Global Information Assurance Certification Paper

A SYSTEM SECURITY POLICY FOR YOU

April 01

Version Number 1.2b

Contents

1 INTRODUCTION

1.1 Purpose

1.1.1 The purpose of this document is to meet the requirements of the GIAC Security Essentials assignment and to provide other interested parties with a reference document that they can use to get their System Security Policy (SSP) document started.

1.2 Introduction

1.2.1 The first thing the auditor asks is "Please provide me with a copy of your System Security Policies and Security Operating Procedures". Then it starts "we haven't got round to that yet" or "we have them but they are only at draft" or "we don't have a policy just some notes on guidance" or "we tried to put one together but the person left the company before the task was completed" or " we have them but they have not been implemented yet", well there are any number of excuses for not having or not implementing a System Security Policy and the associated security operating procedures.

1.2.2 If you have no security policy why are you applying security measures and what are you applying them to? Why do auditors ask for a written policy? Why do the International Standards Organisation (ISO), the Orange Book (US DoD) and the Communication Electronic Steering Group (UK Government organisation) all stress the need for a written security policy.

1.2.3 Simply this, if you do not have a written and approved SSP then how do you apply the correct security measures to an IT System or network in a consistent and auditable manner? How do you know what measures have to be implemented? How do you define and delegate responsibilities? Where is your authority for implementing security measures that may constrain how people interact with the system and network?

1.2.4 The System Security Policy is the basis for the legitimate application of security measures designed to protect your network from both internal and external threats. Without the definition provided by the policy document there is a very good chance that a security measure that should be implemented will be missed or you will implement measures that are not required, expensive and the cost can outweigh the benefit. Considering that for most companies Security is considered a bottom line cost, this is to be avoided.

1.2.5 There is a saying that the job isn't finished till the paperwork is complete. With IT security it should be reversed to say "don't start the job until the paperwork is to hand".

2 Types of Policy

2.1 Where to begin

2.1.1 The hardest part about a System Security Policy (SSP) is getting started. There are many security companies that either offer to write the policy for you or train you to do it yourself. The following Internet sites provide excellent information about creating a policy document and what should go into it, but as businesses are less forthcoming about providing example policies and this is understandable as providing this service is how they make their money. If at this stage in the document you would like to get a better understanding of what is required to complete a security policy document then try out the following sites:

- http://www.iss.net/customer_care/resource_center/whitepapers
- http://www.information-security-policies-and-standards.com/weblinks.htm
- http://www.pentasafe.com/
- http://www.sun.com/software/white-papers/wp-security-devsecpolicy

2.1.2 There are some government organisations that publish their own SSP. These are also an excellent source of information but remember the policy has been formatted and designed to meet their requirements and what they consider is the threat to their network or system.

- http://csrc.nist.gov/secplcy/doc-man.txt US Dept of Commerce
- http://csrc.nist.gov/policies/welcome.html U.S. Customs AIS Security Policy Manual
- http://info.internet.isi.edu/in-notes/rfc/files/rfc2196.txt

2.1.3 If you are interested in seeing how the US DoD deals with securing IT systems then the site URL below sets out the requirements for establishing a trusted computer system evaluation criteria (TCSEC). In the context of this document and for most commercial organisations the criteria detailed in TCSEC are too onerous, however for financial institutions and where the care of other peoples money is a priority the principles laid down in TCSEC are relevant.

- http://www.antionline.com/archives/text/rainbow_books/orange.html

2.2 ISO 17799

2.2.1 ISO 17799 is the International Standards Organisations detailed security standard and is organised into 10 major sections, it was derived from British Standard BS7799 and is designed for implementation by companies in the commercial sector. It is one of the most widely recognised security standards and is comprehensive in its coverage of security issues. However compliance with ISO 17799 is far from trivial and is a difficult task even for the most security conscious organisation, it requires commitment from the top, CEO level, and the money to fund the effort. This URL will take you to ISO information http://www.riskserver.co.uk/iso17799/

2.2.2 After looking at all the available information on putting an SSP together it seems a daunting task. Often just the thought of having to put everything down on paper brings the whole idea to a halt. Having looked at and used various sources of information from BS7799, Communications Electronic Security Group (CESG), a UK Government organisation, DERA the UK Defence Research Agency, the Royal Airforce (RAF), the Orange book and other commercial organisations. The following is a suggested SSP format that can be tackled as you would eat an Elephant, one bite at a time. The following format allows you to address each area into small logical steps. The assumption made is that you know your system, it has been baselined and a risk assessment has been carried out. This ensures that the security measures to be implemented as part of the policy are pertinent to your system.

