



## Contents

<b>CONTENTS</b> .....	<b>1</b>
<b>INTRODUCTION</b> .....	<b>2</b>
SCOPE.....	2
AGREEMENT.....	2
FAMILIARISATION.....	2
SECURITY PRECAUTIONS.....	2
DISCIPLINARY ACTION.....	3
INTERNET SECURITY - WHY IS IT IMPORTANT TO US?.....	3
<b>INTERNET SECURITY POLICY FOR ALL STAFF</b> .....	<b>4</b>
INTERNET ACCESS.....	4
INTERNET E-MAIL.....	5
NON-INTERNET EXTERNAL CONNECTIONS.....	6
DIAL-IN CONNECTIONS.....	7
VIRUS CONTROLS.....	7
INCIDENT REPORTING.....	7
DATA PROTECTION.....	8
SOFTWARE COPYRIGHT.....	8
<b>ADDITIONAL POLICY STATEMENTS FOR IT STAFF</b> .....	<b>10</b>
VIRUS CONTROLS.....	10
INCIDENT REPORTING.....	10
DATA PROTECTION.....	11
SOFTWARE COPYRIGHT.....	11
FIREWALL CONFIGURATION AND MANAGEMENT.....	12
THIRD PARTY ACCESS.....	13
USER IDENTIFIERS.....	14
PASSWORD MANAGEMENT SYSTEM.....	14
DATA ENCRYPTION.....	15
INTERNET SERVICE PROVIDER.....	15
E-MAIL SERVERS.....	16
E-MAIL CLIENTS.....	17
WEB BROWSER CLIENTS.....	18
PROXY WEB SERVERS.....	19
INTRANET WEB SERVERS.....	19



### Introduction

The Internet Security Policy provides an overview to inform all permanent, temporary, contract and agency staff of their responsibilities for Internet security. It is not exhaustive and staff are expected to comply with the company philosophy that security is of paramount importance. It is the responsibility of staff to be aware of Internet Security issues and to seek the advice of their Manager in case of doubt.

### Scope

The company Internet gateway service provides secure access to the Internet from desktop personal computers. Primary security is provided by using a 'firewall' between the company internal network and the Internet; bypassing the 'firewall' is therefore not permitted.

Connections to third parties other than the Internet is usually via the gateway service providing secure access from desktop personal computers. Primary security is provided by using a 'firewall' between the company internal network and the third party; bypassing the 'firewall' is therefore not permitted.

In some cases, individual external connections are permitted. In these cases, the machine used for external access may not be connected to any internal company network.

### Agreement

By using any external connections from company equipment, users indicate that they will comply with this policy.

### Familiarisation

Staff are required to familiarise themselves with the appropriate User Guides before using any external service. Guides should be issued to all registered users.

### Security precautions

All users of external connections must be formally authorised to do so by their management. Limitations on use must be specified. All risks associated with usage of the Internet must be assessed before using the service.



### Disciplinary action

Any breach of security arising from contravention of this code of practice will result in disciplinary action.

### Internet security - why is it important to us?

The company has a significant investment in computer systems and networks. To a large and continually increasing extent, the company is dependent upon the data which is stored and processed on its computers and the management information that is generated from the data and passed between businesses and outside agencies. The loss of data and computer processing facilities or breaches of data access security could incur significant costs or loss of revenue as a result of:

- Business activities being suspended or partially suspended
- Having to restore the data, computer programs and/or equipment
- Confidential business data being available to competitors
- Fraudulent manipulation of cash or goods

Also, in the case of data stored on computer about living persons, the company must comply with any statutory provisions, for example in the UK, the Data Protection Act of 1984.

Therefore, it is important that all computer systems should have the appropriate level of protection from threats arising from Internets and Internet use.



