

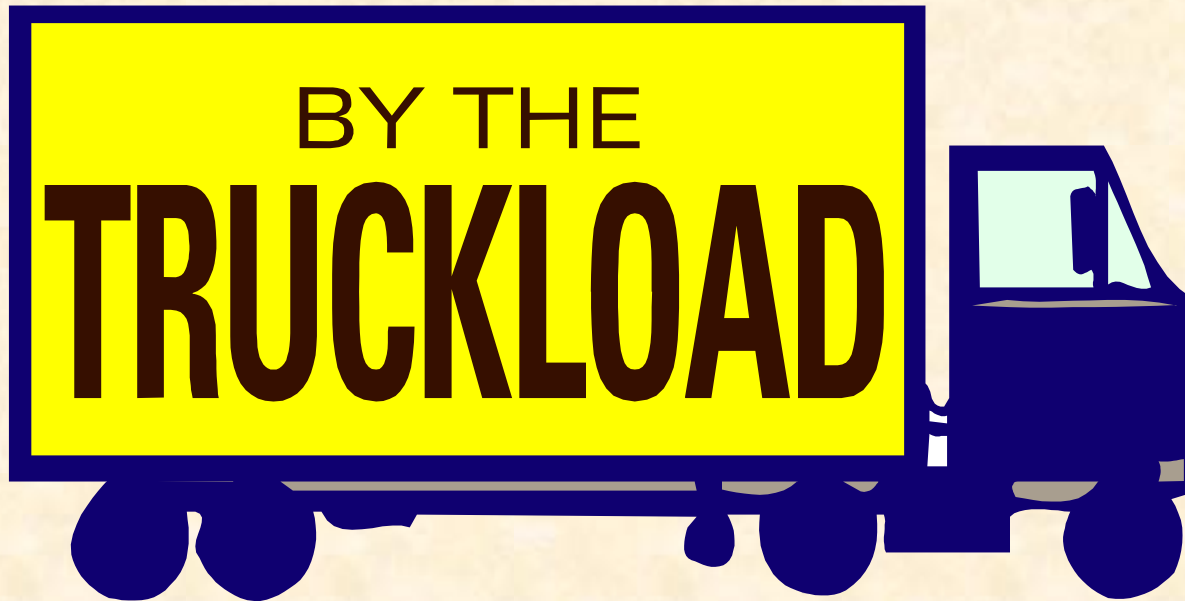
# **Security Policy**



## **Structure, Organization and Presentation**

# Policy ....

---



... Oh Really ?

# What is Policy?



“Policy is management’s directives as to how the organization is to be run”

# Policy Context

- Who are the stakeholders?
- Who are the influences?
- Who is accountable?



# What problem are we trying to solve with Policy?

- Stupidity?
- Technology Problems
- Lack of Training or Awareness
- Poor communication
- Lack of management understanding of what the issues really are...
- Lack of end-users understanding of what the issues really are...

# Purpose of Policy



- As a tool for ...
  - Corporate Governance
  - Corporate Control
  - Controlling Operations

## Corporate Control

- Long Term Goals
  - Align Budget Process
  - Compliance
  - Formalize QA
  - Guide re-engineering
  - Structure Business
  - Shape of Future
- Short Term Goals

# What do People want to know?

---

- Does it apply to ME ?
- How do I know if I'm conforming to policy? ... or not?
- How can I get help and clarification?

