

Information Security Policies

The best approach and the
most common mistakes

ROBERT NIED
CONSULTANCY GROUP

Robert K. Nied, CISSP, CISM, CHS-III

Information Security Policies

Information security is not a technical issue, it is an organizational issue.

An organization's security posture is defined by its policy.

Information Security Policies

- Why do you need policies?
- What policies do you need?
- How do you develop them?

What mistakes should be avoided?

Why do you need security policies?

- **If it's not required it won't happen-** policies guide the organization and ensure consistency.
 - **It's best practice-** following generally accepted approaches is necessary to demonstrate “due diligence” and appropriate governance.
- **If it's not documented it doesn't exist-** informal, de facto and verbal “policies” are not defensible from audit.

What policies do you need?

Understanding the documentation hierarchy:

Policies

Procedures

Instructions



The documentation hierarchy:

Policies define and articulate the organization's commitment to protecting the confidentiality, integrity and availability of information for which it has stewardship.

High Level

Non-Technical

The documentation hierarchy:

Procedures provide guidance on the implementation of the goals and standards articulated in the security policy.

Define specific controls

Detailed

The documentation hierarchy:

Instructions provide a step-by-step roadmap for implementing technical controls in support of security policies and procedures.

Highly granular

Highly technical

Typical Policy Language

“Acme Widget Company will ensure that user workstations are configured in a manner that is consistent with vendor recommendations and best practice standards for information security.”



Typical Procedure Language

“Acme Widget workstations will be configured with the following minimal controls: services and ports that are not specifically required will be disabled,

security settings shall be locked, remote access software shall not be allowed...”

Typical Instruction Language

“Step One: as Administrator, log onto the Vista Services Optimizer.

Step Two: disable the following services: chargen, echo, telnet, ...”



Policies

**Freely disseminated to employees, vendors,
customers, auditors, etc.**



Procedures

Internal documents. May contain proprietary information. Disseminated by work group, as necessary.



Instructions

Highly controlled, sensitive internal documents. Disseminated to staff on a need to know basis only.



Information Security Policies

**Use Best Practice Standards- don't
reinvent the wheel or pull it out of the air.**



Information Security Policies

Follow Best Practice Standards: ISO 27002
(ISO 17799), **ISO 27001**, **NIST 800 Series**,
Compliance Guidelines (HIPAA, GLBA, PCI,
FISMA, NERC, etc.)

BUT...

Information Security Policies

Avoid templates and boiler plate policies.

**Standards-based
does not mean generic**

Information Security Policies

A well defined policy applies the science within the context of the organization.

Do not require controls that you can't sustain, can't fund, or can't enforce

Information Security Policies

Define controls that are reasonable.

“User passwords will be 18 characters in length, use numbers, letters and symbols, must be changed every 10 days and must not be written down.”

Information Security Policies

Define controls that are reasonable.

“User passwords will be 8 characters in length, containing at least one number and one symbol. Passwords must be changed every 30 days.”

Information Security Policies

Define controls that are enforceable.

“Users shall secure portable (laptop) computers to a immovable object, using a cable lock, whenever they are using the device at a customer’s site.”

Information Security Policies

Define controls that are enforceable.

“Portable computers (laptops) will be configured to use hard disc encryption.”

Content

Follow a best practice framework.



Important Policy Areas

- Document Information -document number, issue date, filing instructions, supercedures, etc.
- Overall Security Policy Statement
- Regulatory Compliance
- Organizational Security- roles and responsibilities, personnel security, security training and awareness
- Security of Third Party Access

Important Policy Areas

- Outsourcing- standards for vendors, developers, etc.
- Asset Classification and Control
- Information Classification- classification guidelines, labeling and handling
- Security Incident Response
- Physical and Environmental Security
- Equipment Security- power supplies, secure disposal and re-use
- Protection from Malicious Software and Code
- Network Management

Important Policy Areas

- Removable Media Control
- Exchange of Information- email, IM, etc.
- Access Control
- User Access Management
- User Responsibilities- acceptable use, etc.
- Network Access Control
- Operating System Access Control
- Application Access Control
- Monitoring System and Network Activity
- Mobile Computing

Important Policy Areas

- System Development Life-Cycle
- Cryptographic Controls
- Disaster Recovery
- Business Continuity
- Audit
- Penalties for Non-Compliance
- Policy Update and Review
- Policy Exceptions and Waivers
- Authority

Important Procedures

- Risk Assessment
- SDLC
- Change Management
- Disaster Recovery/Business Continuity
- Audit
- Network Management
- Remote Access/Mobile Computing
- Removable Media
- Encryption

Important Instructions

- Workstation Configuration
- Router Configuration
- Server Configuration
- VPN Configuration
- Wireless Network Configuration
- System by System Recovery
- Incident Response- Forensic Investigation

Dissemination and Socialization

- **Policies must be clearly written, non-technical and easily navigable.**
- **Consider electronic/web-based documents.**
- **Require employees to read and acknowledge where possible.**

AVOID:

- “Policy by the Pound” -don’t expect to cover every technical detail or every eventuality.
- A disjointed series of documents that do not relate in format, tone or content.
- Language that is not consistent across the enterprise- IT, Security, Legal and HR must dovetail.

Questions?



Bob Nied
rnied@niedgroup.com

ROBERT NIED
CONSULTANCY GROUP