



“Developing a Successful Security Policy That Will Survive”

Based on the White Paper on Information Systems Security Best Practices
“Promoting Security Policy Longevity”

© 2008 SAVVIS, Inc.
All trademarks are the property of their respective owners.




MICHAEL METZLER, Ph.D., CISSP, CISM
PAUL HARKER, CISSP, CISM, PMP

“Developing a Security Policy That Will Survive”

Monday, April 28, 2008 – 9:45 am - 12:00 pm



Abstract



The beginning of a sound information system security program is the development of a security policy document, to build the foundation needed to protect the organization's assets and reputation. Often, the policy is written and placed on the shelf to be admired, but is not implemented, enforced or maintained. Not having a security policy today is a legal liability for any corporation, but what about policies that are written, and then never enforced?

This seminar explores the life-cycle and methodology to practice for the successful security policy development, implementation, maintenance, and continued enforcement. Coordination with executive management, information system users, legal counsel, and security professionals are all part of the success model. Specific activities that have been used in the field to establish the security policy as part of the organization's framework for operation are discussed. Attendees will be able to formulate an outline of activity that is necessary to develop security policy, as well as to revive or rework existing policy that has not been implemented or needs to be scaled to match the current operation and environment.

This seminar is based on the SAVVIS Professional Services White Paper titled: “Promoting Security Policy Longevity” and is available upon request.

© 2008 SAVVIS, Inc.

2

Source SAVVIS

White Paper for this session is included in the:
*Spring/Summer 2007
 Computer Security Journal,
 issue Vol XXIII, No. 2/3., pp
 82-96.*

COMPUTER SECURITY JOURNAL
THE JOURNAL NUMBER ONE, SPRING/SUMMER 2007

**NetSec Conference:
 The Roads Less Traveled**
Ever wish that a fantastic conference session would last just a few minutes longer? Ever wonder what other fascinating side roads the speaker would have led you down, if only there was enough time? Some speakers from our NetSec conference take us on these little detours, to smell the roses, see the sites, and learn about data marking and live forensic analysis.—page 1-48

**NetSec CSI Field Notes:
 Case Study Crib Sheets**
New to NetSec this year is our “CSI Field Notes” track, which builds on case studies to feature in-depth discussions and lots of attendee participation. You can’t hide in these sessions, so have a glance at these notes and get ready.—page 49-58

**Forensics:
 Live Response: Collecting Volatile Data**
How to gather crucial but delicate data before it goes up in smoke.—page 59-82

**Management:
 Promoting Security Policy Longevity**
Here’s how to make sure your policy lasts longer than the software it’s written on.—page 82-96

3

Agenda – Lecture/Lab SAVVIS

Monday, April 28, 2008 First Hour 9:45 – 10:45	Lab – Second Hour 11:00 – 12:00
<div style="background-color: #4a7ebb; color: white; padding: 5px; margin-bottom: 5px; display: flex; justify-content: space-between; align-items: center;"> 1 Introduction to Lecture </div> <div style="background-color: #4a7ebb; color: white; padding: 5px; margin-bottom: 5px; display: flex; justify-content: space-between; align-items: center;"> 2 The Secret Sauce </div> <div style="background-color: #4a7ebb; color: white; padding: 5px; margin-bottom: 5px; display: flex; justify-content: space-between; align-items: center;"> 3 Security Policy Life Cycle </div> <div style="background-color: #4a7ebb; color: white; padding: 5px; margin-bottom: 5px; display: flex; justify-content: space-between; align-items: center;"> 4 Expectations </div> <div style="background-color: #4a7ebb; color: white; padding: 5px; margin-bottom: 5px; display: flex; justify-content: space-between; align-items: center;"> 5 Longevity Practices </div> <div style="background-color: #4a7ebb; color: white; padding: 5px; margin-bottom: 5px; display: flex; justify-content: space-between; align-items: center;"> 6 Security Policy Content </div>	<div style="background-color: #4a7ebb; color: white; padding: 5px; margin-bottom: 5px; display: flex; justify-content: space-between; align-items: center;"> 7 The Key Stakeholders </div> <div style="background-color: #4a7ebb; color: white; padding: 5px; margin-bottom: 5px; display: flex; justify-content: space-between; align-items: center;"> 8 Non-Compliance Planning </div> <div style="background-color: #4a7ebb; color: white; padding: 5px; margin-bottom: 5px; display: flex; justify-content: space-between; align-items: center;"> 9 Identifying Hurdles </div> <div style="background-color: #4a7ebb; color: white; padding: 5px; margin-bottom: 5px; display: flex; justify-content: space-between; align-items: center;"> 10 Document Tree </div> <div style="background-color: #4a7ebb; color: white; padding: 5px; margin-bottom: 5px; display: flex; justify-content: space-between; align-items: center;"> 11 Security Awareness and Promotion </div> <div style="background-color: #4a7ebb; color: white; padding: 5px; margin-bottom: 5px; display: flex; justify-content: space-between; align-items: center;"> 12 Wrap - up </div>

© 2008 SAVVIS, Inc. 4

Agenda – Lecture

“Developing a Security Policy That Will Survive” Monday, April 28, 2008 First Hour 9:45 – 10:45

- 1 Introduction to Lecture
- 2 The Secret Sauce
- 3 Security Policy Life Cycle
- 4 Expectations
- 5 Longevity Practices
- 6 Security Policy Content

© 2008 SAVVIS, Inc. 5

Standard Legal Liability Disclaimer --

SECURITY IS NOT FUNNY

Notwithstanding any other provision or understanding to the contrary in any document, SAVVIS makes no representation, warranty, or guarantee that any of the Tasks, Deliverables or other services provided hereunder comply with or satisfy any applicable data security law or industry data security standard. If such Tasks, Deliverables or other services include security services provided by SAVVIS (e.g., scanning or vulnerability testing): (1) Customer acknowledges that SAVVIS may use third party tools for such purposes and that SAVVIS shall have no responsibility whatsoever for the use or effectiveness of such tools; and (2) SAVVIS may not identify all possible incidents or vulnerabilities and SAVVIS expressly disclaims any responsibility for any unidentified or misidentified incidents or vulnerabilities or any and all liability arising out of any Tasks, Deliverables or other services. If SAVVIS provides an assessment, certification, report, or similar work product provided to customer hereunder, such work product is developed and provided in good faith as to its accuracy at the time of inspection or review by SAVVIS, and SAVVIS assumes no liability to Customer or any third party regarding such work product. Full responsibility for any and all regulatory or data security compliance remains the sole and exclusive responsibility of the Customer and not SAVVIS.

© 2008 SAVVIS, Inc. 6

My Standard Paranoid Disclaimer --



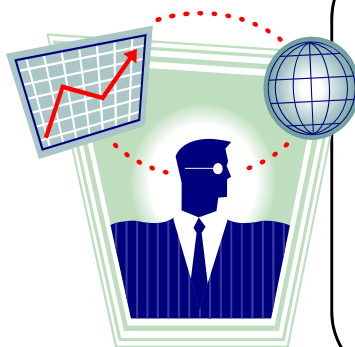
- I am not a Lawyer – just a Security Geek
 - Lots of stuff in Security Policy today has legal implications, review with your legal counsel. If you don't have an attorney – GET ONE.
- I have been doing this stuff for 25 years.
 - Does this mean I know what I am talking about? Maybe...
 - My daughter says it means I am becoming an “old person.”
 - I think it means I think I can get away with presenting at security conferences while not wearing a suit (I hope our marketing department does not read this). **Aloha!**
 - OK, so I have made a few mistakes, and watched other people make a lot of mistakes (this is called “gaining experience”).
 - My goal is to be helpful and share what I learned ...



7

© 2008 SAVVIS, Inc.

Introduction



In 2006, 63 percent of respondents to the *CSI/FBI Computer Crime and Security Survey* indicated that “policy and regulatory compliance” was the most critical issue for their organization in the next two years. This is a growing trend cited in the survey, which has been conducted each year since 1995 by the Computer Security Institute (CSI) and the U.S. Federal Bureau of Investigation (FBI) Computer Intrusion Squad in San Francisco.



8

© 2008 SAVVIS, Inc.

