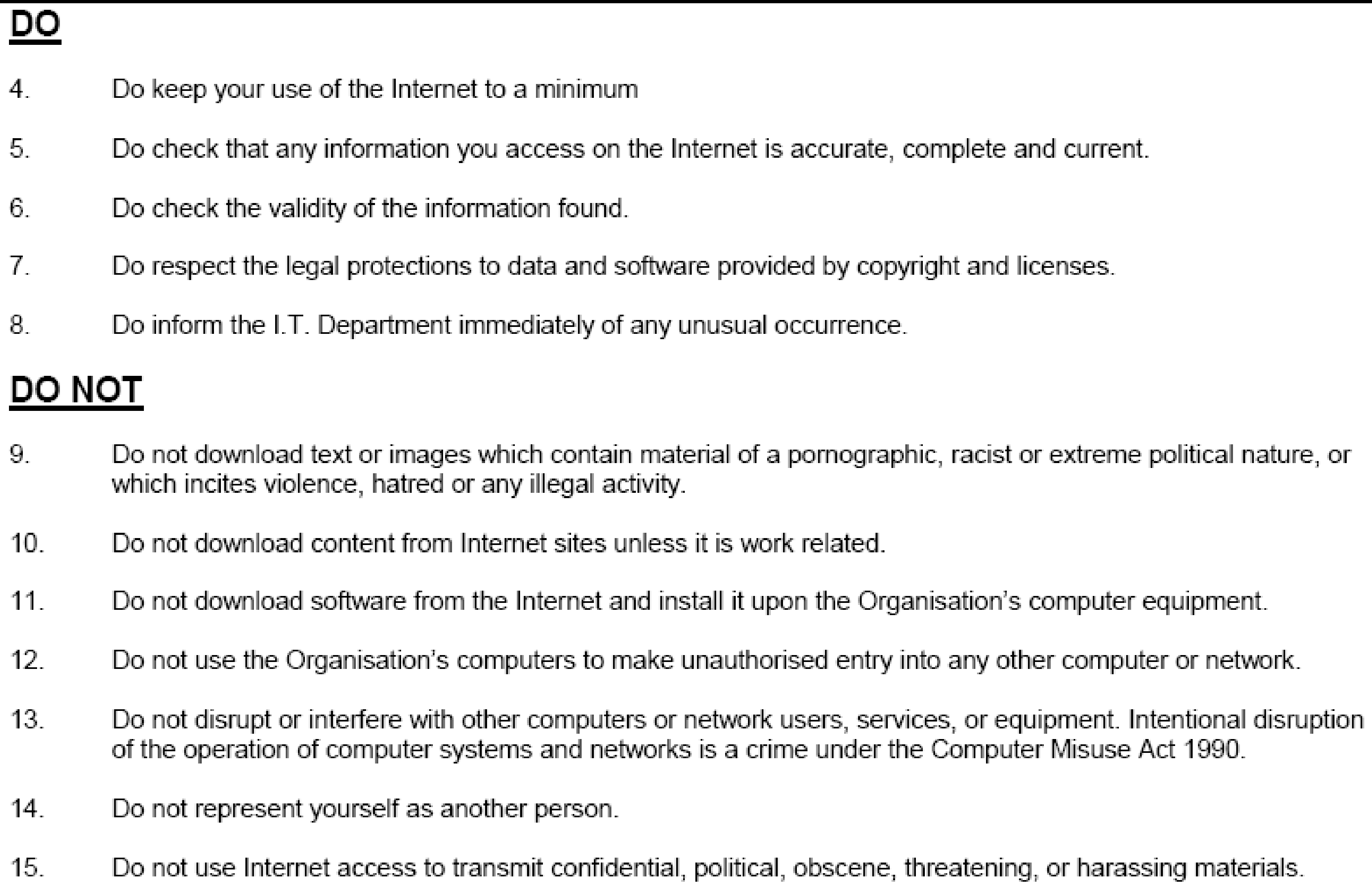
Source: *http://www.watchguard.com/*

Firewall Management policy

1. Ensure firewall management remains strictly controlled.
2. Ensure access control to the firewall and/or operating system to prevent unauthorized access should a firewall platform component be compromised or cease to function.
3. Ensure consistent application of approved rules and configurations on all firewalls.
4. Establish standards and implement secure firewall operating system configurations.
5. Ensure timely implementation of software patches, upgrades and releases.
6. Provide hardware and software maintenance, backup and recovery services to ensure reliable and available services.
7. Ensure only essential services are deployed on each firewall.
8. Restrict access to firewall information such as network addresses, configurations, and attached networks or systems.
9. Provide centralized monitoring and management of all firewalls deployed on the State network.

Source: *http://www.state.tn.us/*

Internet Acceptable Use Policy



DO

4. Do keep your use of the Internet to a minimum

5. Do check that any information you access on the Internet is accurate, complete and current.

6. Do check the validity of the information found.

7. Do respect the legal protections to data and software provided by copyright and licenses.

8. Do inform the I.T. Department immediately of any unusual occurrence.

DO NOT

9. Do not download text or images which contain material of a pornographic, racist or extreme political nature, or which incites violence, hatred or any illegal activity.

