TYPES OF POLICIES - II

Authorized Access and Usage of Equipment

- This section of the policy addresses who can use the technology governed by the policy, and what it can be used for.
- Remember that an organization’s information systems are the exclusive property of the organization, and users have no particular right of use.
- Each technology and process is provided for business operations.
- Use for any other purpose constitutes misuse of equipment.
- This section defines “fair and responsible use” of equipment and other organizational assets, and should also address key legal issues such as protection of personal information and privacy.

Prohibited Usage of Equipment

— While the policy section details what the issue or technology can be used for, this section outlines what it cannot be used for.

— Unless a particular use is clearly prohibited, the organization cannot penalize its employees for misuse.

— The following can be prohibited: Personal Use, Disruptive use or misuse, criminal use, offensive or harassing materials, and infringement of copyrighted, licensed, or other intellectual property.

Systems Management

— There may be some overlap between an ISSP and a systems-specific policy, but the systems management section of the ISSP policy statement focuses on the user’s relationship to systems management.

— Specific rules from management include regulating the use of e-mail, the storage of materials, authorized monitoring of employees, and the physical and electronic scrutiny of e-mail and other electronic documents.

— It is important that all such responsibilities are designated as belonging to either the systems administrator or the users; otherwise both parties may infer that the responsibility belongs to the other party.

Violations of Policy

- Once guidelines on equipment use have been outlined and responsibilities have been assigned, the individuals to whom the policy applies must understand the penalties and repercussions of violating the policy.
- Violations of policy should carry appropriate, not draconian, penalties.
- This section of the policy statement should contain not only the specifics of the penalties for each category of violation but also instructions on how individuals in the organization can report observed or suspected violations.
- Many individuals feel that powerful individuals in the organization can discriminate, single out, or other wise retaliate against someone who reports violations.
- Allowing anonymous submissions is often the only way to convince individual users to report the unauthorized activities of other, more influential employees.

Policy Review and Modification

- Because any document is only as good as its frequency of review, each policy should contain procedures and a timetable for periodic review.
- As the needs and technologies change in the organization, so must the policies that govern their use.
- This section should contain a specific methodology for the review and modification of the policy, to ensure that users do not begin circumventing it as it grows obsolete.

Limitations of Liability

- The final consideration is a general statement of liability or set of disclaimers
- If an individual employee is caught conducting illegal activities with organizational equipment or assets, management does not want the organization held liable.
- So the policy should state that if employees violate a company policy or any law using company technologies, the company will not protect them, and the company is not liable for its actions.
- It is inferred that such a violation would be without knowledge or authorization by the organization.

Systems-Specific Policy (SysSP)

While issue-specific policies are formalized as written documents, distributed to users, and agreed to in writing, SysSPs are frequently codified as standards and procedures to be used When configuring or maintaining systems

Systems-specific policies fall into two groups:

- Access control lists (ACLs) consist of the access control lists, matrices, and capability tables governing the rights and privileges of a particular user to a particular system.

  An ACL is a list of access rights used by file storage systems, object brokers, or other network communications devices to determine which individuals or groups may access an object that it controls.(Object Brokers are system components that handle message requests between the software components of a system)

- A similar list, which is also associated with users and groups, is called a Capability Table. This specifies which subjects and objects a user or group can access. Capability tables are frequently complex matrices, rather than simple lists or tables.
- Configuration rules: comprise the specific configuration codes entered into security systems to guide the execution of the system when information is passing through it.