Introduction



- A sound information system security program begins with the development of a security policy document, to build the foundation needed to protect the organization’s assets and reputation.
- This seminar provides an overview of how a team working together contributes to the longevity of a security policy.
- Topics that make up the content of a security policy that has the quality to survive in most organizations are listed, along with a brief description of each major subject to assist in architecting a policy with a focus on security best practices.

Agenda – Lecture



“Developing a Security Policy That Will Survive” Monday, April 28, 2008 First Hour 9:45 – 10:45

- 1 Introduction
- 2 The Secret Sauce
- 3 Security Policy Life Cycle
- 4 Expectations
- 5 Longevity Practices
- 6 Security Policy Content

The Secret Sauce: “Most Important Ingredient”



- Working Together with the people who are stakeholders in the policy:

- Information Security Officer (ISO) or Chief Security Officer (CSO)
- End-User representatives
- System and Network Administrators
- IT Management
- Production Operations Manager
- Corporate Security
- Legal Counsel

“Each member of the team of contributors must be able to view the security program as a business enabler, rather than considering security a limitation.”

This is what makes security policy survive!

The Secret Sauce: Challenges To Conquer



- Security Policy must be consistent with:
 - Existing corporate directives, guidelines and procedures, personnel or HR policies.
 - Relevant federal, state, and local laws as well as regulatory standards in the industry.
 - Engineering System and Network Specifications
- Policy must not present conflicting requirements.
- Authority chartered in the policy must be able to enforce and implement policy as it is written.
- Senior management, legal counsel, and user support is essential.


The Secret Sauce: Challenges To Conquer 



Security Policy must reflect and support every organization's:

- Culture.
- Mission and business focus.
- Customer expectations for confidentiality, integrity, and availability.
- Level of risk tolerance or acceptance of liability.

© 2008 SAVVIS, Inc. 13

The Secret Sauce: Challenges To Conquer 

- **Words: What is in a name?**
 - “**Policy**” may be a reserved word in any organization, one that does not lend itself to the continual maintenance required for information technology security requirements.
 - When this circumstance presents itself, consider other titles of documents that can be a “Security Policy” such as:
 - *Security Standard*
 - *Security Specification*
 - If the word “**Procedures**” is a reserved word, try “**Process**” or “**Guidelines**.”

© 2008 SAVVIS, Inc. 14

The Secret Sauce: Challenges To Conquer



A balance must be struck between:

- Legal requirements and common sense.
- Value of assets and the cost of protecting them as well as the reputation of the organization.
- Locking down all access vs. conducting business and providing service to the customer.

Essential Awareness and Agreement



- Security Awareness Training
 - Discussed later in the presentation
 - Educates all in the organization about the policy
- Acceptable Use Policy
 - Do's and Don'ts for Users
- End-User Agreement
 - Signature of agreement to Acceptable Use Policy

Agenda – Lecture

SAVVIS

“Developing a Security Policy That Will Survive” Monday, April 28, 2008 First Hour 9:45 – 10:45

- 1 Introduction
- 2 The Secret Sauce
- 3 Security Policy Life Cycle
- 4 Expectations
- 5 Longevity Practices
- 6 Security Policy Content


© 2008 SAVVIS, Inc. 17

Life Cycle of the Security Policy

SAVVIS


- Life-cycle and methodology for successful security policy includes elements such as the policy development, implementation, maintenance, and continued enforcement.
- The community that is protected by and those who must support the policy are important contributors.
- Tailor the life cycle to **your** environment.

© 2008 SAVVIS, Inc. 18

Policy Creation and Editing 

- Outline new policy and produce a draft that can be reviewed with selected stakeholders.
- Base new policy on published standards.
- Schedule reviews, request comments.
- Review released policy once every 12 – 24 months.


© 2008 SAVVIS, Inc. 19

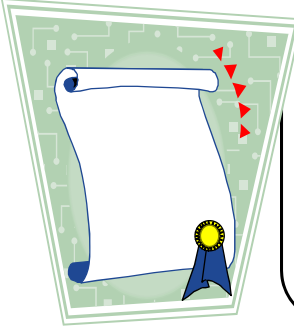
Agenda – Lecture 

“Developing a Security Policy That Will Survive” Monday, April 28, 2008 First Hour 9:45 – 10:45

- 1 Introduction
- 2 The Secret Sauce
- 3 Security Policy Life Cycle
- 4 Expectations
- 5 Longevity Practices
- 6 Security Policy Content

© 2008 SAVVIS, Inc. 20


Expected Compliance to Industry Best Practices and Standards 




Industry Best Practices and Standards:

- Payment Card Industry (PCI) Data Security Standards (DSS).
- ISO-17799, ISO-27001.
- Common Criteria.
- National Institute of Standards and Technology (NIST).

- May not want to use all of the standards, but be sure to use those that your business must comply with (i.e. PCI, HIPAA).
- Use Outline for Security Policy that is “Audit-Friendly” (close to the standard you plan to be compliant with).

 21

© 2008 SAVVIS, Inc.

Expectations for What the Policy Should Provide 

- Clarifies objectives and serves as a guideline in day to day computer activities.
- Declares a plan for how assets are to be protected using specific tools and methodologies.
- Lists measures to protect against identified risks and threats.
- Limits Liability
- Demonstrates Due Diligence and Due Care

© 2008 SAVVIS, Inc. 22

Agenda – Lecture

SAVVIS

“Developing a Security Policy That Will Survive” Monday, April 28, 2008 First Hour 9:45 – 10:45

- 1 Introduction
- 2 The Secret Sauce
- 3 Security Policy Life Cycle
- 4 Expectations
- 5 Longevity Practices
- 6 Security Policy Content

© 2008 SAVVIS, Inc. 23

Examples of Specific Activities Used in the Field

SAVVIS

- Specific activities that have been used in the field to establish the security policy as part of the organization’s framework for operation (part one):
 - Have a meeting with the reviewers about “the policy review meeting.” Managers love this technique (meeting about the meeting), and it is a ploy on my part to remind them to read the policy before the next meeting and provide comments in advance so that I can correlate them and be prepared as well.
 - Meet with the detractors in advance. Their egos need some pampering and you can get them onboard before the review.
 - Providing Donuts and Pizza (and starting rumors that there will be food at the policy review meeting) seems to double the participation for some reason.

© 2008 SAVVIS, Inc. 24

Examples of Specific Activities Used in the Field



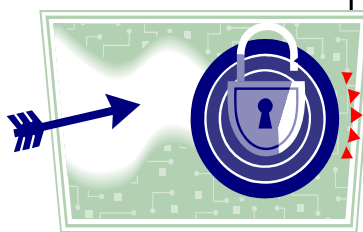
- Specific activities that have been used in the field to establish the security policy as part of the organization’s framework for operation (part two):
 - If there is a corporate security group (you are in a large corporation writing ancillary policy for your specific division) submit your policy draft to corporate security and schedule a review.
 - After the policy has been reviewed and edited, meet with legal counsel to discuss the policy, leave a copy for them to read and make comments, schedule a meeting to discuss those comments.
 - Ask the CEO or President to write a cover letter for the front matter of the policy – write a draft for them if they want.



25

© 2008 SAVVIS, Inc.

Targeting Security Policy Compliance



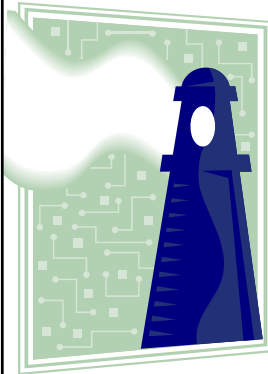
Establish plans for ensuring compliance:

- Plans for periodic monitoring and reviews.
- Procedures and forms for reporting and handling suspected cases of security policy non-compliance.
- Process approval of policy from legal counsel and human resources.
- Guidelines for reporting problems and suspected violations.

26

© 2008 SAVVIS, Inc.