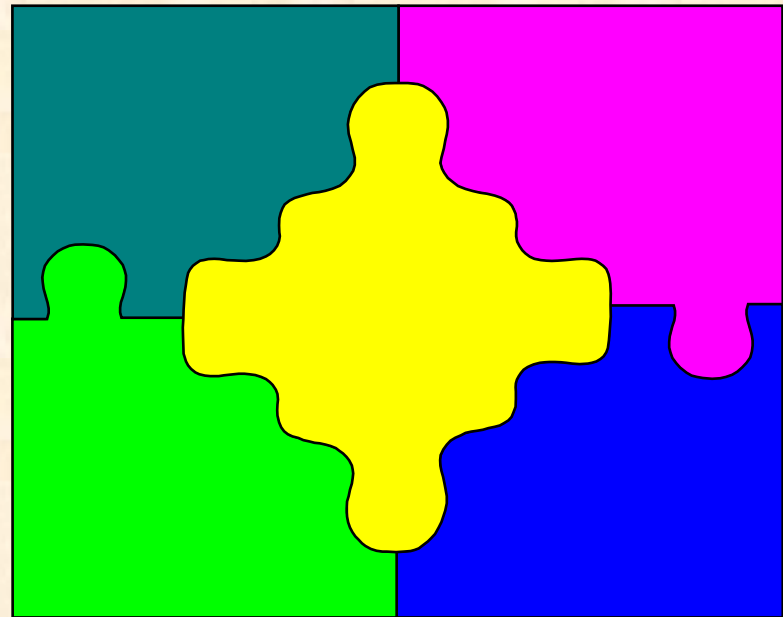
➤ Structure

➤ Index

➤ Search

# What Makes a **GOOD** policy?

- Clear
- Communicable
- Unambiguous
- Concise
- Understandable
- Enforceable
- Followable
- Flexible
- General



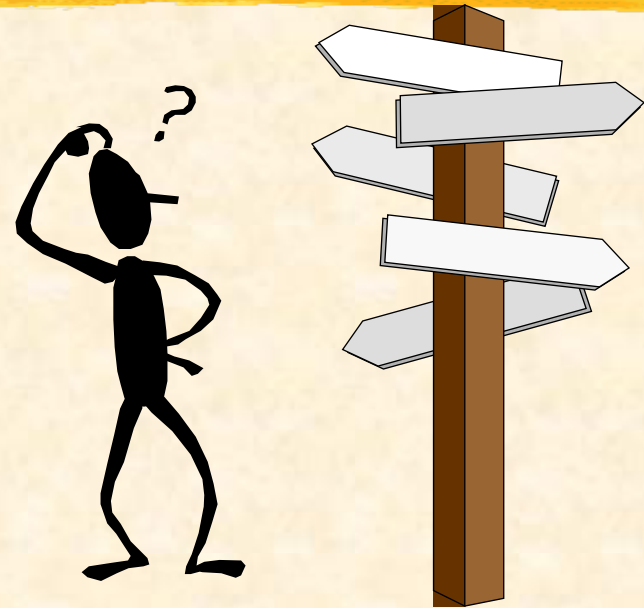
# What Makes a **GOOD** policy?

- Short
- General
- High level
- Widely applicable
- Simple, clear language
- Not tied to ...
  - A particular technology
  - A particular time
  - A particular location
- Understands the Audience

**HAS MANAGEMENT SUPPORT AND COMMITMENT**

# What Makes a **BAD** policy?

- Too specific
- Confusing language
- Confusing Applicability
- No way to measure conformance
- Needs frequent revision
- Lack of management involvement and commitment
- Unclear Audience



- Can't be implemented
- Lack of Structure, Index, Search

# What makes the **WORST** policy?

- The shelf of 3-Ring Binders
- “*You can’t grep dead trees*” - Old UNIX saying
- They sit on the shelf and collect dust
- Mass produced by Management Consulting firms!
  - Get your money’s worth - by the truckload



# The Reality

---

- No-one reads them
- No-one knows where they are
- “Policy” is off in a world of its own

See: “Why people don’t follow Policy” workshop



# How Common “Policies” Rate

## ■ “Good in parts”

- Good phrases
- Attempts at
  - Guidelines
  - Standard

## ■ Good Subtitles:

- Scope, purpose, responsibility, policy

## ■ Overall:

- A collection of thoughts and ideas and admonitions with little structure

## ■ Fails to address many key requirements of a **POLICY**

# How Common “Policies” Fail

- What is this trying to achieve?
- Major Shortcoming:
  - Written manual moved from 3-ring binder to network
- *Responsibility* doesn't answer “me?”
  - Has policy statement
- Confused!
  - Confuses “roles” by talking about password & logoff
- Don't keep going on about passwords!