10. Do not download content from Internet sites unless it is work related.

11. Do not download software from the Internet and install it upon the Organisation's computer equipment.

12. Do not use the Organisation's computers to make unauthorised entry into any other computer or network.

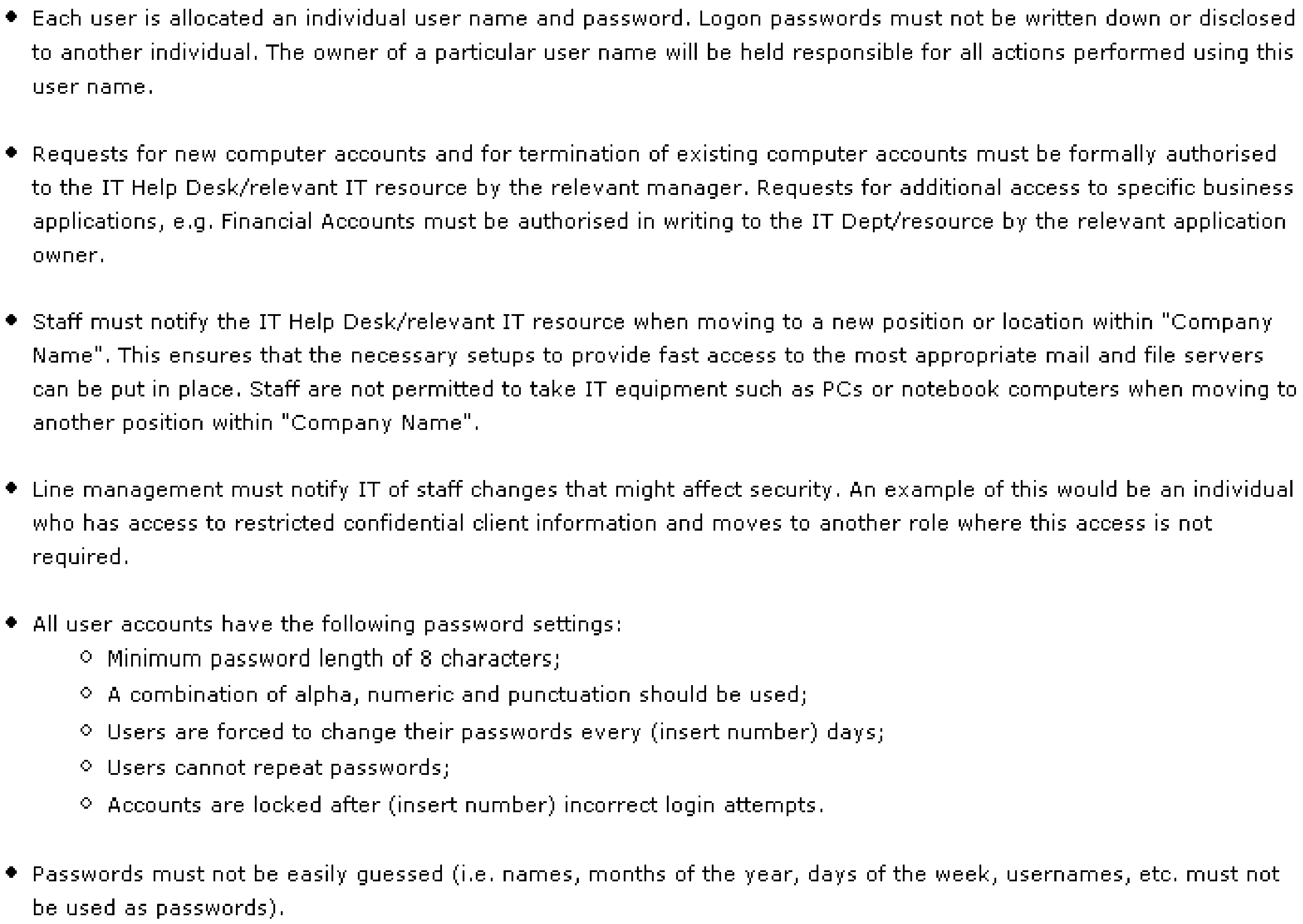
13. Do not disrupt or interfere with other computers or network users, services, or equipment. Intentional disruption of the operation of computer systems and networks is a crime under the Computer Misuse Act 1990.

14. Do not represent yourself as another person.

15. Do not use Internet access to transmit confidential, political, obscene, threatening, or harassing materials.

Source: *http://www.ruskwig.com/*

User Identification and Password Policy



- Each user is allocated an individual user name and password. Logon passwords must not be written down or disclosed to another individual. The owner of a particular user name will be held responsible for all actions performed using this user name.

- Requests for new computer accounts and for termination of existing computer accounts must be formally authorised to the IT Help Desk/relevant IT resource by the relevant manager. Requests for additional access to specific business applications, e.g. Financial Accounts must be authorised in writing to the IT Dept/resource by the relevant application owner.