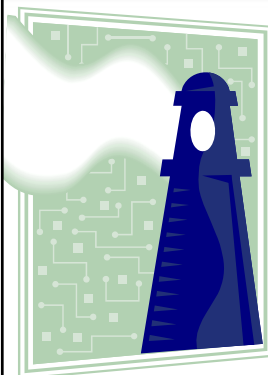
Handling Exceptions – The “Pressure Relief Valve” 



Navigate opposition by offering a Security Policy Non-Compliance Process that provides forms for users to document:

- Business need for the exception requested.
- Manager or Supervisor approval.
- Risk associated with exception.
- Mitigation efforts suggested to minimize risk.
- A get-well plan for compliance or proposal for an alternate security standard.

Handling Exceptions – The “Pressure Relief Valve” 



Navigate opposition by offering a Security Policy Non-Compliance Process that provides forms for users to document:

- Review of exception to identify technology advancements or system improvements that would enable compliance.
- A Non-compliance process “provides a navigational aid” to those who seek exceptions.
- Prepares single-page forms as documentation for audit of non-compliance with policy

Agenda – Lecture

SAVVIS

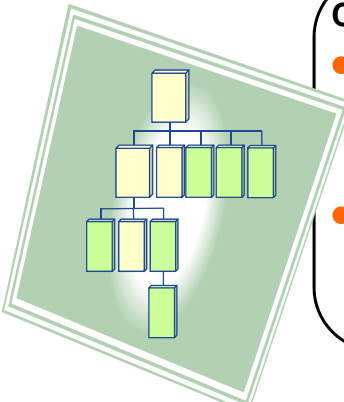
“Developing a Security Policy That Will Survive” Monday, April 28, 2008 First Hour 9:45 – 10:45

- 1 Introduction
- 2 The Secret Sauce
- 3 Security Policy Life Cycle
- 4 Expectations
- 5 Longevity Practices
- 6 Security Policy Content

© 2008 SAVVIS, Inc. 29

Chart Your Course...

SAVVIS

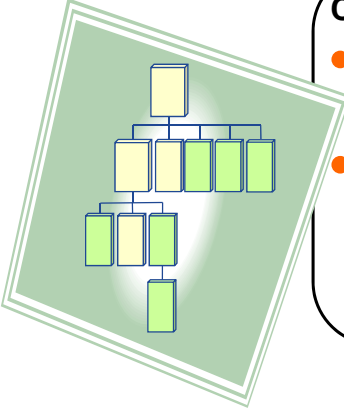



Create a Security Document Tree:

- Use a chart to show the relationship of each security document.
- List percentage of completion, and indicate current status of the document using color.

© 2008 SAVVIS, Inc. 30

Chart Your Course...





Create a Security Document Tree:

- Provide stop-light version of the chart to management
- Use as a map or graphic on an intranet web page to access on-line versions of security documents.

© 2008 SAVVIS, Inc. 31

Information Systems Security Policy




Basic Recommended Structure:

- **Program Policy sets organizational strategic directions, assigns responsibility.**
- **Issue-Specific Policy addresses certain areas of concern such as Internet Access, individual privacy, firewall usage, etc.**
- **System-Specific Policy addresses local standards and procedures for how security is to be implemented on each system.**

© 2008 SAVVIS, Inc. 32

End-User vs. Administrative Security Policy SAVVIS




Everyone
Needs to
Know

Consider Separation:

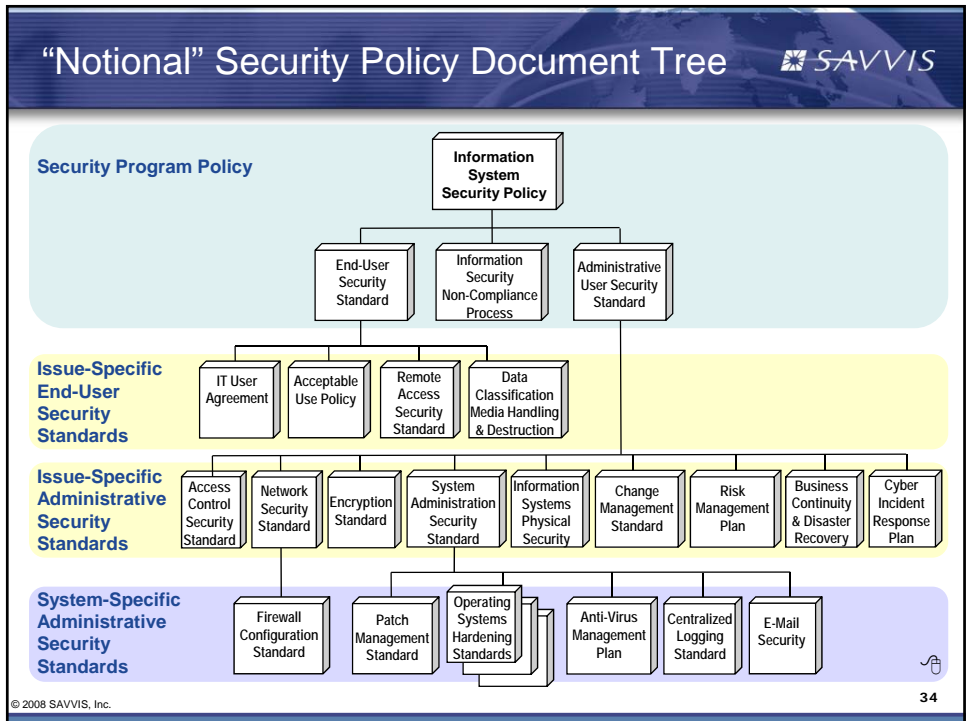
- **End-User Policy focuses on the requirements for all Information Systems Users. Include Acceptable Use Policy.**


- **Administrative User Policy addresses the infrastructure and “behind the scenes” security that End-Users do not really need the full detail on.**




Administrative
Detail

© 2008 SAVVIS, Inc. 33

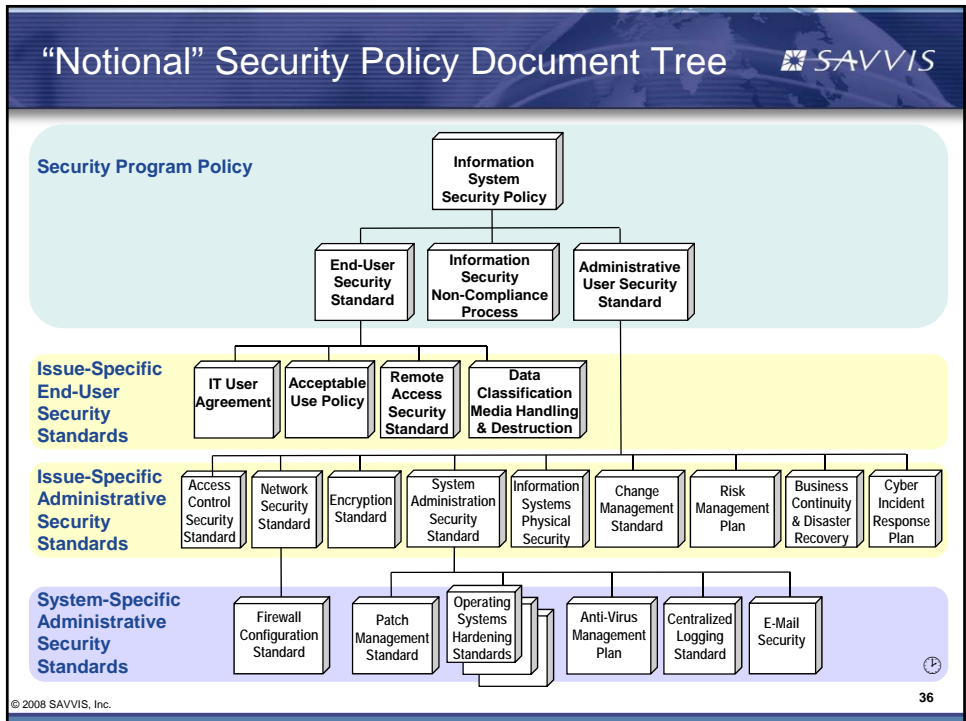


Information Systems Security Program Policy 

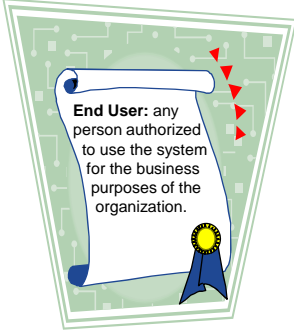



- Purpose and Scope of Information System Security Policies
- Program Promotion & Awareness
- Assignment of Responsibilities and Define Security Roles
- Legal and Regulatory Obligations
- Enforcement of Policy
- Exception Handling Process (reference subordinate Non-Compliance Process)
- Policy Maintenance Requirements
- Security Practices

