

Introduction to Security Policies, Part Four: A Sample Policy

Charl van der Walt 2001-10-22

Introduction to Security Policies, Part Four: A Sample Policy

by *Charl van der Walt*

last updated October 22, 2001

This is the fourth in a four-part overview of security policies. In the [first article](#), we looked at what policies are and what they can achieve. The [second article](#) looked at the organizational support required to implement security policies successfully. The [third installment](#) discussed how to develop and structure a security policy. This installment will take a look at a few examples of security policies.

An IP Network Security Policy

This section contains an example of a position paper for an IP network for a fictitious company that we shall call "Foobar". The policy documented here makes extensive use of the system of classification that was explained in part two of this series. This system of classification should be well understood before continuing.

Intent Statement

The intent of this policy is to ensure that all systems installed on the Foobar network are maintained at appropriate levels of security while at the same time not impeding the ability of Foobar users and support staff to perform their work. The purpose is:

- to define where equipment is to be placed on the network;
- to define who may access network equipment;
- to define how access to this equipment is to be controlled; and,
- to define how data traveling over the network is to be protected.

Applicability

This policy applies to:

- any IP networks (existing and future) to which Foobar network equipment is connected;
- all equipment connected to the networks mentioned above;
- any IP networks across which Foobar data travels;
- data in transit over any of the above-mentioned networks;
- network administrators managing the equipment;
- project leaders requiring new equipment to be connected to the network; and,

- all users utilizing equipment that is connected to the network.

This includes, but is not limited to:

- the User LAN - 2.3.4.0/24;
- the SERVER LAN - 2.3.5.0/26;
- the Backup SERVER LAN - 2.3.5.64/26; and,
- all backbone services, Switches, ADSL, Internal Dial-Up, etc.; and,
- remote sites.

This policy will also apply to all equipment connected to the networks mentioned above, and all Foobar employees using any of this equipment.

Statement of Foobar's Position

The security policy is based on the principles and guidelines described in the Foobar *Information Security Framework* document. All Foobar network equipment (routers, servers, workstations etc) shall be classified according to the standard Foobar classification scheme and placed in a network segment appropriate to its level of classification. Access to these segments must be controlled in an appropriate manner. Whenever data travels over a network segmentation of a lower security classification then the data shall be protected in manner appropriate to its classification level.

Classification

In accordance with the Foobar *Information Security Framework* document, all users, hosts and data must be classified as security level 1 (unclassified), 2 (shared), 3 (company only) or 4 (confidential). All physical network segments, IP subnets and other IP traffic carriers must be classified in the same way. All data travelling on an IP network must be classified, and all users using network equipment or requesting data over the network must be assigned a level of clearance according to the same system.

It is the function of the person designated as the equipment owner to have all equipment under his or her control classified. The owner is defined as the head of division installing the equipment. Classification is done in consultation between the owner (or an assigned representative) and the Security Officer, but the final decision shall lie with the Security Officer.

For a description of the Foobar system of security level classification, the concept of ownership and the role of the Security Manager, refer to the Foobar *Information Security Policy Framework* document.

Network Segmentation

1. Unless otherwise stated in the security policy or in the *Information Security Policy Framework* all

network segments are classified Level 1 - *Unclassified*.

2. The classification of network segments is given in the section of this article entitled *Discussion of Classifications*, which follows.
3. A network segment can only be classified as another security level with approval of the Foobar Security Manager. Its new level of classification must be recorded in this document and all divisional heads must be notified.
4. Wherever a network segment connects to another network segment with a different security level, then the connection between the two networks must be controlled by an approved trusted point. A trusted point is equipment capable of regulating the flow of traffic between two network segments in a manner appropriate to the classification of the networks. Trusted points are covered in detail in the section that follows.
5. No network equipment may be connected to a network segment that is not of the same security level as the equipment itself.
6. The Foobar Security Officer may also choose to segment two networks of the same security level.

Trusted Points

1. The trusted point used to segment two networks shall be appropriate for the network with the highest security level.
2. The default behavior of a trusted point must be to deny all IP traffic between the network segments it protects.
3. At the discretion of the Foobar Security Manager, the default behavior of the trusted point may be to allow all traffic out from the network with the higher security level whilst denying all traffic in.
4. At the discretion of the Foobar Security Manager, the trusted point may be configured to allow specific into the network with the higher security level.
5. All trusted points must be completely under the control of the Security Manager. Access to any trusted point shall only be granted with the explicit permission of the Security Manager and under his or her close supervision.
6. There are a number of technologies that can act as trusted points. They are divided into the following categories:
 - Network Level Control: TCP wrappers, *host.allow* lists, filter routers, network-level firewalls, V-LAN switches etc.;
 - User Level Control: application proxies, user-level firewalls etc.; and,
 - Strong User-Level Control: token-based user authentication systems, certificates etc.
7. Whenever there is a connection that skips over one security level the strong user level control must be used. Even if strong user control is used, a connection may never skip more than one security level.
8. Control of traffic must be exercised in the manner listed below:

For connections into *Unclassified* classified segments

From	Control Type	Comment
Unclassified	No controls	
Shared	No controls	
Company Only	No controls	<i>With the exception of the Internet</i>
Confidential	No controls	

For connections into *Shared* classified segments

From	Control Type	Comment
Unclassified	No controls	
Shared	No controls	
Company Only	No controls	
Confidential	No controls	

For connections into *Company Only* classified segments

From	Control Type	Comment
Unclassified	<u>Via a proxy</u> : Network level control to and from the proxy. <u>Direct</u> : Strong user-level control	<i>This allows both for things like incoming SMTP and user dial-in.</i>
Shared	Network level control	
Company Only	No controls	
Confidential	No controls	

For connections into *Confidential* classified segments

From	Control Type	Comment
Unclassified	Not permitted	
Shared	Not permitted	
Company Only	Strong user-level control	
Confidential	No Control	

Data in Transit

1. Data moving on the network between any two network-components is considered to be "data in transit". This also includes all control and management sessions.
2. All network technologies are regarded as either "safe" or "unsafe" in their native state (i.e. without any encryption). The only networks regarded as safe by Foobar are Frame-Relay PVCs (as used on the Foobar backbone) and switched Ethernet LANs. All other network types are regarded unsafe.
3. All data in transit over an unsafe network segment that has a classification lower than the

classification of the data must be protected by data encryption. Data in transit over a safe network segment may be encrypted at the discretion of the Security Officer.

4. Encryption of data in transit may take any of the following forms:
 - o **network encryption**, in which data is encrypted at the IP layer (for example, with IPSec);
 - o **session encryption**, in which data is encrypted at a TCP layer (for example, with SSL);
 - o **message encryption**, in which blocks of data are encrypted before they are sent (for example, with SMIME); and,
 - o **data encryption**, in which the entire data package is encrypted before it is transmitted (for example, with file encryption).
5. Encryption systems used must offer strong encryption (more than 100 bit encryption keys) and use internationally recognized encryption algorithms. The choice of the crypto-algorithm is the responsibility of the Security Officer and is laid out in Foobar's position paper on Cryptography.

Access to the Internet

Access to the Internet from Foobar networks is considered a special case and is dealt with as an issue on its own in the position paper on Internet Access.

Discussion of Classifications

Classification of Users

1. Every user is designated as *unclassified* until his or her classification is explicitly changed with the written approval of the Security Officer.
2. When a new employee joins Foobar, a request is made by the employee's manager to the Security Officer for a new level of clearance. It is the responsibility of the manager to justify the requested level of clearance.
3. Unless there is strong justification, all new employees shall be cleared for the level *Foobar Only*, but only after they have signed an employment contract including acceptance of this policy and non-disclosure forms.
4. The Security Officer is responsible for managing and controlling the record of clearance levels for all personnel.
5. It is the responsibility of all system owners and system administrators to determine the security level of a given user before granting that user access to any system.
6. It is the responsibility of the user to know his or her own clearance level and to understand the rights and limitations associated with that clearance.

Classification of Equipment

1. All computing equipment must be given a classification by the Foobar Security Officer.

2. Classifications for existing Foobar equipment are as follows:
 - all user workstations, file-servers, print-servers etc should be classified as "Company Only";
 - all Server LAN servers and other hosts used in the management of the Foobar backbone infrastructure or Foobar internal network infrastructure will be classified as "Confidential";
 - all backbone equipment (including switches, remote access servers, ADSL chassis etc) that is not located on Foobar premises will be classified as "Shared"; and,
 - all equipment used in the transfer of data to and from the Internet will be classified as "Shared".
3. The Security Officer must maintain a complete list of the classifications of all computing equipment in the Foobar network and in the Foobar backbone.

Classification of Networks

The Foobar Security Officer must classify every network segment that constitutes part of the Foobar infrastructure. A complete list of the classifications of all network segments in the Foobar network and in the Foobar backbone is maintained by the Security Officer. Classifications for existing Foobar network segments are as follows:

- The Foobar User LAN located is classified as *Company Only*.
- The SERVER LAN & backup SERVER LAN are classified as *Confidential*.
- The Foobar Frame-Relay Backbone is classified as *Shared*.
- The Remote sites are classified as *Shared*.
- The SERVER LAN and the Portal Segment are classified as *Shared*.

Classification of Data

Any Foobar user with legitimate access to Foobar data may, with sufficient justification, change the classification of the data. The user may only change the classification of data if there is sufficient, justifiable reason to do so. Users will be held strictly responsible for these decisions.