### Internet Security Policy for All Staff

#### Internet access

1. All access to the Internet must be via the company firewall, bypassing the firewall is not permitted.
2. All users of the Internet must be formally authorised to do so in writing by their management. Limitations on use must be specified.
3. All risks associated with usage of the Internet must be assessed before using the service. Lack of availability, confidentiality and integrity must be considered as the Internet provides no guarantees in these areas.
4. Personal computers accessing the Internet must run resident virus protection software.
5. Each user must have a dedicated username and password; sharing of usernames and passwords is not permitted.
6. Staff must ensure that they are logged off from company systems and the Internet when they leave the office or when leaving their computer unattended for lengthy periods of time.
7. Any license conditions related to the commercial use of software available on the Internet must be observed.
8. Any software program or script downloaded from the Internet must be approved by the IT department. In any event, entertainment software (e.g. games, screen savers) will not be approved.
9. Copyrighted material should not be sent, received or copied via the Internet unless encrypted. Authors should be encouraged to encrypt E-Mail messages that contain manuscripts.
10. Any software program or script downloaded from the Internet should be separately virus checked. Particular care must be taken with compressed files which may disguise the presence of a virus from normal detection.



### Internet e-mail

1. E-mail must not contain indecent, obscene or libellous material, material likely to cause offence or any material which harasses any other employee or third party on the basis of sex, race or disability.
2. Staff must not send or deliberately attempt to receive e-mail known to contain a virus.
3. Staff must not use e-mail for gambling, conducting illegal activities or soliciting for personal profit.
4. Staff must not reveal or publicise information which is confidential either to the company or its customers and clients.
5. E-mail chain letters must not be forwarded.
6. Staff may not access confidential information using the password of another user.
7. Staff may not use company e-mail systems for personal use.
8. Staff should only send information by Internet e-mail which they would be prepared to send on the company's headed paper.
9. Unless specifically authorised by Management, staff should not buy or sell goods or services via Internet e-mail, as such transactions could bind the company. In any event, personal purchases by E-Mail are not allowed.
10. Scanned signatures must not be attached to Internet e-mails. Such signatures can be disseminated by recipients and fraudulently attached to other documents apparently in the name of the company.
11. E-mail attachments should not be opened unless the recipient knows who they are from and is expecting to receive them.
12. E-mail messages sent via the Internet may be accessed by people other than the intended recipient, it should, therefore, only be used for information which is not commercially sensitive or covered by the Data Protection Act unless the information is encrypted.
13. E-mail containing sensitive information may need to be encrypted. Trading partners to be sent encrypted material will require equivalent software.

## Example (Generic) Internet Security Policy



14. E-mail names should not be the same as system logons.
15. Business standards should be observed in e-mail messages.
16. When sending an attachment always mention the format as it may not be obvious from the file name.
17. Some e-mail systems can only accept one attachment at a time, so you may need to send separate e-mails for each attachment if you are unsure.
18. Before forwarding a single e-mail to a new or revised distribution, make sure you read all the earlier messages, as they may contain personal comments that should not be redistributed.
19. Regularly review stored e-mail and delete unwanted material.

### Non-Internet External Connections

1. All external connections must be via the company firewall, bypassing the firewall is not permitted. The only exception is where specific permission has been granted and the machine used for external access is not connected to any internal company network.
2. All users of external connections must be formally authorised to do so in writing by their management. Limitations on use must be specified.
3. All risks associated with usage of external connections must be assessed before using the service.
4. Personal computers accessing any external service must run resident virus protection software.
5. Each user must have a dedicated username and password; sharing of usernames and passwords is not permitted. The only exception is a dedicated service required a group logon, where special controls must be applied.
6. Staff must ensure that they are logged off from company systems and any external service when they leave the office or when leaving their computer unattended for lengthy periods of time.
7. Any data downloaded from an Internet should be separately virus checked. Particular care must be taken with compressed files which may disguise the presence of a virus from normal detection.



### Dial-in connections

1. Staff must ensure that approval is obtained from their manager before using any dial-in service.
2. Equipment held off-site for the purpose of dial-in connections should be appropriately protected (e.g. by power-on password).
3. Equipment held off-site for the purpose of dial-in connections should not be left unattended in a public place.
4. Staff should use a user name and password unique to themselves for all dial-in connections. If this is impractical then tokenised (e.g. SecurID) remote access devices should be employed.
5. Staff should change remote access passwords regularly.