© 2008 SAVVIS, Inc. 35





End-User Security Policy



- Issue-Specific End User Policy
 - Acceptable Use Policy
 - Remote Access Standard
 - User Agreement
 - Data Classification, Media Handling and Disposal


© 2008 SAVVIS, Inc. 37

End-User Security Policy

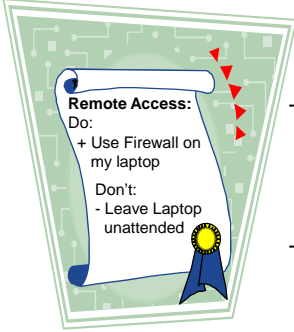


- Acceptable Use Policy
 - Definition for users of the appropriate use of technology owned and operated by the organization.
 - May itemize specific prohibited activities.
 - Specific warnings or cautions related to personal use should be provided, such as personal communications or transactions that may be subject to routine monitoring of systems owned or operated by the enterprise.
 - Normally reviewed by legal, or may be owned by legal services.


© 2008 SAVVIS, Inc. 38

End-User Security Policy 

- Remote Access Security Standard
 - Addresses the usage of any tools (software or hardware) to access the internal network and systems of the organization.
 - Often accompanied by a Remote Access User Agreement that is signed each year by all users who use dial-in access or Virtual Private Networking (VPN).
 - May include specific security standards regarding portable computing devices such as laptop computers and Personal Data Assistants (PDAs).




© 2008 SAVVIS, Inc. 39



End-User Security Policy 

- Data Classification, Media Handling and Disposal:
 - Data Categories with different access control and transmission protection requirements:
 1. Public – *copyrighted, but free to anyone.*
 2. Proprietary or “Official Use Only” – *intellectual property.*
 3. Sensitive, Limited Distribution – *only for access by those with a need to know.*

AVOID using the word “CONFIDENTIAL” as it is a government data classification requiring clearance (just like SECRET and TOP SECRET).
 - Identify Data Retention periods for Specific Data.

© 2008 SAVVIS, Inc. 
40

End-User Security Policy



Removable media handling and data disposal policy subject matter may include:

- Off-Site Backup Protection.
- Mobile Computing Security Policy.
- Data Destruction Standards for each Data Classification.
- Sensitive data encryption on storage and transmission.
- Schedule for performing backups.
- Strategies for tape storage and protection during transit.

Some of the detail on this topic is maintained in Administrative User Security Policy and Operational Procedures.


© 2008 SAVVIS, Inc. 41

End-User Security Policy



- **User Agreement**
 - Signature of agreement to Acceptable Use Policy and Security Policy.
 - Must be signed by all users (both end-users and administrative).
 - Will require scrutiny and review by the organization’s legal counsel.
 - Security best practice standards require the user agreement be signed annually.
 - As with Acceptable Use Policy may be owned by legal services.
 - Ownership or investment by legal counsel in these documents helps to preserve the longevity of the security program.

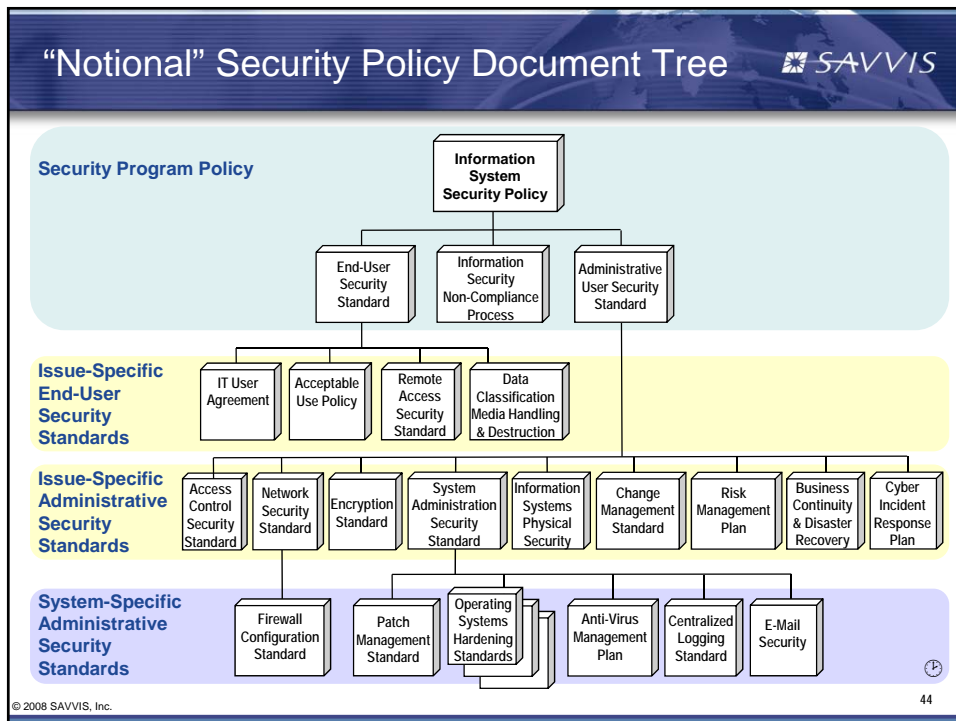
© 2008 SAVVIS, Inc. 42


WARNING 

PREPARE FOR WARP SPEED

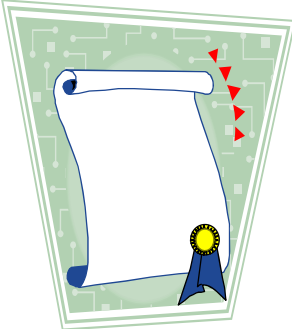
(You can read this stuff in the white paper)

© 2008 SAVVIS, Inc. 43





Information Systems Security Policy 

- Issue-Specific Administrative User Policy
 - Security Awareness Training
 - Access Control
 - Authentication & Password Management
 - Encryption
 - Network Security
 - Desktop and Server Security
 - Software Security
 - Physical Security
 - Incident Response
 - Business Continuity & Disaster Recovery
 - Change Management
 - Secure Review & Audit
 - Risk Management



© 2008 SAVVIS, Inc. 45


Issue-Specific Security Policy 




Security Awareness Training Tips (may include in text of policy):

- Users need to understand why they should be motivated to be involved in Information Assurance.
- Include case studies from the headlines (or those from the movies and books) to show countermeasures known to prevent security breaches.


© 2008 SAVVIS, Inc. 46


Issue-Specific Security Policy 




Security Awareness Training Policy:

- Focus on raising awareness of the:
 - ✓ Value of information assets,
 - ✓ Risks to those assets,
 - ✓ Role users play in protection of assets, and
 - ✓ Impact user actions can have on security posture.
- Highlight A Security Focus for the year.
- Always include Social Engineering as one of the topics (change examples and lesson each year).


© 2008 SAVVIS, Inc.  47

Issue-Specific Security Policy 



Security Awareness Training Policy:

- Allow Training to be video or web-based, 30-45 minutes, and require annual revision.
- Track user completion for audit, require annual completion for each employee.
- Avoid lengthy lectures on consequences of illegal activities, but clearly state consequences that the organization and the individual may face.

© 2008 SAVVIS, Inc.  48

Administrative User Security Policy



- **Data Security**

- Access control (who decides who can access what --for what purpose).
 - Authorization
 - Authentication
 - File Access Structure
- Password Management



- **Encryption Policy**

- Accepted algorithms to protect sensitive data.
- Key strength required for each algorithm.
- Policy for Public Key Infrastructure (PKI) if in use.

© 2008 SAVVIS, Inc.

