MANAGEMENT 514

Information Security Policy in Depth Excerpt

http://www.sans.org/info/66343

Information Security Policy

Learn Policy by Writing, Analyzing and Reviewing Policy Fragments With a Series of Guided Labs and Exercises

Preface

It never ceases to amaze me that you can't take a class in Information Security without being told to do this or that in accordance with "your security policy," but nobody ever explains what the policy is, let alone how to write or evaluate it.

That is why we undertook this research and education project on basic security policy. We hope you will find this module useful and that you will participate in its evolution. Consensus is a powerful tool. We need the ideas and criticisms from the information security community in order to make this, "The Roadmap," a usable and effective policy. Thank you!

Stephen Northcutt

The SMART Approach to Policy and Procedure

This is an excerpt from the course

Management 514: Information Security Policy in Depth

SMART Security Policy and Procedure

- **Specific, Measurable, Achievable, Reasonable, Time Based**
  - Who does the procedure?
  - What is the procedure?
  - When is the procedure done?
  - Where is the procedure done?
  - Why is the procedure done?

How Specific Should Your Security Policy Be?

- There really is no one-size-fits-all answer
- Remember it is usually easier to get a procedure approved or changed
- Largely depends on your organization's policy review turnaround time

General or specific and why?

"Secret shall be applied to information the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe."

General or specific and why?

- "Equipment which is working, but reached the end of its useful life will be made available for purchase by employees. A lottery system will be used to determine who has the opportunity to purchase available equipment.
- All equipment purchases must go through the lottery process. Employees cannot purchase their office computer directly or "reserve" a system. This ensures that all employees have an equal chance of obtaining equipment.
- Finance and Information Technology will determine an appropriate cost for each item.
- All purchases are final. No warranty or support will be provided with any equipment sold. "

How do we make policy measurable?

- Don't use common acronyms as part of your password.
- Don't use common words or reverse spelling of words in part of your password.
- Don't use names of people or places as part of your password.
- Don't use part of your login name in your password.
- Don't use parts of numbers easily remembered such as phone numbers, social security numbers, or street addresses.
- (Note the use of negative voicing)

Less Measurable

"Under circumstances when a password is required, each user will establish a password, known only to him/her. The individual user will be responsible for the confidentiality of the password and for any breaches of security committed via access gained through his/her password or other electronic identifier."

Achievability Part I

"Once the data and application requirements are established, computer security personnel can then evaluate risk and determine methods, processes, equipment, and procedures to mitigate known risks. "

- Application security in general is a tough policy to write. This first policy fragment is not specific, not measurable and probably not achievable.

Achievability Part II

"The computer security personnel, customers, and application developers will work together to provide required and reasonable **access capability** to systems and data both during development and final project implementation while providing the best computer security possible for a reasonable cost."

- This part of the policy fragment, access control, is specific and probably achievable.

Realistic

"All employee use of the Internet shall be for business purposes only."

- Sounds good, but not realistic. The U.S. government used to say something similar, but modified their policy.
- What is a more realistic policy statement?

Time based I

"Account termination: The supervisor of a terminated employee must notify ITCS of the separation on or before the employee's termination date so that account access can be revoked appropriately."

- You will also commonly see account termination policies that say account must be terminated "immediately" after it is not needed, but without supporting procedure this is not achievable.

Time based II

"Backup: Full backups are performed nightly on Monday, Tuesday, Wednesday, Thursday, and Friday. If for maintenance reasons, backups are not performed on Friday, they shall be done on Saturday or Sunday."

SMART Exercise I

"When requested, and for the purpose of performing an audit, consent to access needed will be provided to members of audit.com. ACME hereby provides its consent to allow audit.com to access its networks and/or firewalls to the extent necessary to allow audit.com to perform the scans authorized in this agreement.

ACME shall provide protocols, addressing information, and network connections sufficient for audit.com to utilize the software to perform network scanning."

SMART Exercise II

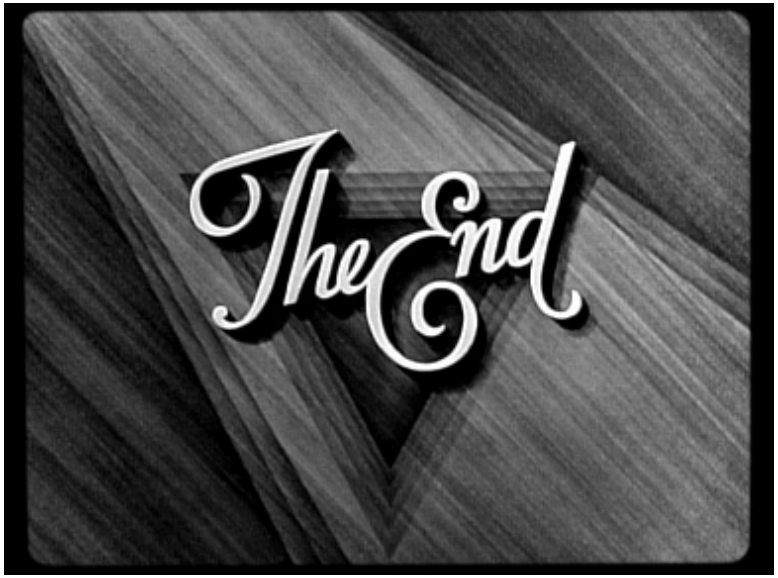
"All ACME encryption shall be done using NIST approved cryptographic modules. Common and recommended ciphers include AES 256, Triple DES and RSA. Symmetric cryptosystem key lengths must be at least 128 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength. ACME's key length requirements shall be reviewed annually as part of the yearly security review and upgraded as technology allows."

SMART Exercise III

"Employees may not install software on ACME computing devices operated within the ACME network. Software requests must first be approved by the requester's manager and then be made to the Information Technology department or Help Desk in writing or via email. Software must be selected from an approved software list, maintained by the Information Technology department, unless no selection on the list meets the requester's need."

MANAGEMENT 514

Information Security Policy In Depth



http://www.sans.org/info/66343