# How Common “Policies” Fail

- *Responsibility*
  - Must be identified
- *Policy*
  - Collection of ideas with not thought to ....
  - List of admonitions
  - Lots of things that are not policy
- Not consistent – sometimes contradicts itself
- Guidelines are not Policy
- “Reporting problems” is not Policy

# What the Obsession with Passwords?

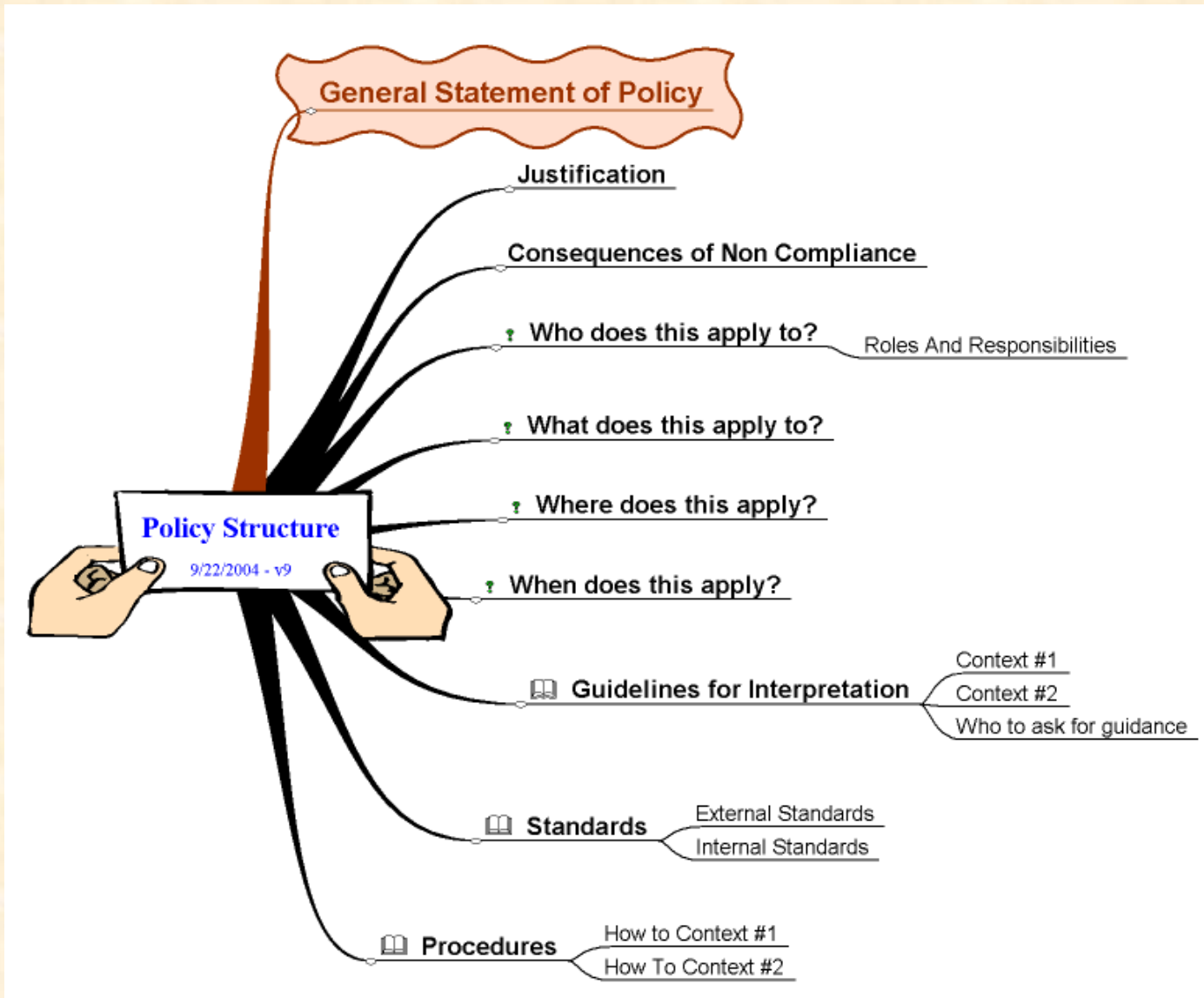
- Easy to specify
- Easy for technical people to write about
- Easy to enforce by technology
- Easy to measure conformance to policy