- Staff must notify the IT Help Desk/relevant IT resource when moving to a new position or location within "Company Name". This ensures that the necessary setups to provide fast access to the most appropriate mail and file servers can be put in place. Staff are not permitted to take IT equipment such as PCs or notebook computers when moving to another position within "Company Name".

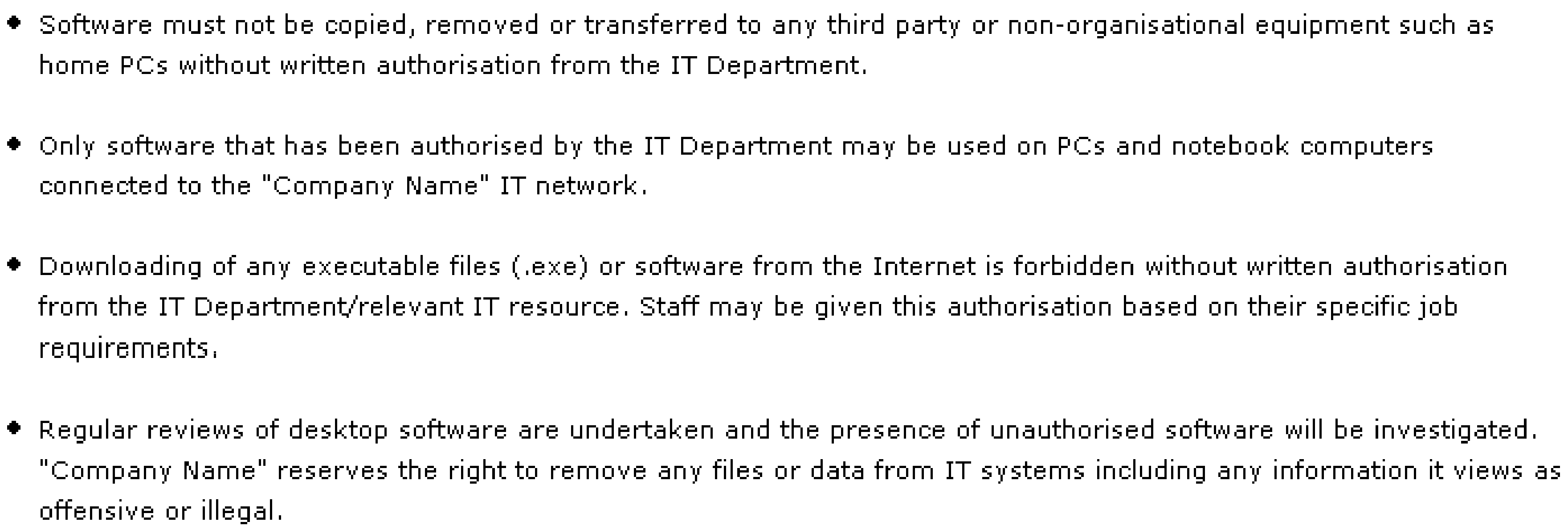
- Line management must notify IT of staff changes that might affect security. An example of this would be an individual who has access to restricted confidential client information and moves to another role where this access is not required.

- All user accounts have the following password settings:
  - Minimum password length of 8 characters;
  - A combination of alpha, numeric and punctuation should be used;
  - Users are forced to change their passwords every (insert number) days;
  - Users cannot repeat passwords;
  - Accounts are locked after (insert number) incorrect login attempts.

- Passwords must not be easily guessed (i.e. names, months of the year, days of the week, usernames, etc. must not be used as passwords).

Source: *http://www.enterprise-ireland.com/*

Software Licence Policy



- Software must not be copied, removed or transferred to any third party or non-organisational equipment such as home PCs without written authorisation from the IT Department.
- Only software that has been authorised by the IT Department may be used on PCs and notebook computers connected to the "Company Name" IT network.
- Downloading of any executable files (.exe) or software from the Internet is forbidden without written authorisation from the IT Department/relevant IT resource. Staff may be given this authorisation based on their specific job requirements.
- Regular reviews of desktop software are undertaken and the presence of unauthorised software will be investigated. "Company Name" reserves the right to remove any files or data from IT systems including any information it views as offensive or illegal.

Source: *http://www.enterprise-ireland.com/*

Summary

Security Policy is a set of objectives and rules of behavior for users and administrators

Prudent Policy provides maximum security while allowing known but necessary dangers

Security Policy suggests the safety measures to be followed in an organization

Security Policy Implementation follows after building, revision, and updating of the security policy

A wireless network policy helps to secure wireless networks, including which devices are allowed to be connected, what security measures should be followed

An e-mail security policy is created to govern the proper usage of corporate e-mail

Copyright 2006 by Randy Glasbergen.
www.glasbergen.com

"No fingerprints, no picture ID, no Social Security number.
I'm afraid your baby presents a serious security risk."

"We don't need to worry about information security or message encryption. Most of our communications are impossible to understand in the first place."