2.2.3 In the next section a suggested format for an SSP is detailed.

3 The System Security Policy

3.1 Basic Facts

3.1.1 The following details need to be in this section

- Name of System/Project
- Location of System
- Key Target dates (if required)

3.2 Security Responsibilities

3.2.1 Unless responsibilities are defined there is a tendency for staff to claim that as nothing was written down it was not their responsibility.

- System Manager/Project Manager (originator of SSP)
- Prime Contractor (if relevant)
- System Administrator
- System Security Officer/Administrator
- Database Administrator

3.3 Status of Document

3.3.1 Just good housekeeping and configuration control.

- Version Number
- Superseded documents

3.4 System Description

3.4.1 This section is designed to enable the Project Manager or System administrator to define exactly what they are looking after and for any third party to be able to quickly understand their responsibilities.

- Role of system. The role of the system in terms of data processing, data storage and communications as follows:
  - Type of information to be held on the system and output from system
  - Types of user (administration, normal user, print controller etc)
  - Number of users
  - Classification of data (Finance Only, HR Only, Project Eyes Only, if required)
  - Quantity of data (Nbytes)
- System Configuration. A description of the working elements of the system that carry out specific tasks.
  - Number of terminals
  - Number of control consoles

- Number and types of terminals (intelligent, dumb, print etc)
- Media loading arrangements
- Software (OS and version number)
- Interconnections (LAN and WAN)

3.5 Security Requirements and Measures

3.5.1 This section consists of a statement of the security requirements to be met and the measures needed to achieve them. This should be agreed with a higher authority usually referred to as an Accreditor, and should be broken down as follows:

- Threats to confidentiality, integrity and availability of data. The nature and resources of possible attackers and the attractiveness of the system and data as a target.
- What will the impact be if the data is accidentally disclosed.

3.6 Security Domains

3.6.1 This is a key element of this policy document, by defining the security domains for the system it is possible to break down the policy into manageable pieces that can be completed domain by domain until the document is fit for purpose. For this type policy there are three domains, Global Security Environment (GSE), Local Security Environment (LSE) and the Electronic Security Environment (ESE).

3.6.2 They are defined as follows:

- GSE is the area in which the system is located in which the security relevant factors are defined that are considered to be outside of the control of the project manager/system administrator. E.g. control of access to the building which is usually the responsibility of the security company or facilities manager.
- LSE this consists of the security environment under the control of the project/system manager and the security boundaries with the GSE.
- ESE deals with the security aspects of the system and its interfaces with the LSE and GSE.

3.6.3 By using domains to break down each section of the policy to be worked on it will be easier to put together in small logic steps that follow a consistent pattern throughout the document. It will also ensure that by following this pattern defence in depth is achieved.

3.7 Definition of Security Measures

3.7.1 In this section of the security policy the measures to be taken to achieve security should be described. The list below is not necessarily comprehensive and others maybe required to meet specific system security requirements. As a minimum the following headings are recommended:

- Identification and Authentication - establishment of a claimed identity
- Access Control - the control and authorisation of access to information by a user

- Integrity – prevention of unauthorised amendment or deletion of information
- Accounting - the recording of an account holder's security related actions
- Audit - the monitoring of security related events
- Reliability of Service - the preservation of availability
- Data Exchange - the protection of inter-communication.
- Non-repudiation - to render an event undeniable

3.7.2 In order to ensure consistency throughout the document each section dealing with the security measures should start with the following headings:

- Definition of the Term
- Security principle to be upheld
- General security risks to be countered
  - If required specific examples of risks that need to be considered can be detailed
- Assertions – an explicit statement in a SSP that security measures in one domain constitute and adequate basis for security measures in another.

4 Example using Domains

4.1.1 In order to show how the use of domains and security measures are put together in small logical steps to build up to a complete policy, the following is how a single section of the document "Access Control" would be put together.

4.2 Access/Access Control

4.3 Definition

Access is defined as the condition where the potential exists for information to flow between entities. Access Control is control over the flow of information between entities.