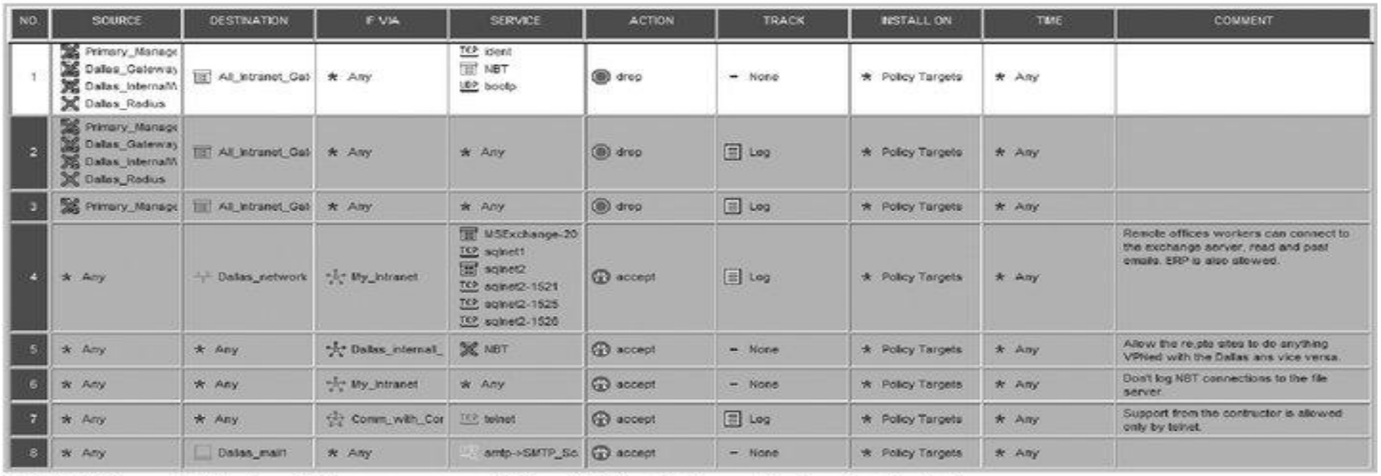
ACL Policies

- ACL's allow configuration to restrict access from anyone and anywhere. Restrictions can be set for a particular user, computer, time, duration-even a particular file.
- ACL's regulate:
  - Who can use the system
  - What authorized users can access
  - When authorized users can access the system
  - Where authorized users can access the system from
  - How authorized users can access the system

- The WHO of ACL access may be determined by an individual person's identity or that person's membership in a group of people with the same access privileges.
- Determining WHAT users are permitted to access can include restrictions on the various attributes of the system resources, such as the type of resources (printers, files, communication devices, or applications), name of the resource, or the location of the resource.
- Access is controlled by adjusting the resource privileges for the person or group to one of Read, Write, Create, Modify, Delete, Compare, or Copy for the specific resource.
- To control WHEN access is allowed, some organizations choose to implement time-of-day and / or day-of-week restrictions for some network or system resources.
- For the control of WHERE resources can be accessed from, many network-connected assets have restrictions placed on them to block remote usage and also have some levels of access that are restricted to locally connected users.
- When these various ACL options are applied cumulatively, the organization has the ability to describe fully how its resources can be used.
- In some systems, these lists of ACL rules are known as Capability tables, user profiles, or user policies. They specify what the user can and cannot do on the resources within that system.

Rule Policies

- Rule policies are more specific to the operation of a system than ACL's
- Many security systems require specific configuration scripts telling the systems what actions to perform on each set of information they process
- Examples of these systems include firewalls, intrusion detection systems, and proxy servers.
- Fig 6.5 shows how network security policy has been implemented by Check Point in a firewall rule set.



NO.	SOURCE	DESTINATION	IF VIA	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
1	Primary_Manage Dallas_Gateway Dallas_InternalM Dallas_Radius	All_intranet_Gat	★ Any	ident NBT bootp	drop	– None	★ Policy Targets	★ Any	
2	Primary_Manage Dallas_Gateway Dallas_InternalM Dallas_Radius	All_intranet_Gat	★ Any	★ Any	drop	Log	★ Policy Targets	★ Any	
3	Primary_Manage	All_intranet_Gat	★ Any	★ Any	drop	Log	★ Policy Targets	★ Any	
4	★ Any	Dallas_network	My_Intranet	MSExchange-20 sqlnet1 sqlnet2 sqlnet2-1521 sqlnet2-1525 sqlnet2-1526	accept	Log	★ Policy Targets	★ Any	Remote offices workers can connect to the exchange server, read and post emails. ERP is also allowed.
5	★ Any	★ Any	Dallas_internal_	NBT	accept	– None	★ Policy Targets	★ Any	Allow the re,ote sites to do anything VPNed with the Dallas ans vice versa.
6	★ Any	★ Any	My_Intranet	★ Any	accept	– None	★ Policy Targets	★ Any	Don't log NBT connections to the file server.
7	★ Any	★ Any	Comm_with_Cor	telnet	accept	Log	★ Policy Targets	★ Any	Support from the contructor is allowed only by telnet.
8	★ Any	Dallas_mail	★ Any	smtp->SMTP_Se	accept	– None	★ Policy Targets	★ Any	

VPN-1/Firewall-1 Policy Editor courtesy of Check Point Software Technologies Ltd.

FIGURE 6-5 Checkpoint VPN-1/Firewall-1 Policy Editor

Policy Management

- Policies are living documents that must be managed and nurtured, and are constantly changing and growing
- Documents must be properly disseminated (Distributed, read, understood, and agreed to) and managed
- Special considerations should be made for organizations undergoing mergers, takeovers, and partnerships
- In order to remain viable, policies must have:
  - an individual responsible for reviews
  - a schedule of reviews
  - a method for making recommendations for reviews
  - a specific effective and revision date

Source : http://elearningatria.files.wordpress.com/2013/10/ise-viii-information-and-network-security-06is835-notes.pdf