**This Distorts the Policy Framework**

**Don't Focus on the easy Stuff !!!**



# Policy Structure



# **Example of a GOOD policy**



**"Access to Corporate Information System resources will be restricted to authorized users in accordance with their roles. Users will uniquely identify themselves and be accountable for the actions carried out under this identification"**

# Why is this a **GOOD** policy



- It is ..
  - Simple, non technical English
  - Short
  - Unambiguous
  - Difficult to misinterpret
  - Encompassing
  - Clearly states what is expected and required

# Why is this a **GOOD** policy

- It applies to ...
  - Access to computers
    - | Passwords, tokens, cards, biometrics
  - Access to wiring closets
  - Access to computer room
    - | Turnstiles, gates, combination locks
  - The Parking Lot
  - The Stationary Cupboard

# Why is this a **GOOD** policy

- It applies to ...
  - Everybody using ANY IS resource
- It mentions ...
  - Roles, restrictions, authorization
- It doesn't say ..
  - How they identify themselves

# Why is this a **GOOD** policy

- It doesn't ...
  - Need revising with new technology
  - Go into the details of what technology to use
    - Passwords, LDAP, Biometrics, cards ...
- It ***IS*** a Policy statement
  - Not a guideline
  - Not a standard
  - Not a procedure

# Rule of Thumb

Suppose you have 90 seconds in front of the Board of Directors ...

■ ... once every three months

How often do you want to revise your policy?

How much do you want to have to explain and justify?



# Justification



- People react better if they know the reason!
- Keep it to the point!

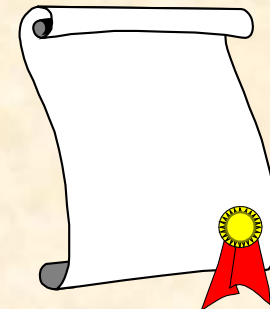
# Consequences of Non Compliance



- Amplification of Justification
- Personal Consequences
  - Legal “Warning”

# A Standard is not a Policy

- Refer to standards, don't state them
  - External Standards
    - Industry standards - ECMA, ANSI, ISO, W3, MIL-STD, Rainbow Books, Common Criteria
    - Government Standards
    - Vendor Standards
  - Internal Standards
- Saves a lot of detail work



# Who What Where When Why

- “Does it apply to me”
- Where do I apply it?
- How do I recognize that I need to apply it?



# Guidelines & Procedures



## Major Failing

- Many People write guidelines when they should be writing policy
- Many People write procedures when they should be writing policy
  
- Many people are too specific and detailed

# Example

Passwords:

- Not Policy:

- Length, Strength, Aging, Re-use

- Is that a standard or a guideline?

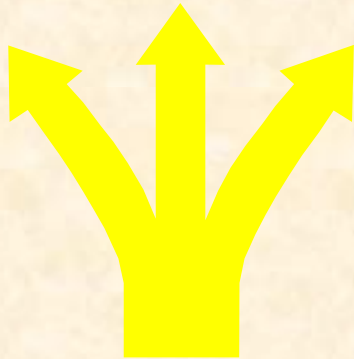
- Limited by technology

Do you understand why?