All newly created data must be classified "Company Only" until it is reclassified by a user, who does so on his or her own prerogative. Users are held solely responsible for any data whose classification they change. Classifications for existing Foobar data are given below:

- Foobar business information (memos, financial documents, planning documents etc) should be classified as "Company Only";
- Foobar customer data (contact details, contracts, billing information etc) should be classified as "Company Only";
- network management data (IP addresses, passwords, configuration files, etc.) should be classified as "Confidential";

- human resources information (employment contracts, salary information, etc.) should be classified "Confidential";
- Published information (pamphlets, performance reports, marketing material, etc.) should be classified "Shared";
- E-mail between Foobar employees should be classified "Foobar Only"; and,
- E-mail between Foobar employees and non-Foobar employees should be regarded as "Unclassified".

Classifications: Roles and Responsibilities

1. It is the responsibility of the user to:
 - know his or her own clearance level and to understand the rights and limitations associated with that clearance;
 - ensure all the data he or she works with is correctly classified;
 - ensure that he or she understands the restrictions associated with the data he or she is working with; and,
 - ensure all the data he or she works with is housed and protected appropriately.
2. It is the responsibility of all system owners and system administrators to:
 - determine the security level of a given user before granting that user access to any system;
 - verify the classification of the equipment they manage; and,
 - verify that the equipment is installed and protected in accordance with its classification.
3. It is the responsibility of each divisional manager to:
 - obtain clearance for employees in his or her divisions;
 - clarify the classification of data on systems under his or her control;
 - clarify the classification of equipment under his or her control and to ensure that those systems are correctly installed; and,
 - ensure all employees in that division understand and implement this policy;
4. It is the responsibility of the Security Officer to:
 - approve all classifications
 - maintain a list of all classifications
 - approve the final layout of the Foobar network and backbone
 - control and manage all trusted points
 - determine the type of cryptographic protection to be used for data in transit

Compliance

1. Any user accessing a data, equipment or a physical location with insufficient clearance can face disciplinary action, dismissal and criminal or civil prosecution.
2. Any user allowing access to a system that he or she controls for someone with insufficient clearance can face disciplinary action, dismissal and criminal or civil prosecution.

3. Any person connecting equipment that is not classified to the network or connecting equipment to an inappropriate part of the network or in an inappropriate location can face disciplinary action, dismissal and criminal or civil prosecution.
4. Any person transmitting data over any network without the appropriate cryptographic protection for that data can face disciplinary action, dismissal and criminal or civil prosecution.
5. Any person changing the classification of data in a way that is reckless, irresponsible or in any damaging to Foobar, their share holders or any of their clients can face disciplinary action, dismissal and criminal or civil prosecution.

Points of Contact and Supplementary Information

1. For a description of the Foobar system of security level classification, users should refer to refer to the Foobar *Information Security Framework* document;
2. The security policy should also provide contact details for the Foobar Security Officer.?

For enquiries regarding the classification of data, equipment, network segments or physical locations or the clearance level of users, interested parties should be directed to contact the Foobar Security Officer.

Conclusion

This has been a long series of articles and a lot of material was covered. Let me try to summarize the important points should remain stuck in your mind:

1. If policies are properly implemented, they can become an effective and efficient part of your information security arsenal. Because policies secure the 'human element', they address an element of your risk profile that is seldom touched by technology.
2. There are no silver bullets in security, and the same is also true for information security policies. Your policies should be written to counter your specific risk profile and should be based on the findings of a security risk analysis exercise.
3. Policies can only be effective in a corporate environment that makes information security a high priority. It may be necessary to make some far-reaching changes to your organizational structure and culture before policies can effectively achieve the organization's security objectives. Foremost among these changes are the designation of responsibility and the commitment of funds.
4. Your policies must be designed 'for the people' and be easy to access, use and understand. To facilitate this, I suggest that the documents be structured in a hierarchical fashion with documents having different levels of detail. Responsibility for the management of this document tree should be specifically assigned.
5. Although the actual content of policy documents should vary radically from organization to organization, there are some fundamental principles that each policy should enforce. These principles have been discussed in this series of articles.

Once your policies have been implemented you will have a structured, formal framework to guide your security strategy and according to which the progress of process can be measured.

Relevant Links

[Introduction to Security Policies, Part One: An Overview of Policies](#)

[Charl van der Walt](#)

[Introduction to Security Policies, Part Two: Creating a Supportive Environment](#)

[Charl van der Walt](#)

[Introduction to Security Policies, Part Three: Structuring Security Policies](#)

[Charl van der Walt](#)

[Privacy Statement](#)

Copyright 2006, SecurityFocus