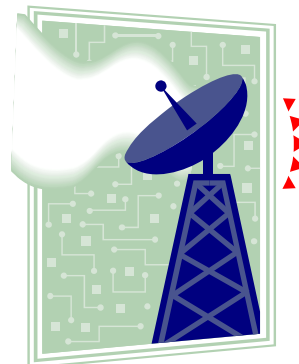
49

Administrative User Security Policy



- **Network Security**

- Firewalls and Boundary Protection for Internet and Extranet Connections
- Intranet Protection between Security Enclaves
- Intrusion Detection
- Remote Access
- Network Security Management
- Wireless Laptop Connectivity, Portable Computing use on Local Area Network (LAN)
- Telecommunications
- Security Policy for LAN Wiring Closets
- Wide Area Network (WAN) Facility
- Wireless LAN (WLAN) Security



© 2008 SAVVIS, Inc.

50

Issue-Specific Security Policy



- **Intrusion Detection**

- Host-based Sensors.
- Network-based Sensors.
- Monitoring, auditing, and logging.
 - Use of tools
 - Responsibility
 - Frequency
- Management of false-positive reporting.
- Raising employee and management awareness of attack threat.
- Support for forensic and Incident response activity.

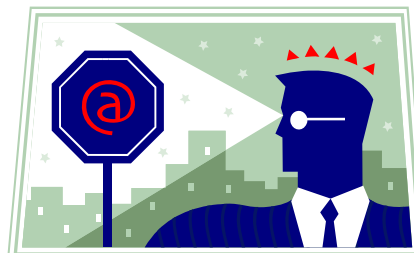


Administrative User Security Policy



- **Desktop and Server Security**

- Security Standards for System Administrators
- File Integrity Checking and Configuration Control
- System, Administrator, or 'root' Accounts
- Account Management and Termination

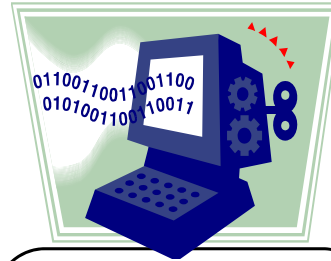


Administrative User Security Policy



- **Software Security**

- Virus prevention and detection.
- Downloading of software.
- Software licenses.
- Software acquisition policy.
- Secure coding practice.
- System backups.
 - Sensitive data must always be encrypted
 - Schedule for performing backups.
 - Strategies for tape storage.
 - Protection during transit



Secure Coding Practices include:

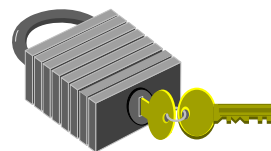
- Conducting code review on software developed in-house.
- Web page security to prevent SQL injection attacks and other character insertion methods.
- Encryption or hashing of all passwords.
- Encryption of sensitive data transmission and storage.
- Prevention of back doors.

Issue-Specific Security Policy



- **Physical Security**

- Measures that augment the physical security for the company or organization (badges, guards, dogs, fences, etc.).
- Protection of computing resources.
- Entry and exit procedures for data center or server room.
- Controls on copy machines.
- Controlled removal of equipment.
- Use of password protected screen savers.
- Laptop theft reduction (cable locks).



Issue-Specific Security Policy 



Incident Response Plan:

- Plan and prepare a process of steps for how the organization will react when a problem occurs.
- Have policies in place to enforce when problem is internal.
- Make contacts with appropriate law enforcement agencies who handle computer crime, investigations and prosecution.
- Incident Response Planning is critical, there are many resources to help the team get started.

© 2008 SAVVIS, Inc. 55

Issue-Specific Security Policy 

- **Business Continuity & Disaster Recovery**
 - Disasters of any kind may cause an internal service disruption, infrastructure failure, facility failure, or a region-wide outage.
 - Minimizing disruption from these events includes protective measures to reduce event impact, business continuity measures to ensure critical operations remain functional, and a strategy for business recovery to restore the damaged resource to its pre-disaster status or service level.
 - Normally these plans are only developed because of fiduciary duties to shareholders.
 - Statistics show that 93% of businesses that suffer a disaster and lose their data center for 10 days or more, filed for bankruptcy within 12 months. (U.S. National Archives and Records Administration).



© 2008 SAVVIS, Inc. 56

Issue-Specific Security Policy



• Change Management

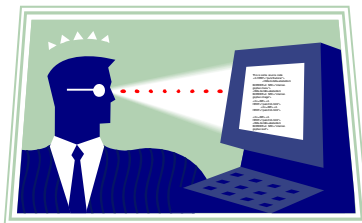
- Change Management provides for the continued review of networks, systems, applications, appliances, and configurations which may impact security and/or operations, while ensuring that changes have been reviewed and approved by management.
- Must be documented as a thorough process, as it is **critical to help ensure the security and operations of all IT infrastructures.**
- Requirements should include:
 - Documentation of all changes to systems and networks.
 - Verification that back-out procedures exist.
 - Backups are made before proceeding with the migration or change activities.

Issue-Specific Security Policy



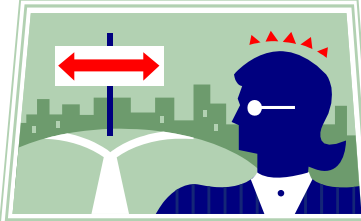
• Secure Review & Audit

- Development and review of a Risk Management Plan.
- Security Monitoring of log files and daily reviews.
- Definition of Internal Audit Testing Methodology.
- External Vulnerability Assessments and Penetration Testing on a quarterly basis and after each change or upgrades are made to any system, application or network component.
- Secure Code Review of any in-house developed software, web pages, or patches.

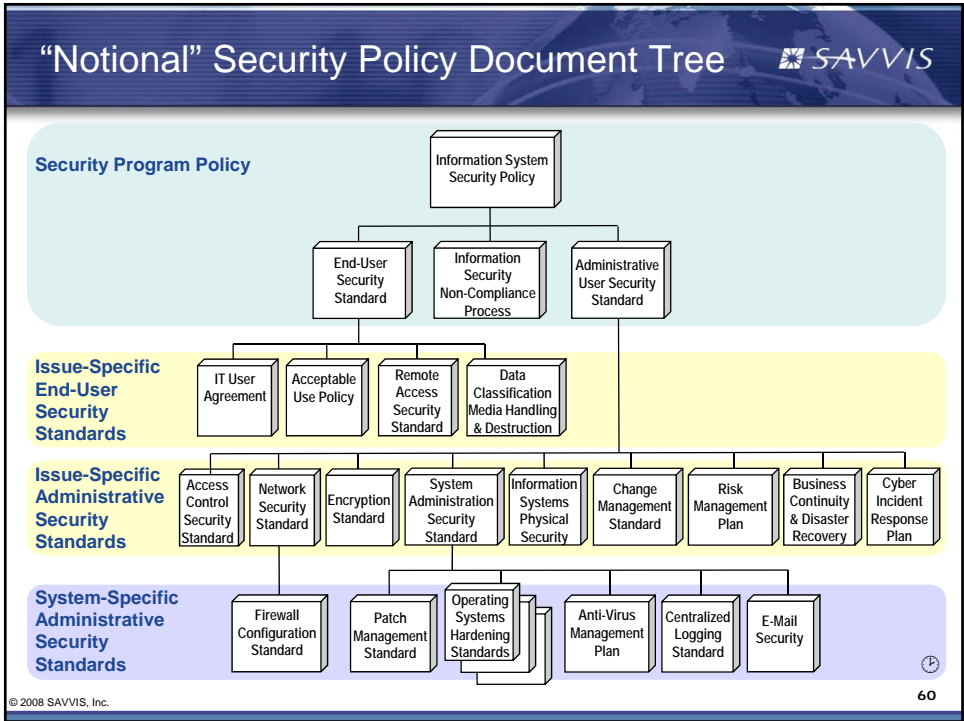



Issue-Specific Security Policy

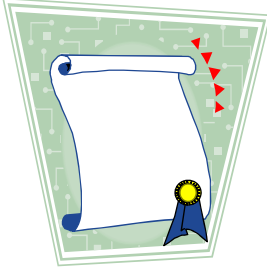
- **Risk Management Plan**
 - Assists the organization in producing a risk assessment with a high-level summary of risks and guidelines for acquiring, deploying, and operating risk mitigation controls.
 - The security policy should require that a risk assessment be performed each year, as threats and potential exploits of existing systems are subject to change.
 - The policy should also suggest a Business Impact Analysis as well.