4.4 Security Principle

Access to business sensitive information should be limited to persons with the appropriate rights and need to know.

4.5 Security Risk

Individuals, without the correct clearance or need-to-know, may intentionally or accidentally gain unauthorized access to business sensitive information. Business sensitive information may be sent to destinations not authorised to receive it.

4.6 Assertions

4.6.1 Access to the GSE is under the control of the local Security Guard and reception staff.

4.6.2 Users protect all business sensitive information passed from the systems to the GSE in accordance with its classification.

4.6.3 Access to system hardware is restricted to those authorized to do so.

4.6.4 All unescorted individuals within the LSE are known and trusted by The Company.

4.6.5 SyOPs specify the procedures associated with managing user access rights, and define procedures for :

a) identification, marking, recording and handling and storage of magnetic media

b) handling of system hard copy outputs

c) disposal and repair of faulty or surplus equipment containing memory.

4.6.6 System Administration staffs are responsible for maintaining systems security, using permitted administrative functions.

4.6.7 The System Administration staff functions are identified by roles and associated permissions. Such roles control access to, and use of, the systems Administration functions. These controls are restricted to what is authorized and necessary for the performance of their tasks. The roles include:

a) Network System Manager

b) System Administrators

c) Site Support

d) System Security Officer

e) Audit Administrator (The role of the Audit Administrator is carried out by the Security Administrator).

4.7 GSE Measures

4.7.1 Reception staff or Security Guards shall control access by personnel to buildings in which a system is installed. Physical security of sites is the responsibility of The Company.

4.7.2 Workstations, printers, graphical scanners and optical device readers shall be placed in office space within the GSE.

4.7.3 Automatic virus detection shall be installed on server to ensure any magnetic media intended to hold or holding User data is virus checked.

4.7.4 The Security Guards shall ensure that offices are left secure at the end of the working day and all desks are cleared, where possible.

4.8 LSE Measures

4.8.1 Servers, routers, Firewalls and where possible control consoles shall be accommodated in the secure computer room. Access to the computer room shall be limited to authorized personnel and shall be re-verified on a periodic basis.

4.8.2 SyOPs shall define user responsibilities with regard to use of the systems. Users shall not be admitted to the systems until they have been adequately trained in the use of the system and security features.

4.8.3 System Administration staff shall ensure that administrative functions are not made available to normal users.

4.8.4 Access to the Configuration Management (CM) system and its data shall only be allowed to personnel authorized to carry out CM tasks.

4.8.5 User permissions shall be set up and maintained as per the site specific security procedures.

4.8.6 Removable classified material shall be secured in lockable containers, when not in use.

4.8.7 SyOPs shall define procedures for:

a) access control, recording, supervision and escorting of personnel in the Computer Room

b) control of Protectively Marked material

c) recording of actions undertaken by System Administration personnel.

4.8.8 Magnetic Media and Paper Output: Access to systems magnetic media shall be restricted to authorized staff. The following shall be marked:

a) Magnetic media for the storage of system and archived user data

b) Systems hard copy outputs shall be marked and handled as for the highest data protective marking for the systems or server, unless the owner of the data can assert that it should be of a lower data protective marking.

4.9 ESE Measures

4.9.1 The user profile shall define the set of facilities each user is authorized to access. The systems shall constrain the profile by password mediation to only those facilities that the User is authorized to use.

4.9.2 The System Administration facilities shall be:

a) issuing initial passwords

b) maintenance of user and role accounts

c) maintenance of hardware accounts

d) Domain management (controlled at corporate level)

e) management of system addresses

f) setting password expiration period

g) management of groups

h) creation and distribution of new software packages

i) update site or system inventory

j) perform back-up and restore

k) configuration of workstation or server

l) unlock workstation

m) set system time

n) management of print resources

o) close down and start-up of system

p) monitor system performance

q) perform diagnostic routines

r) check software integrity

s) examine and analyze the accounting logs

t) maintain accounting filters

u) administer audit alarms

v) allow the operator to archive and delete an accounting log.

4.9.3 The Security Administration facilities shall be:

a) Audit User accounts

b) Audit security logs

c) Audit of password logs

d) Audit of Administrative accounts

4.9.4 All users shall have automatic virus detection software installed on their workstations and/or Laptops.

4.10 Configuration of Electronic Mail

4.10.1 E-mail shall be provided internally for all users of the systems as requested. User responsibilities shall be as stated in SyOPs.