### Virus controls

1. Anti-virus software must be used on all personal computers.
2. All electronic information received by the company must be checked for viruses. This includes all floppy disks, CDs, electronic mail, magnetic tapes, optical disks and removable hard disks.
3. Personal computers which have been identified as having a higher risk of infection must use the extra or alternative products specified by the IT Manager.

### Incident reporting

1. Staff must report all security incidents to the IT Manager.
2. Staff must note any observed or suspected security weakness in or threats to company systems or services. Staff must report any such weaknesses to the IT Manager as quickly as possible.
3. Staff must not, in any circumstances, attempt to prove a suspected weakness, since such an action may be interpreted as a breach of security.
4. Staff must note and report any software that appears to be malfunctioning (i.e. not performing according to specification) to the relevant support staff. If the problem is due to malfunctioning software or the cause cannot be identified, the problem should be reported to the IT Manager.

## Example (Generic) Internet Security Policy



5. If the malfunction appears to be due to a computer virus or other malicious software, the user must follow the actions listed below.
  - 5.1. Note the symptoms and any messages appearing on the screen.
  - 5.2. Stop using the computer and isolate it from other users if possible.
  - 5.3. Inform the IT Manager immediately.
  - 5.4. Do not transfer diskettes from the suspect computer to other machines.
  - 5.5. Do not attempt any recovery procedure.

### Data protection

1. No personal data<sup>1</sup> is to be processed by computer unless the Manager responsible for overseeing compliance with local Data Protection legislation has been notified and until s/he has certified that the intended processing complies with legal requirements, such as the UK Data Protection Act 1984.
2. Applications handling personal data on individuals must comply with data protection legislation and principles.
3. Personal data must be:
  - 3.1. obtained and processed fairly and lawfully;
  - 3.2. held only for specified and lawful purposes;
  - 3.3. not used or disclosed for any reason incompatible with its original purpose;
  - 3.4. relevant and adequate;
  - 3.5. accurate and kept up-to-date;
  - 3.6. not be kept for longer than is necessary;
  - 3.7. made available to the individual concerned on request and that provision is made for corrections;
  - 3.8. kept secure from unauthorised access, alteration, disclosure, loss or destruction.

### Software copyright

1. Copies of licensed software must not be made without authorisation. In any event, software theft is illegal.
2. Software available free or cheaply through bulletin boards and computer clubs should not be used unless a good business case can be made and approval is obtained from the IT Manager.

---

<sup>1</sup>Personal data is any data relating to a living individual.

## Example (Generic) Internet Security Policy



3. Staff must not run their own software on a company computer. If there is a valid business purpose which can best be satisfied by using software for which the company does not hold a license, then a business case should be made and the software acquired by the company. If there is a valid business case for a member of staff to use their own software on a company computer, the system owner must:
  - 3.1. obtain evidence that the user has a valid license to use the software for the intended purpose on company equipment;
  - 3.2. obtain approval for this use from the IT Manager;
  - 3.3. ensure that the software is appropriately tested before it is loaded onto company equipment;
  - 3.4. periodically check that the user continues to hold a valid license; and
  - 3.5. ensure that the software is deleted as soon as the user leaves the company or ceases to hold a valid license for the software.



### Additional Policy Statements for IT Staff

#### Virus controls

1. Anti-virus software must be used on all personal computers.
2. All network servers must run an approved virus protection product.
3. All electronic information received by the company must be checked for viruses. This includes all floppy disks, CDs, electronic mail, magnetic tapes, optical disks and removable hard disks.
4. Personal computers which have been identified as having a higher risk of infection must use the extra or alternative products specified by the IT Manager.
5. A member of the IT support function should be responsible for updating the anti-virus software every month following a defined procedure approved by the IT Manager.
6. A log of when each update was received and distributed should be kept.
7. Where possible the software updates should be distributed automatically to all networked computers.
8. Updates for non-networked computers should be installed by a member of the IT support function and not left to the end user. The only exception to this is non-networked equipment which is not located at company premises e.g. laptops. In such cases, the user should be supplied with regular updates from IT together with a clear set of written guide lines.
9. The software should be write-protected on every machine as part of the distribution or update procedure.
10. The IT support function must ensure that resources are available to respond to any suspected virus infection.
11. The IT support function must report all virus incidents to the IT Manager.