© 2008 SAVVIS, Inc. 59





Information Systems Security Policy 



- **System-Specific Policy**
 - Operational Security Procedures
 - Hardening Procedures
 - O/S
 - Applications
 - Electronic Mail
 - Security Monitoring
 - Centralized Logging
 - Security Patch Management
 - System Development Life Cycle (SDLC)

© 2008 SAVVIS, Inc. 61

System-Specific Security Policy 



- **Hardening Standards**
 - Develop for each operating system
 - Especially important for Microsoft Windows servers.
 - Hardening standards may include:
 - Removal of unused scripts, drivers, features, subsystems, file systems, and unnecessary web servers
 - Applying security patches
 - Limiting each server to only one function or application (e.g., web servers, database servers, security applications, and DNS should be implemented on separate servers)
 - Implementing automated audit trails for server functions
 - Changing default passwords


© 2008 SAVVIS, Inc. 62

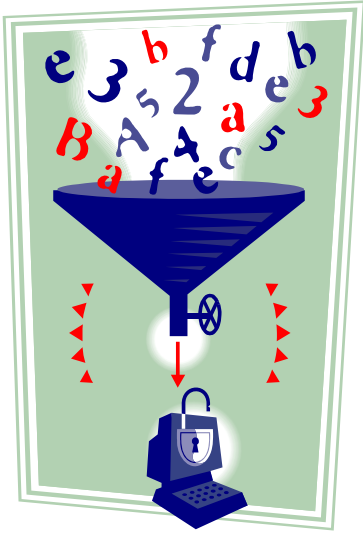
System-Specific Security Policy 

- Patch Management
 - Ensure that security patches for systems and components are applied within a reasonable amount of time as they become available.
 - A configuration database must be maintained to record all managed system states, and all patches available to apply to those systems.
 - Include requirements for all patches to be tested in a test network or environment prior to deployment in any production environment.



© 2008 SAVVIS, Inc. 63

System-Specific Security Policy 



- Centralized Logging
 - Require an implementation that provides a single point for observation and notification of network security events throughout the organization.
 - Provides data for audit purposes and computer forensic investigations to support incident response.
 - Require an independent log data collection and archival system on separate servers.

© 2008 SAVVIS, Inc. 64

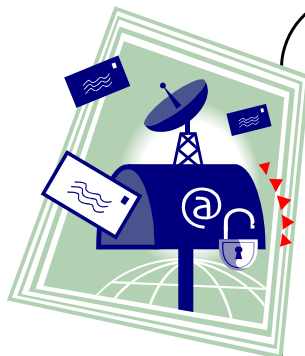
System-Specific Security Policy



E-mail Security Policy Considerations:

- List permissible uses of electronic mail.
- Set user expectations of privacy, may be able to claim that all e-mail is company property and may be monitored at any time.
- Establish monitoring frequency and purpose.
- Limit examination or disclosure of messaging for any purpose other than authorized security investigations to prohibit random monitoring for personal reasons, and to control the dissemination of sensitive or personal information.

System-Specific Security Policy



E-mail Security Policy Considerations:

- Internal E-mail has multiple security issues.
 - Content restrictions.
 - Transmission of confidential data.
 - Privacy expectations.
 - E-mail belongs to the organization.
 - Must be handled legally as documents.
- Handling of e-mail attachments.
- Management and retention of e-mail messages.

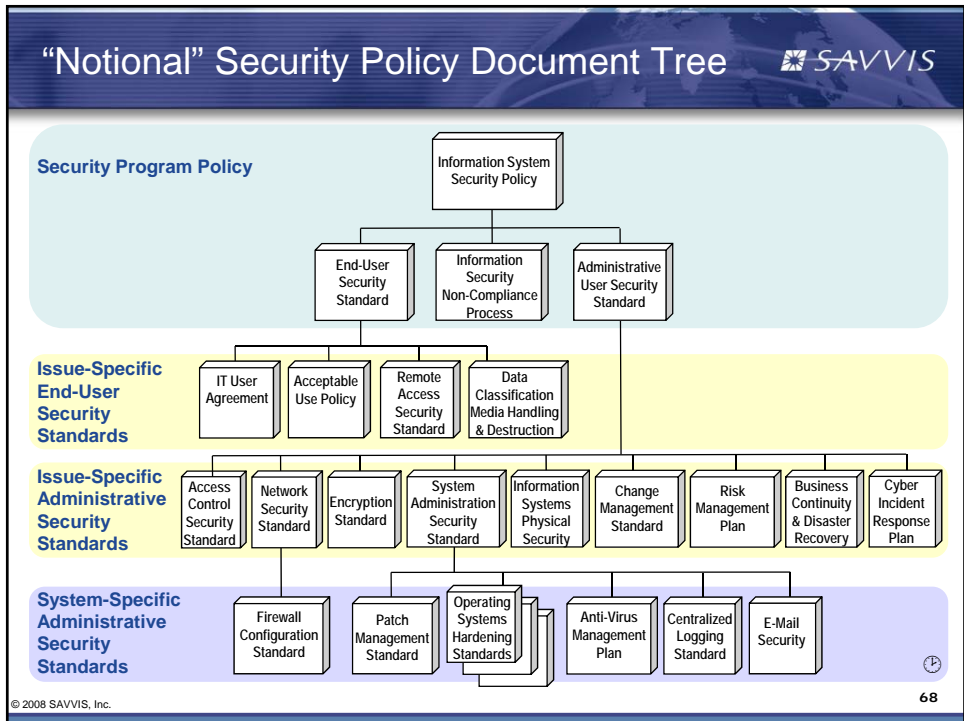
When choosing approach, consider:


- What is truly enforceable?
- What are liabilities and employee rights?

System-Specific Security Policy

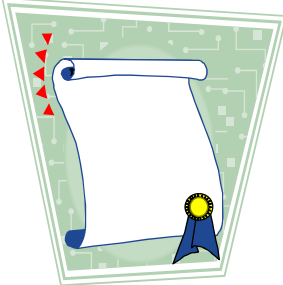
- **System Development Life Cycle (SDLC)**
 - Establishes guidelines for managing the acquisition and development of systems and applications.
 - Includes multiple stages from establishing feasibility, to the execution of post implementation reviews.
 - Guides the evolution of new systems with a security focus to achieve compliance with applicable state and federal laws as well as regulatory and required industry security standards such as PCI DSS.

© 2008 SAVVIS, Inc. 67



Information Systems Security Program Policy 

- Highlights on some Program Policy:
 - Program Promotion & Awareness
 - Enforcement of Policy




© 2008 SAVVIS, Inc. 69

Information Systems Security Program 


- Security Awareness Promotion
 - Use Posters:
 - http://www.us-cert.gov/reading_room/distributable.html#work
 - Add info on your team and policy.
 - Put Security Awareness Training materials and a copy of your Security Policy (PDF file or HTML) along with contact information on your internal IT security Web Page.





© 2008 SAVVIS, Inc. 70

Information Systems Security Policy 

- Policy Enforcement
 - Establish plans for ensuring compliance.
 - Plans for periodic monitoring and reviews.
 - Procedures and Forms for reporting and handling suspected cases of non-compliance.
 - Involve Legal Counsel and Human Resources for Process Approval
 - Guidelines for reporting problems and suspected violations.




© 2008 SAVVIS, Inc.  71

Summary 

- Involve stakeholders in policy development
- Evaluate how policy will be enforced
- Prepare for Incident Response
- Provide Security Awareness Training
- Test and Audit Controls in Place
- Audit Compliance and Conduct Penetration Studies

© 2008 SAVVIS, Inc. 72


Questions? 

e-mail us and ask us for the
White Paper at:

michael.metzler@savvis.net 

 paul.harker@savvis.net

© 2008 SAVVIS, Inc.





**“Developing a Successful Security
Policy That Will Survive”**

Part 2 - Lab

Based on the White Paper on Information Systems Security Best Practices
“Promoting Security Policy Longevity”

© 2008 SAVVIS, Inc.
All trademarks are the property of their respective owners.