# Models and Views

---



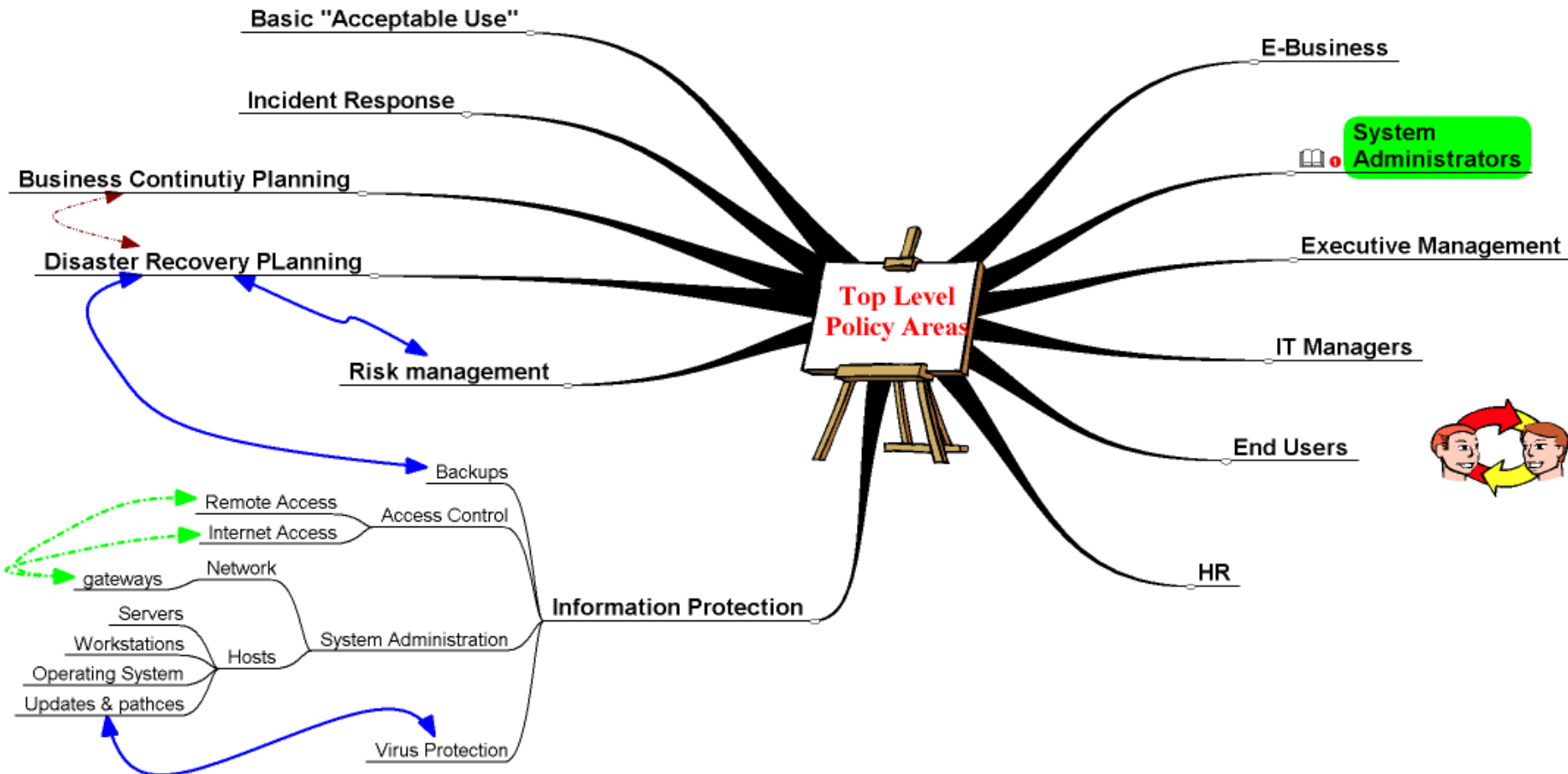
**Top Down  
or  
Bottom Up**



# Policy Division – Static View

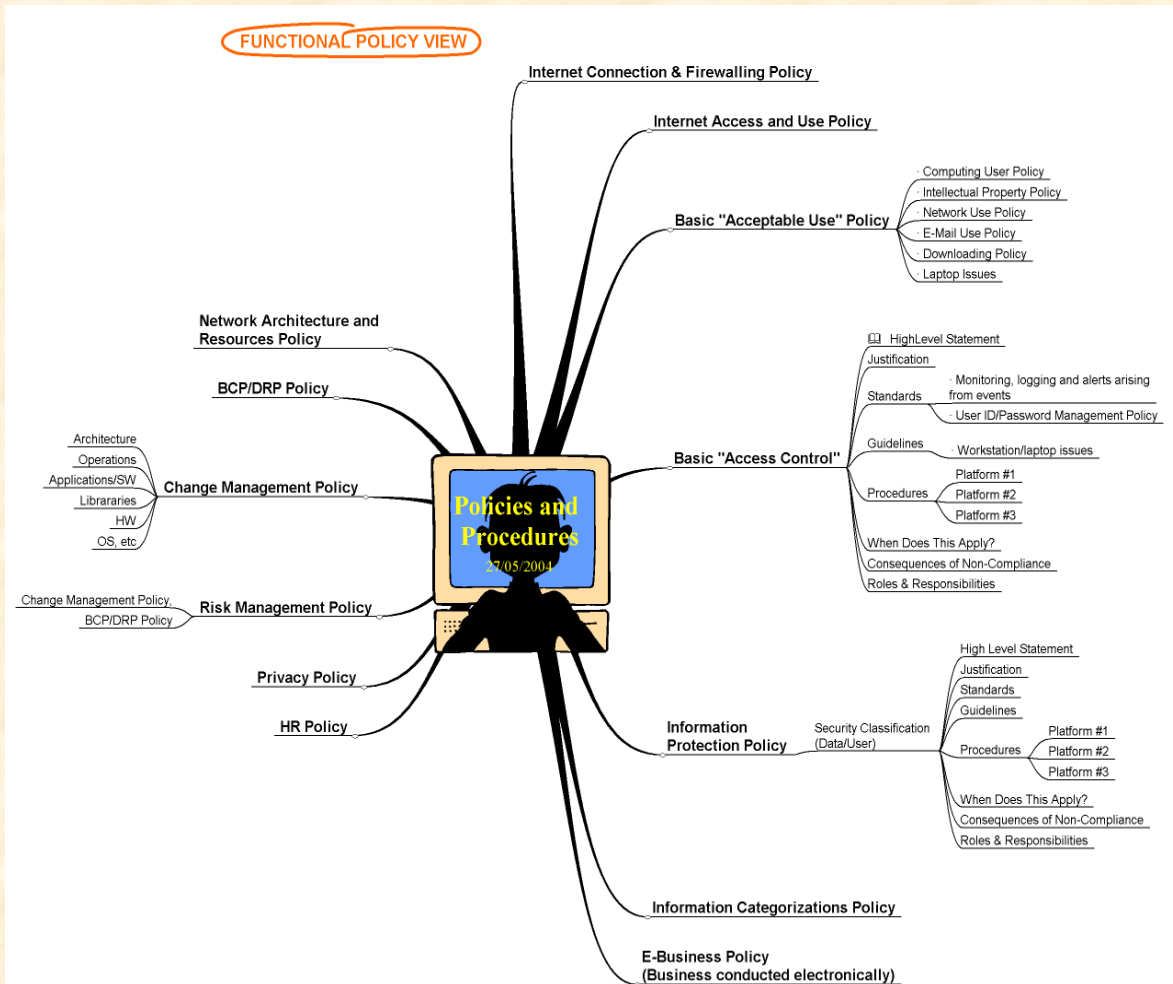


# Top Level Overview



# Functional

- Good for "Random Design"
- Build Links Later



# Use of Intranet



- Hypertext means linkages
- Some static
- Some dynamically generated

Build lots of “low level” pages

Database used to establish links, relevance

User view dynamically generated

# Use of Intranet

- Visual map
  - Drill Down
- Specific Query
  - Search Engine
  - Search by example
  - Search by category
  - Search by topic
  - Search by keyword
- Personalize
  - For job role
  - For individual
- Deal with Questions
  - User BB ?

All this is straight forward with well established and easily available web application tools

# **Issues to Discuss**



**In and out of scope**

# Issues to discuss



- The Policy Lifecycle
- Techniques of Policy Development
- Why People do/don't Follow Policy