# Policy 2

*Dr.Talal Alkharobi*



## Create Appropriate Policy

- Each organization may need different policies.
- Policy templates are useful to examine and to learn from.
- Copying some other organization's policy word for word is not the best way to create your policies

Create Appropriate Policy

3

## Defining What is important

- The first step in creating information security policy is to define which policies are more important for a given organization.
- An organization that delivers information over the Internet may require a disaster recovery plan more than a computer use policy
- The organization's security staff should be able to identify which policies are most relevant and important to an organization.

Defining What is important

4

## Sources of information

- Security staff
- Risk assessment
- System Administration,
- Human Resources, and the
- General counsel's office

Create Appropriate Policy

5

## Defining Acceptable Behavior

- What is acceptable employee behavior will differ based on the culture of the organization.
- Open
  - Allow all employees to surf the Internet without restriction.
  - The organization is relying on the employees and their managers to make sure work is being completed.
- Restricted
  - Place restrictions on which employees are allowed access
  - Load software that restricts access to "unacceptable" web sites.

Create Appropriate Policy

6

## Defining Acceptable Behavior

- The policies for these two organizations may differ significantly.
- In fact, the first organization may decide not to implement an Internet use policy at all.
- Before a security professional begins drafting policy for an organization, the security professional should take some time to learn the culture of the organization and the expectations of the organization with regard to its employees.

Create Appropriate Policy

7

## Identifying Stakeholders

- Policy that is created in a vacuum rarely succeeds.
- Who to includ in the process of developing the policy so that they will gain an understanding of what is expected.
  - Security professionals
  - General counsel
  - Human Resources department
  - System administrators,
  - Users of computer systems,
  - Physical security staff.
- Generally speaking, those who will be affected by the policy

Policy Create Appropriate

8

## Defining Appropriate Outlines

- The development of a policy starts with a good outline.
- There are many sources of good policy outlines available in books, and on the Internet.
- RFC 2196, "The Site Security Handbook, "provides a number of outlines for various policies.

Policy Create Appropriate

9

## Policy Development

- Security should drive the development of security policies but without discarding input from other stockholders
- Begin the process with outline and a draft of each policy section
- Meet stakeholders to discuss there comments (1 or more meetings)
  - Work through the policy section by section.
  - Listen to all comments and allow discussion.
  - Keep in mind, however, that some may not be.
  - In case of inappropriate suggestions, provide the reasons why a risk would be increased or not managed properly.

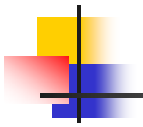
Policy Create Appropriate

10

## Policy Development

- Make sure that the stakeholders understand the reasoning behind the choices of the policy.
- It may be appropriate to meet with stakeholders for the final draft
- When complete, take it to management for approval and implement.

11



# Deploy Policy

- To create policy, you only had to get a small number of people involved.
- To effectively deploy the policy, you need to work with the whole organization.



12

# Gaining Buy-In

- Every department of the organization that is affected by the policy must buy concept behind it.
- This will be easier when you involve stakeholders from all departments in the creation of the policy.
- A message from upper management will go a long way to gain department management buy-in.

Deploy Policy

13

# Education

- Employees who will be affected by a new policy must be educated by the security department.
- This is especially important when it comes to changes that directly affect all users
  - Changing the password policy
  - Changes to authentication systems

Deploy Policy-Education

14

# Changing the password Approach 1

- As of Monday all user passwords
  - Must be eight characters in length
  - Mixture of letters and numbers,
  - Will expire in 30 days
  - All current passwords expire immediately.
- Without education, employee will
  - choose not good (easy) passwords or
  - choose passwords they cannot remember,
    - They will call helpdesk again and again or
    - They will write the password down.

Deploy Policy-Education

15

## Changing the password Approach 2

- Conduct security-awareness training where employees are told about the coming change and why it must be made.
- Teach employees how to pick strong passwords that are easy to remember.
- The help disk can be informed to know what to expect (be ready).
- Security can work with system administrators to phase the change (not every employee needs to change passwords on the same day)

Deploy Policy

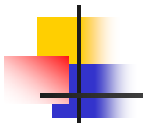
16

## Education

- A better approach would be to conduct security-awareness training where employees are of the coming change and why it must be made.
- At the same time. they can taught pick strong passwords that are easy to remember.
- The can be informed the change so they know what to expect.
- Security can work with system administrators to see if way in the change so not every employee needs to change passwords on the makes for a smoother transition.
- Changes to authentication systems affect the greatest number of employees (all of them!) and must therefore made very carefully.

Deploy Policy

17



# Implementation

- Radical changes to the security can have adverse effects on the organization.
- Gradual, well-planned transitions are much better.
- Security should work with System Administration or other affected departments to make the change as easily as possible.

18

# Use Policy Effectively

- Policy can be used as a club, but it is much more effective when used as an education tool.
- Keep in mind that the vast majority of employees have the best interests of the organization at heart and do try to do their jobs to the best of their abilities.

Use Policy Effectively

19

## New Systems and Projects

- As new systems and projects begin, the existing security policies and design procedures should be followed.
- This allows Security to be a part of the design phase of the project and allows for security requirements to be identified early in the process.
- If a new system will not be able to meet a security requirement, this allows time for the organization to understand the added risk and to provide some other mechanism to manage it.

Use Policy Effectively

20

## Existing Systems and Projects

- As new policies are approved, each existing system should be examined to see if it is in compliance.
- If not, the system should be examined to see if it can be made to comply with the policy.
- Security, system administrators and the department that uses the system need to make the needed changes to the systems.
- This may entail some development changes that cannot implemented immediately (some delay may occur).
- Security need to work with the administrators and other departments to make sure the changes are done in a timely fashion within the budget and design constraints of the system

Use Policy Effectively

21

## Audit

- Many organizations have internal audit department that periodically audit systems for compliance with policy
- Security should approach the audit department about new policies and work with them so that the auditors understand the policy before they have to audit aging.
- Security should explain to audit how the policy was developed and what is expected from that policy.
- Audit should explain to Security how the audits will be done and what they will look for.
- There should also be some agreement on what types of systems will be considered adequate for various policy sections.

Use Policy Effectively

22

## Policy Reviews

- Even a good policy does not last forever.
- Every policy should be reviewed on a regular basis (annually) to make sure it is still relevant for the organization.
- Some procedures, such as an incident response procedure or disaster recovery plan, may require more frequent reviews.
- All of the original stakeholders should be contacted to collect comments on the existing policy (meeting may be required)
- Make the policy adjustments, get approval, and start the education process again.

23

# Assignment

- Develop the needed set of policies for information security in a bank. Enplane first how the security department will start the process and who should be evolved
- Due in 2 weeks from today
- Weight 5% of total mark