4.10.2 All Email shall be virus checked.

4.11 Remote Access Control

4.11.1 Only the Company systems staff, authorized by the System Manager shall be permitted remote access to the systems.

4.11.2 The SecurID security application shall be implemented on the network to ensure secure User authentication for remote access. No other forms of remote access shall be permitted. The application shall maintain an encrypted list of authorized users, their passwords and profiles for identification and authentication before access is permitted.

4.11.3 Remote access shall be implemented by the use of a Remote Access Server with integral auto switching, a security application and systems Interface.

4.12 Internet Access & Firewall Configuration

4.12.1 Firewalls shall be employed to ensure data are only accessed by individuals with a need to know, and with the correct access privileges.

4.12.2 All Firewalls shall implement a Default Deny security strategy. That is a strategy that states "that which is not expressly permitted is denied". The Firewall security policy is maintained as a separate document.

4.12.3 Where deemed necessary, an encrypted VPN shall be implemented using a minimum of 56bit, and where possible 128bit encryption, for secure communication over the Internet.

4.12.4 In order to facilitate changes in client access requirements to shared resources, the System Manager, on the authority of the Security Manager, shall be able to permit access to the systems via the Firewall without the requirement to re-submit this document to the Accreditation Authority. This interconnection shall be subject to the provisions of a Partner to Partner Interconnection Policy.

4.13 Putting it all Together

4.13.1 Once you have completed Access control it is a simple matter of selecting another Security Measure from the list and applying exactly the same process as you have above. Add them all together with the detail as outlined in paragraphs 3.1 to 3.4 and you will have your SSP and be ready to move on to the Security Operating Procedures.

5 Security Operating Procedures (SyOPs)

5.1 Where SyOPs fit in

5.1.1 The role of Security Operating Procedures (SyOPs) is to look downwards to those who must enforce the SSP. SyOPs are the means by which the System or Project Manager can ensure that the responsibilities he/she has accepted are actually carried out in the day to day operation of the system.

5.1.2 Once again it is not the intention to include a complete document but as an example and to show that SyOPs are directly related to the SSP, the following is the section within the SyOPs dealing with Access Control for an NT based system:

5.2 Access Authorization

The LAN Team leader and LAN Team Administrators shall have the ability to restrict access to information to those Users/groups who have a need-to-know. All maintenance engineers and visitors must be in receipt of a valid visitor's security pass.

5.3 System Access - Authorized Users

5.3.1 All Users shall be authorized, by the LAN Team Administrators to access the system via a unique account and password.

5.3.2 The LAN Team Administrators shall maintain a list of Authorized Users including:

a) Full name of the Authorized User

b) Name of Group/Office/Department etc

c) Authorized Userid allocated for The Company

d) Renewal date for access permissions.

5.3.3 Authorized Users shall be retired from the list by the LAN Team Administrators under the following circumstances:

a) Upon expiration of their authorization

b) When advised by the Line Manager

c) When advised by Human Resources

d) Upon termination of employment or contract.

5.4 New User Account Creation

This process shall be carried out as documented in the local site IT Operations Handbook.

5.5 Rights and Permission Approval

Special rights, permissions and privileges are granted to those whose job function requires it and are to be monitored and controlled on an ongoing basis. A formal request shall be submitted using a Company Request form and signed by an authorized submitter stating justification for all escalation of rights, permissions and privileges.

5.6 User Account Properties Options

5.6.1 User Must Change Password at Next Logon

Default = OFF

After a new user account is automatically generated by the system and the appropriate request has been approved (see section titled "Joining the THE COMPANY_MASTER Windows NT Domain in the Windows NT Policies and Procedure document), an initial password will be automatically generated using a random generator for each account. This option is initially turned on and forces the user to change the initial password and avert any unauthorized logons with the randomly generated password. After this initial required reset, the option is turned off automatically.

5.6.2 User Cannot Change Password

Default = OFF

5.6.3 Account Disabled

Default = Off

This option is turned off by default except in cases of misconduct, suspicion of a breach in security or simply because a user goes on vacation or on temporary leave. User accounts may also be disabled if the activity status of the account shows that it has been inactive for 30 days or more. The ON setting prevents anyone, other than an administrator or account operator, from accessing the user account.

