PURDUE
UNIVERSITY

CERIAS
Center for Education and Research in Information Assurance and Security

CS62600: Information Security Policy

Prof. Chris Clifton
10 January, 2013

Some material drawn from "A Short Primer for Develpoing Security Policies"
Michele D. Guet, SANS Institute

What is a policy?

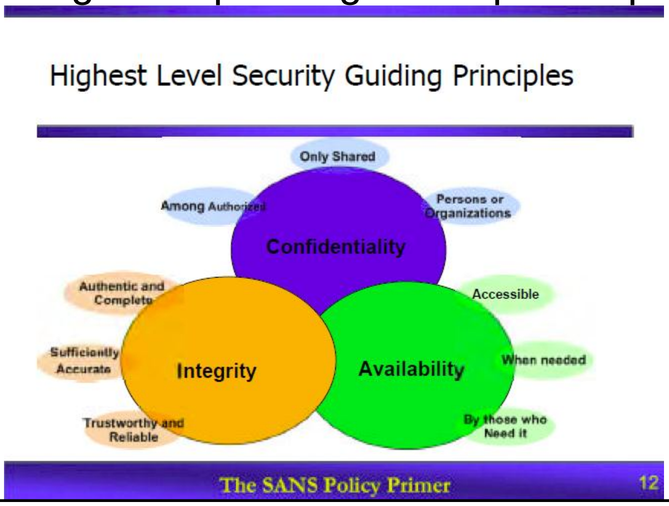
- Statement/plan that is:
  - Formal, Brief, High-level
- Captures
  - General beliefs
  - goals
  - objectives
  - acceptable procedures

Implementing policy

- Standard
  - – Mandatory action/rule
  - – Includes accepted specifications
- Guideline
  - – General statements / recommendations / instructions
  - – May change frequently
  - – Not mandatory
- Position Paper

What goes in a policy?

- Guiding Principles – general philosophy



Highest Level Security Guiding Principles

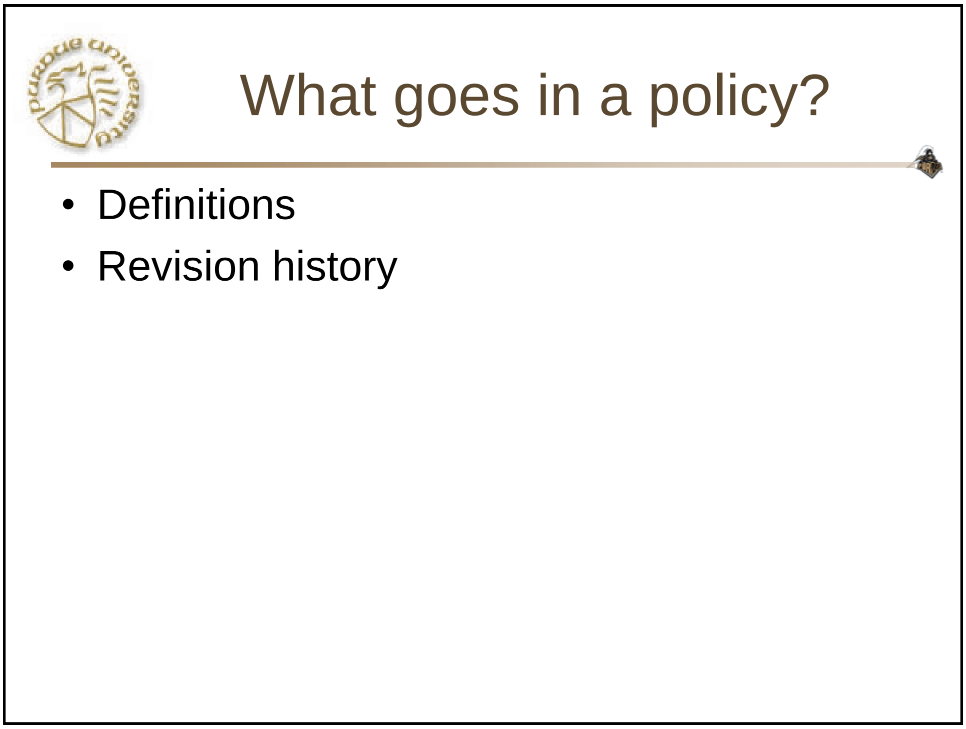
The SANS Policy Primer 12

What goes in a policy?