#### Incident reporting

1. Incident management procedures must exist to enable a quick, effective and orderly response to security incidents. The procedures must cover:

## Example (Generic) Internet Security Policy



- 1.1. analysis and identification of the cause of an incident;
  - 1.2. remedial action to reduce the impact of the incident and recover any lost assets;
  - 1.3. planning and implementation of controls to reduce the probability or impact of future occurrences;
  - 1.4. collection of evidence;
  - 1.5. communications with staff or customers affected by recovery from the incident.
2. Staff must be made aware of the company procedure for reporting security incidents, and understand that they are required to report such incidents as quickly as possible.
  3. The IT Manager must maintain a formal reporting and incident response procedure, defining the action to be taken to raise and action an incident report.

### Data protection

1. Applications handling personal data on individuals must comply with data protection legislation and principles.
2. Personal data must be:
  - 2.1. obtained and processed fairly and lawfully;
  - 2.2. held only for specified and lawful purposes;
  - 2.3. not used or disclosed for any reason incompatible with its original purpose;
  - 2.4. relevant and adequate;
  - 2.5. accurate and kept up-to-date;
  - 2.6. not be kept for longer than is necessary;
  - 2.7. made available to the individual concerned on request and that provision is made for corrections;
  - 2.8. kept secure from unauthorised access, alteration, disclosure, loss or destruction.

### Software copyright

1. A valid license must exist for all software to be used on company computers. This includes evaluation copies which may have a limited use license. If there is a limit on the number of copies that may be used, it is the responsibility of the holder of the multi-user license to ensure that this number is not exceeded.
2. Copies of licensed software must not be made without authorisation. In any event, software theft is illegal.



3. Where a PC is attached to a network it is the responsibility of the administrator of the network server to ensure that software on the server is properly obtained, licensed and tested.
4. Software available free or cheaply through bulletin boards and computer clubs should not be used unless a good business case can be made and approval is obtained from the IT Manager.

### Firewall configuration and management

1. Firewalls are only as sound as their supporting firewall policies. It is imperative that the rules concerning the configuration of every component in the firewall (Internet router, firewall, proxy server, virus software) are properly understood, fully documented and carefully implemented. Independent testing of the firewall on a regular basis, and especially immediately after installation, is essential. The majority of successful hacking attempts are due to inadequate or faulty configuration of one or more firewall components. Apply the following in your firewall strategy:
  - 1.1. Implement an address translating router, configured to pass only packets destined for the firewall computer
  - 1.2. A firewall computer supporting at least two (preferably three) network cards, one connecting only to the external router, one to the corporate network and (optionally) one to the demilitarised zone, to which any proxy servers are connected
  - 1.3. Implement an alerting system to warn of attempted attacks. Alerts should ideally be generated by the router, firewall and proxy servers.
  - 1.4. The firewall should be proof against denial of service attacks (either by rejecting packets or by shutting down)
  - 1.5. Remote management of any component in the firewall is not permitted.
  - 1.6. Independent testing of the firewall configuration is essential. Attacks on the firewall by a firm specialising in such services should be carried out immediately after implementation and on a regular basis thereafter.
  - 1.7. Careful screening of employees who are to have physical or logical access to the firewall components or their documentation is most important.
  - 1.8. All firewall components should be located in a secure room with controlled and limited access.
  - 1.9. If Internet downtime is perceived as a potential problem, a duplexed installation might be considered. Bear in mind that the opportunity for configuration error is also doubled in this situation and extra care should be taken in documenting, implementing and testing such an installation.
2. The bottleneck effect of each firewall component must be carefully measured to ensure that future traffic volumes are not constrained by today's choice of product. Performance is as important as security in each of these components.