5.6.4 Account Locked Out

Default = Off

This option appears if an account locks because there were too many failed logon attempts. This last option is an indication that someone has attempted to break into an account unless the user simply forgot the password. Only a domain administrator can remove the lock.

5.6.5 **Logon To:** Here you specify the names of the computers that the user can log on to. This is an important security feature, because it forces users to log on to systems where their activities can be physically monitored. It also prevents hackers from logging on to an account from their base of operation, which might be outside your company. The Company will not limit the machines a user can log onto except in situations where the limitation is warranted. Each user and manager will be notified in advance if such a situation becomes necessary.

5.6.6 **One user account for each member of staff:** The Company standard is that each member of staff should only have one user account. The exception is for Administrators and other power users who are allowed to have two accounts, one for everyday tasks and another for administrative functions.

5.7 Locked User Accounts

5.7.1 The LAN Team Administrators shall investigate all occurrences of locked accounts. The LAN Team Administrators or designee, who shall ensure the

correct, User-id is being input, shall assist users with failed log-ins. If the User again fails to log-in a password change shall be initiated.

5.7.2 The LAN Team Administrators under the authority of the LAN Team Leader shall proactively lock accounts for administrative and/or security reasons.

5.8 Password Standard

Alpha, numeric with at least one capital

5.8.1 **Maximum Password Age - 45 days**

This is the period of time that a user is allowed to use a password before Windows NT requires that the user change the password. The Company require that you set this value to 45.

5.8.2 **Minimum Password Age - 1 day**

This setting can be used to prevent a user from immediately reverting back to a previous password after a change. It specifies how long a user must wait after changing a password before the user can change it again. The Company require that this value be set to 1.

5.8.3 **Minimum Password Length - 8 Alphanumeric characters**

This is a critical setting for security reasons. If users create short passwords, a cracker is more likely to discover a password. The Company require that this value is set to 8.

5.8.4 **Password Uniqueness - 10**

This option can prevent users from toggling among their favorite passwords and reduces the chances that a hacker/password breach attempt will discover passwords.

NOTE: Because of the way passwords are saved in a table, users cannot reuse a password until they have changed passwords n+2 times, where *n* is the number of passwords remembered. So if Password Uniqueness is set to 10, users cannot revert to the first password until they have changed their passwords twelve times (10+2).

5.8.5 **Account Lockout - after x bad logon attempts = 5**

The Account lockout feature is implemented to prevent brute force password cracking/guessing attacks on the system. Each failure will then appear in the Security Event Log, which can be viewed with the Event Viewer. The account that is attempting log on and the machine where the logons are occurring are listed in the log file. When enabled, the Account Lockout option in the Account Policy dialog box allows the following options:

5.8.6 **Users must log on in order to change password = Yes**

This option prevents users from changing their passwords if the passwords expire. They will not be able to log on and will need to call an administrator to have their password changed.

5.9 System Passwords

5.9.1 Any standard passwords supplied with System e.g. SYSTEM, MASTER, GUEST etc. shall be changed before the System is accessible to unprivileged Authorized Users.

5.9.2 All System passwords shall be treated as confidential and protected accordingly. It is the responsibility of the User to ensure his/her password is secure at all times. The password shall not be written down, except the copy written down and held securely by the Security Administrator.

5.9.3 If a User feels his password has been compromised in any way then action shall be taken immediately to change the password. Under no circumstances shall a User allow others to use his/her User-id and password.

5.9.4 Passwords that allow access to System administration facilities shall be written down and held securely by the Security Administrator.

5.9.5 The Security Administrator and LAN Team Leader have overall responsibility for the policing of User-id's and passwords and for maintaining a record of all Users.

5.9.6 The initial User-id and password is allocated by the Windows NT Administrator or designee, when first used the System shall prompt for a password change.

5.9.7 The Windows NT Administrator or designee shall reinstate a locked out Authorized User only when satisfied that an attempt to breach the security policy has not taken place.

NOTE: Manually adding new user accounts to the Windows NT security database on THE COMPANY MASTER is strictly prohibited without specific approval from Server Engineering Manager.

5.9.8 Authorized User-id shall be considered for retirement if the authorized Users have not logged on for a period of two months.

5.9.9 Once authorized the LAN Team Administrators shall assign privileges associated with the User role for all Users prior to there having access to the system. If a User-id is no longer required the LAN Team Administrators shall be informed, and shall then initiate removal of that User-id from the system.