- Overview
  - – Why? What behaviors governed?
  - – What problem does the policy resolve?
  - – Overall benefit?
- Scope
  - – Who must follow
  - – Who must understand
  - – What technologies/groups included
  - – Exceptions

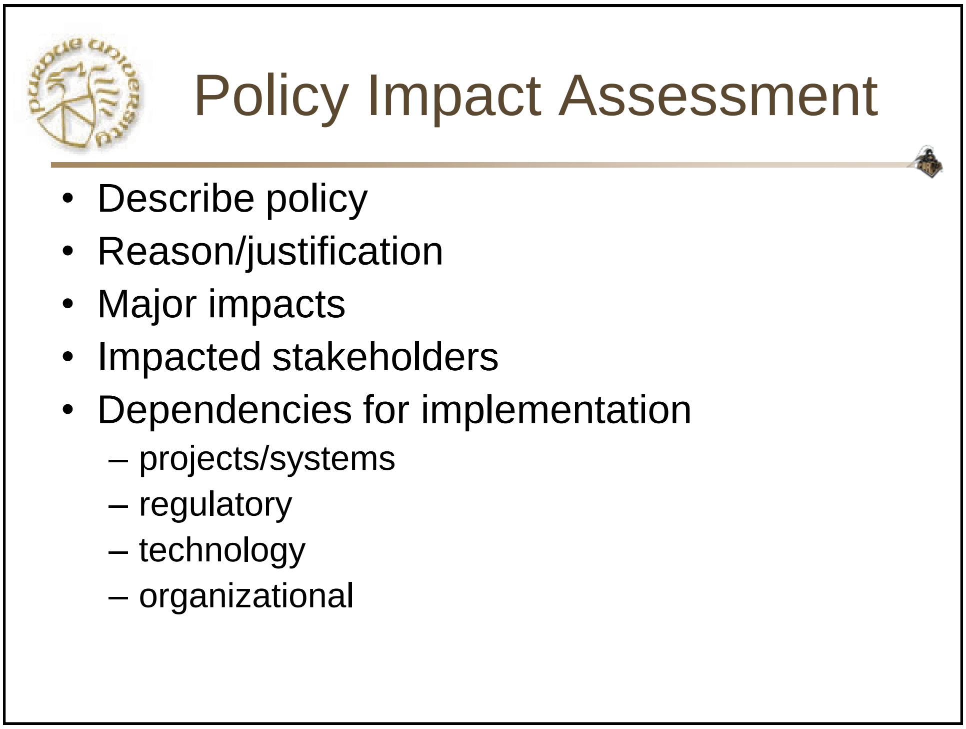
What goes in a policy?

- Policy statements
  - – Behaviors being governed
  - – Responsibilities for compliance
  - – General technical requirements
- References
  - – Standards documentation
  - – Related guidelines
- Enforcement
  - – Penalties



What goes in a policy?

- Definitions
- Revision history



Policy Impact Assessment

- Describe policy
- Reason/justification
- Major impacts
- Impacted stakeholders
- Dependencies for implementation
  - – projects/systems
  - – regulatory
  - – technology
  - – organizational

Procedures

- Defines how to accomplish policy
- Quick reference
- Ensure knowledge codified

ISO/IEC 27002:2005

- security policy
- organization of information security
- asset management
- human resources security
- physical and environmental security
- communications and operations management
- access control
- information systems acquisition, development and maintenance
- information security incident management
- business continuity management
- compliance

Further reading

- SANS Policy Website
  - – http://www.sans.org/resources/policies