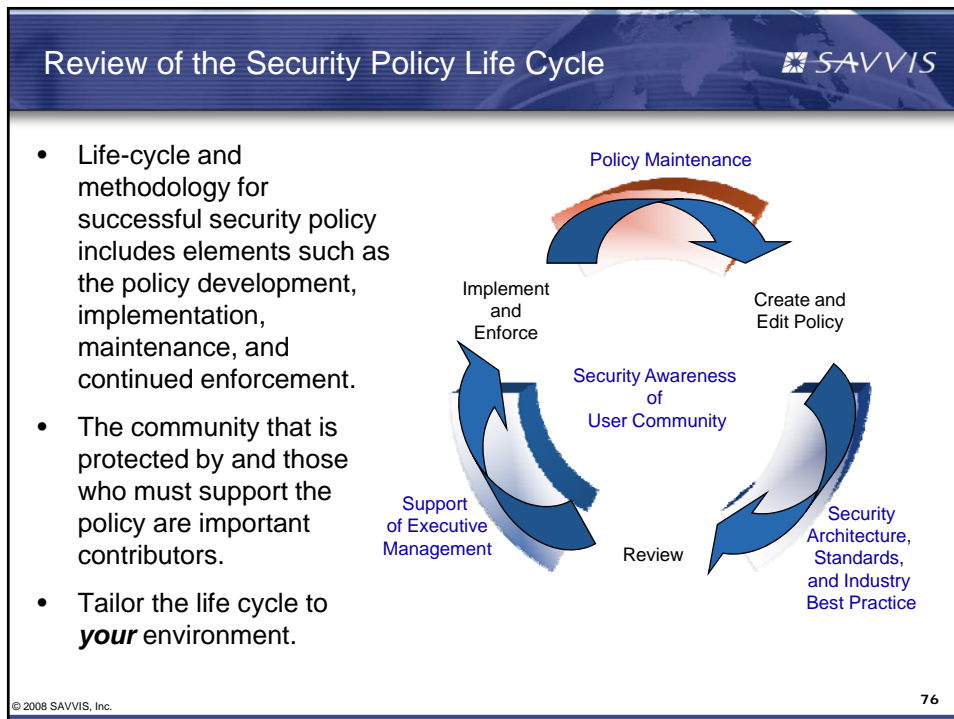
 MICHAEL METZLER, Ph.D., CISSP, CISM
PAUL HARKER, CISSP, CISM, PMP
“Developing a Security Policy That Will Survive”
Monday, April 28, 2008 – 9:45 am - 12:00 pm 

Agenda – Lecture/Lab

SAVVIS

Monday, April 28, 2008 First Hour 9:45 – 10:45	Lab – Second Hour 11:00 – 12:00
1 Introduction to Lecture	7 The Key Stakeholders
2 The Secret Sauce	8 Non-Compliance Planning
3 Security Policy Life Cycle	9 Identifying Hurdles
4 Expectations	10 Document Tree
5 Longevity Practices	11 Security Awareness and Promotion
6 Security Policy Content	12 Wrap - up

© 2008 SAVVIS, Inc. 75



Agenda – Lab

“Developing a Security Policy That Will Survive” Monday, April 28, 2008 Second Hour 11:00 – 12:00

- 7 → The Key Stakeholders – 5 Minute Lab
- 8 → Non-Compliance Planning
- 9 → Identifying Hurdles
- 10 → Document Tree
- 11 → Security Awareness and Promotion
- 12 → Wrap - up

© 2008 SAVVIS, Inc. 77

The Secret Sauce: “Most Important Ingredient”

- Working Together with the people who are stakeholders in the policy:
 - Information Security Officer (ISO) or Chief Security Officer (CSO)
 - End-User representatives
 - System and Network Administrators
 - IT Management
 - Production Operations Manager
 - Corporate Security
 - Legal Counsel

This is what makes security policy survive!

“Each member of the team of contributors must be able to view the security program as a business enabler, rather than considering security a limitation.”

© 2008 SAVVIS, Inc. 78

LAB WORKSHEET

The Key Stakeholders: Create a Checklist

Take 5 Minutes to make a list of Names and / or Title of Each Person or Group

- Who is the author of the Security Policy and Standards?
- Who will need to approve the documents before they are released? CIO? Legal?
- Who will the policy affect the most? Are the End-Users represented?
- Are there Administrative Users (SysAdmins) who can work on the policy?
- Anyone else needed to support the policy implementation?
- Number the list in the order they should be involved in the review of the document.

Agenda – Lab

SAVVIS

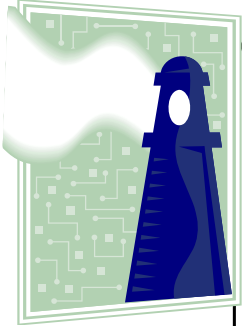
“Developing a Security Policy That Will Survive” Monday, April 28, 2008 Second Hour 11:00 – 12:00

- 7 → The Key Stakeholders
- 8 → Non-Compliance Planning
10 Minute Lab
- 9 → Identifying Hurdles
- 10 → Document Tree
- 11 → Security Awareness and Promotion
- 12 → Wrap - up

© 2008 SAVVIS, Inc. 80

Handling Exceptions – The “Pressure Relief Valve”

SAVVIS



Navigate opposition by offering a Security Policy Non-Compliance Process that provides forms for users to document:

- Business need for the exception requested.
- Manager or Supervisor approval.
- Risk associated with exception.
- Mitigation efforts suggested to minimize risk.
- A get-well plan for compliance or proposal for an alternate security standard.
- Review of exception to identify technology advancements or system improvements that would enable compliance.

- A Non-compliance process “provides a navigational aid” to those who seek exceptions.
- Prepares documentation for audit of non-compliance with policy

© 2008 SAVVIS, Inc. 81

LAB WORKSHEET

Non-Compliance Planning: Create a Checklist

*Take 10 Minutes to make a list of sections in the One-Page Forms Needed for a Non-Compliance Process – **or** – plan an outline of the steps to be used for processing requests.*

- Policy Statements that are in Non-Compliance need to be listed and Non-Compliance should be explained.
- Justification for Exception Request needs to be stated.
- Risk of the Non-Compliance should be identified (assistance/oversight for this task may be required).
- Existing or Proposed Mitigation of Risk, if any exists, should be noted.
- Who in the organization or company will approve the variance/exception?
- What time limits are placed before review? Six Months? 12 Months?

Agenda – Lab

SAVVIS

“Developing a Security Policy That Will Survive” Monday, April 28, 2008 Second Hour 11:00 – 12:00

- 7 → The Key Stakeholders
- 8 → Non-Compliance Planning
- 9 → Identifying Hurdles – 10 Minute Lab
- 10 → Document Tree
- 11 → Security Awareness and Promotion
- 12 → Wrap - up

© 2008 SAVVIS, Inc. 83

The Secret Sauce: Challenges To Conquer

SAVVIS




Security Policy must reflect and support every organization's:

- Culture.
- Mission and business focus.
- Customer expectations for confidentiality, integrity, and availability.
- Level of risk tolerance or acceptance of liability.

A balance must be struck between:

- Legal requirements and common sense.
- Value of assets and the cost of protecting them as well as the reputation of the organization.
- Locking down all access vs. conducting business and providing service to the customer.



© 2008 SAVVIS, Inc. 84

LAB WORKSHEET

Identifying Hurdles: Create a Checklist

Take 5 Minutes to make a list of challenges you are facing that are holding you back from creating and implementing the policy you want or your organization really needs!

- (This Page - 5 Minutes) What are the top five challenges facing you or your organization that prevent you from having a top-quality best-practices security policy?
- (Next Page - 5 Minutes) Brainstorm 2-3 actions you plan to take to resolve each challenge.
- Keep in mind the previous “The Key Stakeholders” and “Non-Compliance Planning” information from this lab for ways to overcome the obstacles you have listed. In other words, could the issue be resolved by including the right stakeholder or implementing a temporary exception in the policy?