## Example (Generic) Internet Security Policy



3. Remote access via dial-in directly to company premises must be carefully controlled. A “dial back” policy, requiring the user to be accessing from a known telephone number, further protected by user name and password is strongly recommended. If this is impractical then tokenised (e.g. SecurID) remote access devices should be employed. In any event, proper records of users permitted remote access, controls regarding access time of day, location, etc. must be instigated. Passwords must be changed regularly (most remote access passwords are not) and user names must be unique to each individual. Where possible, audit trails should be generated (and inspected!) for any remote access devices.
4. Staff must be made aware of their responsibilities in using Internets, via a thorough Internet Security Policy.
5. Policies and procedures must be applied to contractors and third-party employees as thoroughly as to staff. Third-party organisations must be asked to sign “like measures” contracts to ensure that they apply similar controls to the company’s.
6. Firewalls can't protect against attacks that don't go through the firewall. Many corporations that connect to the Internet are very concerned about proprietary data leaking out of the company through that route. Unfortunately for those concerned, a magnetic tape or diskette can just as effectively be used to export data.

### Third party access

1. When permitting third parties access to company networks, consider including the following in the contract with the third party:
  - 1.1. permitted access methods, and the control and use of unique identifiers (user IDs) and passwords;
  - 1.2. a description of each IT service to be made available;
  - 1.3. a requirement to maintain a list of individuals authorised to use the service;
  - 1.4. times and dates when the service is to be available;
  - 1.5. the respective liabilities of the parties to the agreement;
  - 1.6. procedures regarding protection of company assets, including information;
  - 1.7. responsibilities with respect to legal matters, e.g. data protection legislation;
  - 1.8. the right to monitor, and revoke, user activity;
  - 1.9. responsibilities regarding hardware and software installation and maintenance;
  - 1.10. the right to audit contractual responsibilities;
  - 1.11. restrictions on copying and disclosing information;
  - 1.12. measures to ensure the return or destruction of information and assets at the end of the contract;
  - 1.13. any required physical protection measures;

## Example (Generic) Internet Security Policy



- 1.14. mechanisms to ensure that security measures are followed;
  - 1.15. user training in methods, procedures and security;
  - 1.16. measures to ensure protection against the spread of computer viruses;
  - 1.17. an authorisation process for user access;
  - 1.18. arrangements for reporting and investigating security incidents;
  - 1.19. involvement by the third party of subcontractors and other participants.
2. When permitting third parties access to company networks, the route from the third party to the computer service may need to be controlled. Consider the following options:
- 2.1. allocating dedicated lines or telephone numbers
  - 2.2. automatically connecting ports to specified application systems or security gateways
  - 2.3. limiting menu and sub-menu options for individual users
  - 2.4. preventing unlimited network “roaming”
3. When permitting third parties access to company networks, consider the need for authentication:
- 3.1. Authentication can be carried out at the application computer or network level. An assessment of business risks and impacts may be required to determine the level of authentication required.
  - 3.2. At both network and computer level, authentication of remote users can be achieved using, for example, a challenge/response system or a line encryption system. Dedicated private lines or a network user address (NUA) checking facility can also be used to provide assurance of the source of connections.

### User identifiers

1. All users should have a unique identifier (user ID) for their personal and sole use, to ensure that activities can subsequently be traced to the responsible individual. User IDs should not give any indication of the user's privilege level (e.g. manager, supervisor)
2. In exceptional circumstances, where there is a clear business benefit, the use of a shared user ID for a group of users or a specific job can be used. Approval by management should be documented for such cases. Additional controls may be required to maintain accountability.