5.9.10 Only authorized LAN Team administration personnel shall have access to the OS. The Operating System shall be backed up and periodically compared to the live version, anomalies shall be investigated by the Company Security Manager in conjunction with the LAN Team Leader and fully documented for audit purposes.

5.9.11 The Administrator account is a built-in account that is installed when a Windows NT system is set up. In a domain environment, the Administrator account is set up simultaneously with the primary domain controller in the domain. The person setting up the system specifies the initial password for the Administrator account.

5.9.12 The Administrator account can never be disabled or deleted. This safeguard ensures that the Administrator can never be locked out of the system, thus allowing for a total denial of service assault. You cannot even set lockout features for the account to prevent someone from trying multiple passwords in an attempt to illegally access the account.

5.9.13 Because of the security risk to the Administrator account, every possible precaution shall be taken to ensure the account's security. Select individuals are to be assigned individual accounts with essentially the same permissions but without the no-lockout feature built into the Administrator account.

5.9.14 The original Administrators account is not to be used except in emergency situations such as a denial of service attack whereby all other administrative accounts are disabled, locked out or deleted. The account will be renamed and given an alphanumeric password. Copies of this password will be held securely by the Security Administrator.

6 Summary

6.1.1 After having looked at and modified various methods of putting an SSP together I consider that the use of Domains to breakdown the structure of the document into manageable sections makes the production and implementation of a reasonable and effective security policy an achievable task.

6.1.2 The sections included at paragraph 3.7.1 are by no means exhaustive but if completed diligently will ensure that the requirements of Confidentiality, Integrity and Availability are achieved.

6.1.3 The format of the SSP as presented can be expanded or reduced depending on the assessed security measures required for an individual system. The SANS organisation has a number of excellent policy examples and the policy content as outline by Michele Crabb-Guel is excellent for ensuring that all areas that need to be in a policy are given due consideration. These can be found at http://www.sans.org/newlook/resources/policies/policies.htm

6.1.4 Security is a bottom line expense and this should always be borne in mind. Businesses need to be convinced of the need to pay for security and often regard security more as a hindrance than help in supporting or providing services to their users and customers. For a more flexible approach to implementing an SSP I have therefore borrowed the term "Adaptive" used by the company Internet Security Services at:

http://www.iss.net/customer_care/resource_center/whitepapers/

6.1.5 The term "Adaptive" is used to ensure that the SSP is flexible and ensures that the business is not a prisoner to a Security Policy that is set in concrete. By allowing and documenting exceptions to a policy it is possible to meet the requirements of business and at the same time maintain the security stance required by the CEO's policy direction.

6.1.6 It is therefore recommended that consideration is given to adding an "Exceptions Policy" in which any variation to the security measures detailed in the SSP can be assessed for risk, which is then written down. Based on the risk assessment the exception to policy can be approved by the Accreditor or if the risk it too great but the service is still required additional security measures can be implemented. This action is then documented as part of the Exception Policy and held with the SSP.

7 References and Cited Sources

CESG Electronic Information Systems (Infosec) Memorandum No 5: System Security Policies, Issue 3.0, July 1994 Unclassified

CESG Computer Security Memorandum No 1 – Glossary of Computer Security Terms, Issue 2.2, November 1993

AP 3086 – RAF Manual of Security 5th Edition

Department of Defense Trusted Computer System Evaluation Criteria (TCSEC) also referred to as the "Orange Book"

Internet Security Systems (ISS) Creating, Implementing and Managing the Information Security Lifecycle

Principles and Practice of Computer Security, Admiral Management Services Ltd

Manual of Army Security Vol 4 – Information Technology Security dated 1991.

Site Security Handbook RFC 1244 dated July 1991.

http://www.iss.net/customer_care/resource_center/whitepapers/

http://www.information-security-policies-and-standards.com/weblinks.htm

http://www.sun.com/software/white-papers/wp-security-devsecpolicy

http://csrc.nist.gov/secplcy/doc-man.txt US Dept of Commerce

http://csrc.nist.gov/policies/welcome.html U.S. Customs AIS Security Policy Manual

http://info.internet.isi.edu/in-notes/rfc/files/rfc2196.txt

www.sans.org/newlook/resources/policies/policies.htm

http://www.antionline.com/archives/text/rainbow_books/orange.html