1. _____

2. _____

3. _____

4. _____

5. _____

LAB WORKSHEET

Identifying Hurdles: Create a Checklist

- Now take 5 minutes to brainstorm a list of 2-3 actions you plan to take to resolve each challenge on the previous page.
- Keep in mind the previous “The Key Stakeholders” and “Non-Compliance Planning” information from this lab for ways to overcome the obstacles you have listed. In other words, could the issue be resolved by including the right stakeholder or implementing a temporary exception in the policy?

1. _____

2. _____

3. _____

4. _____

5. _____

Agenda – Lab

SAVVIS

“Developing a Security Policy That Will Survive” Monday, April 28, 2008 Second Hour 11:00 – 12:00

- 7 → The Key Stakeholders
- 8 → Non-Compliance Planning
- 9 → Identifying Hurdles
- 10 → Document Tree – 10 minute Lab
- 11 → Security Awareness and Promotion
- 12 → Wrap - up

© 2008 SAVVIS, Inc. 87

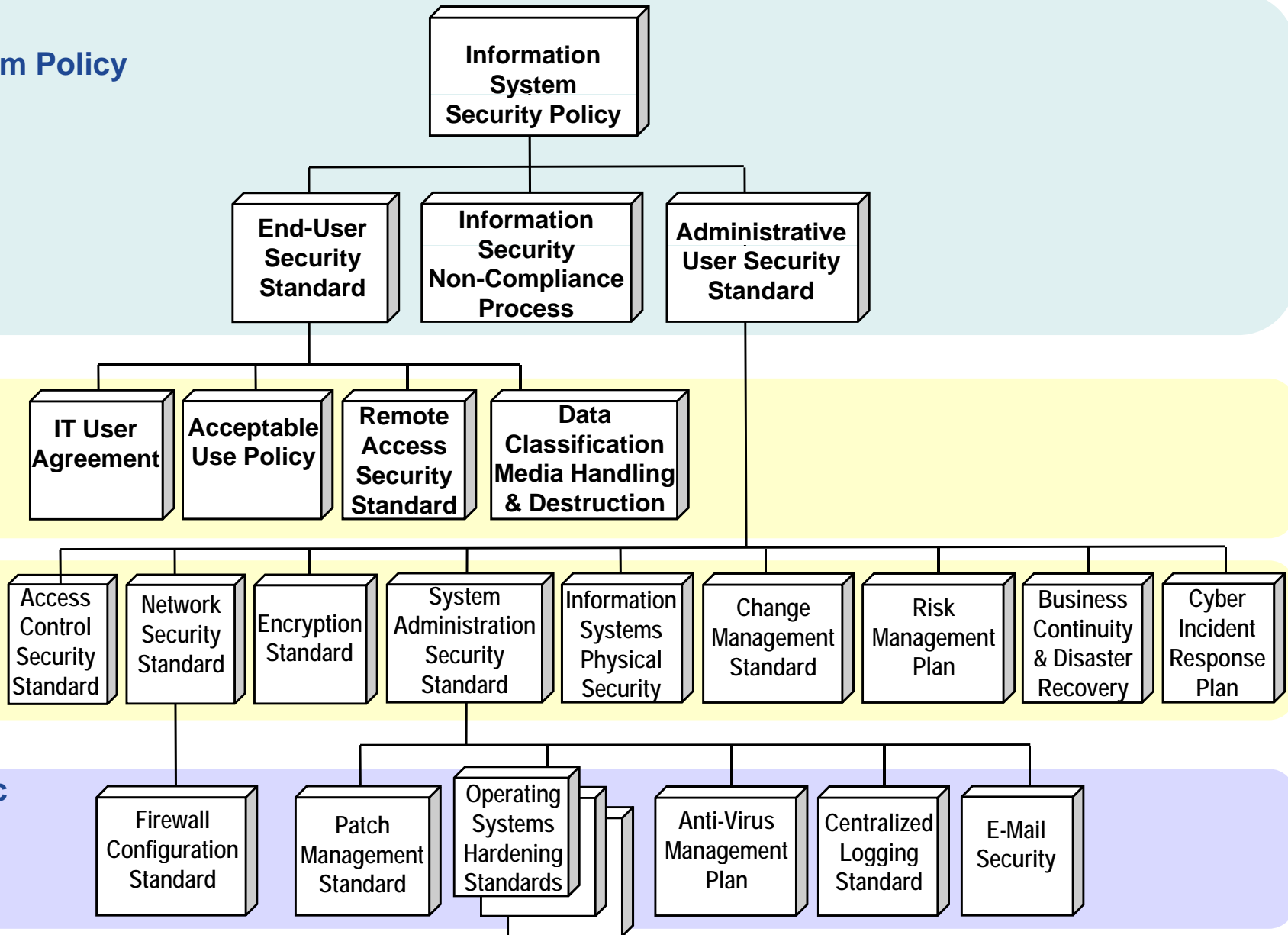
“Notional” Security Policy Document Tree

Security Program Policy

Issue-Specific End-User Security Standards

Issue-Specific Administrative Security Standards

System-Specific Administrative Security Standards



LAB WORKSHEET

A Notional Document Tree

Diagram 1

Take 10 Minutes to make a beginning outline (draw a diagram) of how Security Policy should be structured into sections or multiple documents in your organization. Feel free to mark up the example on the previous page!

MICHAEL METZLER, Ph.D., CISSP, CISM

PAUL HARKER, CISSP, CISM, PMP

“Developing a Security Policy That Will Survive”

Monday, April 28, 2008 – 9:45 am - 12:00 pm

MICHAEL METZLER, Ph.D., CISSP, CISM

PAUL HARKER, CISSP, CISM, PMP

“Developing a Security Policy That Will Survive”

Monday, April 28, 2008 – 9:45 am - 12:00 pm

MICHAEL METZLER, Ph.D., CISSP, CISM

PAUL HARKER, CISSP, CISM, PMP

“Developing a Security Policy That Will Survive”

Monday, April 28, 2008 – 9:45 am - 12:00 pm

Agenda – Lab

“Developing a Security Policy That Will Survive” Monday, April 28, 2008 Second Hour 11:00 – 12:00



7 → The Key Stakeholders

8 → Non-Compliance Planning

9 → Identifying Hurdles


10 → Document Tree

11 → Security Awareness and Promotion
5 Minute Lab

12 → Wrap - up

© 2008 SAVVIS, Inc. 92

Issue-Specific Security Policy



Security Awareness Training Policy:

- Focus on raising awareness of the:
 - ✓ Value of information assets,
 - ✓ Risks to those assets,
 - ✓ Role users play in protection of assets, and
 - ✓ Impact user actions can have on security posture.
- Highlight A Security Focus for the year.
- Always include Social Engineering as one of the topics (change examples and lesson each year).
- Allow Training to be video or web-based, 30-45 minutes, and require annual revision.
- Track user completion for audit, require annual completion for each employee.

© 2008 SAVVIS, Inc. 93

LAB WORKSHEET

Security Awareness and Promotion: Create a Checklist

Take 5 Minutes to make a list of activities that will be used to promote the Security Policy during the next 12 months.

- When is the next Security Awareness Training scheduled?
- Are posters allowed to be placed where people congregate to promote information systems security?
- Is there an internal web site for Information Security? What should be included in the web pages for IT security or Information Assurance?

NOTE: If there is no Security Awareness Program in your organization or site – go back to the lab on “Identifying Hurdles” and add it to the list!

Agenda – Lab

“Developing a Security Policy That Will Survive” Monday, April 28, 2008 Second Hour 11:00 – 12:00

7 → **The Key Stakeholders**

8 → **Non-Compliance Planning**

9 → **Identifying Hurdles**

10 → **Document Tree**

11 → **Security Awareness and Promotion**

12 → **Wrap - up**

© 2008 SAVVIS, Inc. 95

Wrap-Up

- Involve stakeholders in policy development
- Evaluate how policy will be enforced
- Identify the Challenges and List Solutions
- Build A Document Tree
- Use Security Awareness to Promote Policy

© 2008 SAVVIS, Inc. 96

Questions?



e-mail us and ask us for the
White Paper at:

michael.metzler@savvis.net



paul.harker@savvis.net

© 2008 SAVVIS, Inc.