### Password management system

1. Encourage the use of individual passwords to maintain accountability
2. Allow users to select and change their own password
3. Enforce a minimum length for passwords (six characters are recommended)

## Example (Generic) Internet Security Policy



4. Enforce a password change at regular intervals (for systems based on time periods, a period of 30 days is recommended as a default)
5. Enforce a more frequent password change for privileged accounts, e.g. those with access to system utilities
6. Alter default vendor passwords following installation of software
7. Encourage users to select a quality password, not based on:
  - 7.1. months of the year, days of the week or any other aspect of the date
  - 7.2. company names, identifiers or references
  - 7.3. user ID, user name, group ID or other system identifier
  - 7.4. more than two consecutive identical characters

### Data encryption

1. Encryption should be considered for highly sensitive data.
2. Encryption might be necessary to protect sensitive information that is vulnerable to unauthorised access, either in transmission or storage. An assessment of security risks should be carried out to determine if encryption is necessary, and to identify the level of protection required. Specialist advice should be sought to identify suitable products with adequate security, and to design a secure system of key management.

### Internet Service Provider

The security issues surrounding the selection of an Internet Services Provider can be summarised by these questions:

## Example (Generic) Internet Security Policy



1. What employee screening / information security processes are there? (*staff, contractors, third parties*)
2. What physical security measures are there at their sites?
3. What documentation is generated?
4. What are the change control processes?
5. What review and audit processes are there?
6. What audit trails are generated?
7. What testing processes are there?
8. What are the reporting processes to the client?
9. What are the incident response processes?
10. What procedures exist?
11. Level of BS7799 compliance?
12. What Data Protection registration is required for these services?

### E-mail servers

For optimal security, the company will need to adopt the following operational security measures for E-Mail systems:

1. The company needs to ensure that all security controls available in the e-mail server software have been activated. For example, if audit trails are available they should be turned on. If password control is available, it should be turned on. If the password control has a password ageing feature, that too should be turned on. If there is access control to limit users freedom of movement within the e-mail system, it should be activated. If encryption is an available feature, it too should be offered to users. (But only after an evaluation of the implications) If the logical controls in the software are inadequate (for example, no password ageing) then written procedures and awareness education should be used to encourage users to comply with policy.
2. The company should change any default passwords or user accounts, to avoid the common problem of widely-known accounts being subverted by intruders.
3. Once all available security controls have been implemented and any default user accounts disabled, the company must decide whether or not it would be worthwhile and economically feasible to add another layer of security over the e-mail software itself. A third party e-mail security package should be considered, such as Entrust from Northern Telecom or

## Example (Generic) Internet Security Policy



SecureExchange from Axent Technologies.

4. E-mail servers should be given the same level of security as other network servers. Such systems should be kept in a locked computer room or at the very least in a place where they are not readily available to unauthorised access or accidental mishap.
5. The following e-mail security checklist should be followed:
  - 5.1. Implement all available, appropriate e-mail security controls.
  - 5.2. For servers designated as post offices: require ID/password signon, disable "guest" IDs and activate file controls.
  - 5.3. Use a dedicated e-mail server, running no other applications.
  - 5.4. If no dial-up access is required, isolate the post office servers from LAN segments that allow dial-up.
  - 5.5. Try to separate the duties of the LAN administrator and the post office administrator.
  - 5.6. Give users "least privilege" access.
  - 5.7. Use encryption if appropriate to your needs.
  - 5.8. Be sure to destroy e-mail archives when possible.

### E-mail clients

E-mail client software should complement the Internet Security Policy where possible, and should help to enforce the below guidelines. Where logical controls are not available in the software, procedures should be used to encourage users to comply with policy.

1. Users must choose a strong password, preferably one that is composed of an alpha-numeric mix, rather than either a dictionary word (whether English or any other language) or even a series of random numbers. It should be easy to remember but hard to forget. Once they have chosen a strong password, they must keep it secret. And they must change their password frequently.
2. Users should never leave their e-mail accounts open and accessible when they leave their workstations, even for a brief trip to the coffee machine. They should never share their e-mail accounts or e-mail passwords with other employees.
3. E-mail should not be used for document retention.

## Example (Generic) Internet Security Policy



4. Users must be educated about the dangers of e-mail. They should be provided with examples of legal implications of improper behaviour and the threat of snooping or spoofing from competitors. They should be made aware of the different types of external threat. They should know what to do and who to alert when they discover something unusual. They should be able to identify sensitive information and treat it accordingly. They should understand what constitutes appropriate and inappropriate use of e-mail both in terms of content and usage.
5. Users should be educated in the use of "emoticons" so that the intent of their e-mail comments is not misconstrued or taken out of context. Emoticons are the "smiley faces" symbols used in e-mail messages to convey emotional states by representing facial gestures, for example a smile :-), a smirk :-] laughter :-D, or a frown :-(. (You have look at them sideways to get the point.)
6. Use the following e-mail security checklist:
  - 6.1. Develop an intensive security awareness program for e-mail users.
  - 6.2. Establish strong, enforceable policy on individual responsibility and accountability.
  - 6.3. Let users know that e-mail monitoring is a possibility.
  - 6.4. Advertise punishments for those caught snooping.
  - 6.5. Formally define and explain which messages are sensitive and how to handle them.
  - 6.6. Make ID and password mandatory for workstations handling sensitive messages and consider adding an extra security layer.
  - 6.7. Develop and distribute password management guidelines.
  - 6.8. Add lock out and screen-blank capability to workstations able to access a post office; require a password to resume operation.
  - 6.9. Use encryption if appropriate to your needs.
  - 6.10. Be sure to regularly destroy e-mail archives, unless prevented by law or otherwise from doing so.

### Web browser clients

The majority of security controls in connection with Web browsing should be applied at the Firewall. However, some issues may be addressed at the browser:

1. The download directory should be set to a standard directory name. This will control any file transfers, reducing the problems of file management and the potential for virus and Trojan



infection.

2. All default warnings in the browser should be enabled.
3. The use of plug ins and helper applications should be restricted to those tested and approved by IT.
4. JavaScript, Java and ActiveX should be disabled where possible.
5. Users should be trained on the risks and vulnerabilities of using any additional software, including plug ins, helper applications, Java and ActiveX.

### Proxy web servers

A Proxy Web Server can be customised to a degree where its function resembles that of an Intranet Web server. This chapter discusses security controls for Proxy Web servers that purely serve as Web page cache systems. Should the company ever wish to customise Proxy Web server functionality, security comments for Intranet Web Servers should be observed.

Recommended Proxy Web Server security measures:

1. The operating system carrying the web proxy should be “hardened”, whether it is UNIX or NT. Checklists are available from First Base to assist in this process.
2. Regular testing of the security configuration is essential.
3. Web servers should be subject to the same physical security measures as other servers.
4. Thorough documentation should be generated for all elements of the web servers.
5. Change control procedures must be applied to all web servers.
6. Regular review and audit processes must exist for all web servers.
7. Alert software and supporting procedures should exist for unauthorised changes or intrusion.

### Intranet web servers

1. CGI scripts are a major source of security holes. Although the CGI (Common Gateway Interface) protocol is not inherently insecure, CGI scripts must be written with just as much care as the server itself. Unfortunately some scripts fall short of this standard and trusting Web administrators install them at their sites without realising the problems.

## Example (Generic) Internet Security Policy



2. Server side includes (snippets of server directives embedded in HTML documents) are another potential hole. A subset of the directives available in server-side includes instruct the server to execute arbitrary system commands and CGI scripts. Unless the author is aware of the potential problems it's easy to introduce unintentional side effects. Unfortunately, HTML files containing dangerous server-side includes are seductively easy to write.
3. To maximise security, the company should adopt a strict "need to know" policy for both the document root (where HTML documents are stored) and the server root (where log and configuration files are kept). It's most important to get permissions right in the server root because it is here that CGI scripts and the sensitive contents of the log and configuration files are kept.
4. The operating system carrying the Intranet server should be "hardened", whether it is UNIX or NT. Checklists are available from First Base to assist in this process.
5. Regular testing of the security configuration is essential.
6. Intranet servers should be subject to the same physical security measures as other servers.
7. Thorough documentation should be generated for all elements of the Intranet servers.
8. Change control procedures must be applied to all Intranet servers.
9. Regular review and audit processes must exist for all Intranet servers.
10. Alert software and supporting procedures should exist for unauthorised changes or intrusion.