CHƯƠNG 04

CHÍNH SÁCH AN TOÀN THÔNG TIN

Chương 04 - MỤC TIÊU

- Nắm được khái niệm CSATTT và vai trò trung tâm của nó trong một chương trình ATTT thành công
- Liệt kê và mô tả ba loại CSATTT chính và các thành phần chính của mỗi loại
- Giải thích những gì cần thiết để thực hiện CS hiệu quả và những hậu quả mà tổ chức có thể phải đối mặt nếu không thực hiện CS hiệu quả
- Hiểu quá trình phát triển, thực hiện và duy trì các loại CSATTT.

CHÍNH SÁCH AN TOÀN THÔNG TIN

- Tầm quan trọng của CSATTT
- CSATTT trong doanh nghiệp
- Phân loại CSATTT
- Quản lý và điều phối chính CSATTT
- Câu hỏi ôn tập

Chính sách an toàn thông tin

- Các hướng dẫn bằng văn bản do cấp quản lý cung cấp nhằm thông báo cho nhân viên và những người khác tại nơi làm việc về hành vi thích hợp liên quan đến việc sử dụng thông tin và tài sản thông tin một cách thích hợp và an toàn.

Vai trò của CSATTT…

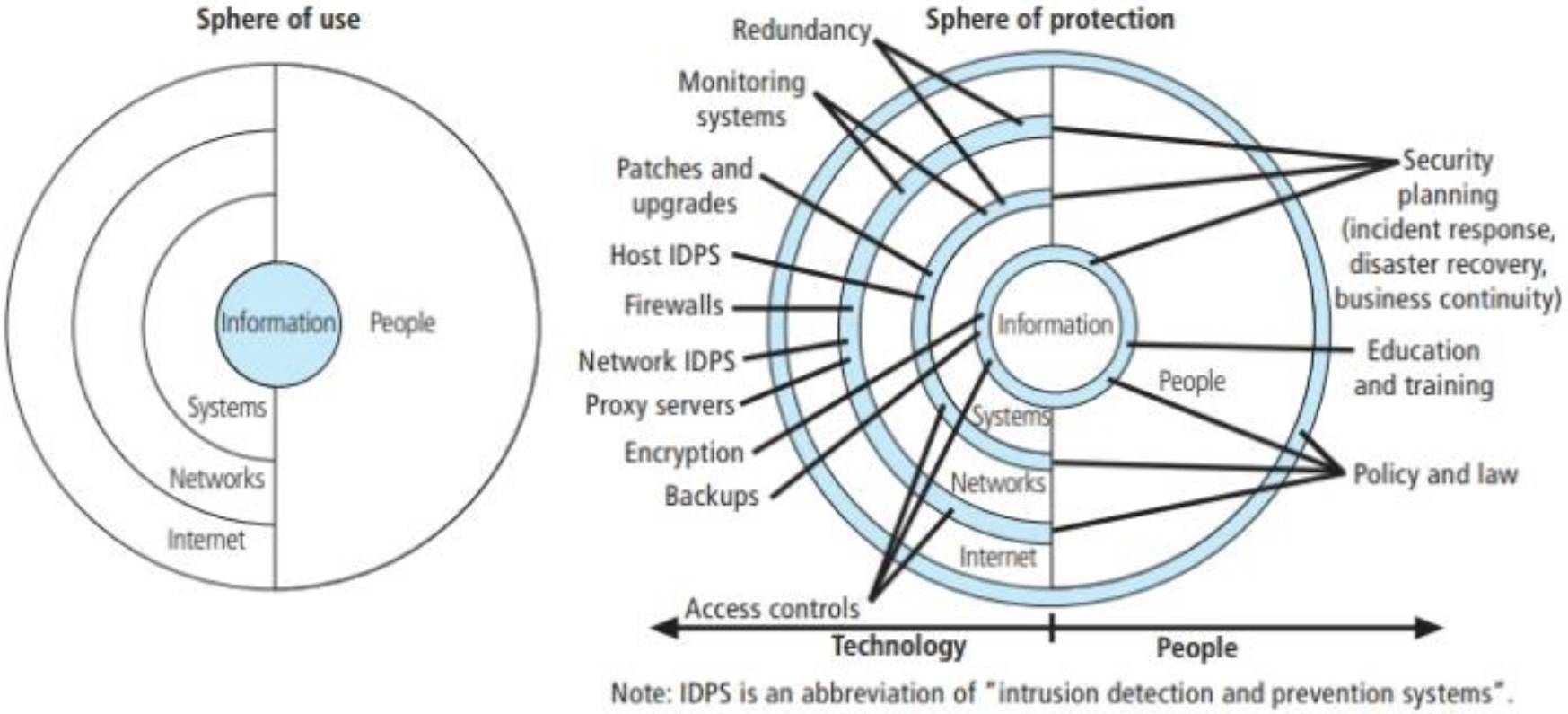
- Một chương trình ATTT chất lượng bắt đầu và kết thúc với chính sách
- là nền tảng thiết yếu của một chương trình ATTT hiệu quả
- Có vị trí trung tâm đối với tất cả các vấn đề trong lĩnh vực ATTT
- được thiết kế để tạo ra một môi trường làm việc năng suất và hiệu quả, không có những phiền nhiễu không cần thiết và các hành động không phù hợp
- được phát triển và thực hiện một cách thích hợp cho phép chương trình ATTT hoạt động gần như liên tục tại tổ chức.

Vai trò của CSATTT…

- là phương tiện kiểm soát ít tốn kém nhất, nhưng thường khó thực hiện nhất.
- Là tài liệu tham khảo quan trọng
  - Đối với đánh giá nội bộ
  - Để giải quyết các tranh chấp pháp lý về trách nhiệm giải trình của ban quản lý
  - Các văn bản chính sách có thể hoạt động như một tuyên bố rõ ràng về ý định của ban quản lý

Vai trò của CSATTT

- có thể là một trong số rất ít các biện pháp kiểm soát hoặc biện pháp bảo vệ một số thông tin nhất định



CHÍNH SÁCH AN TOÀN THÔNG TIN

- Tầm quan trọng của CSATTT
- **CSATTT trong doanh nghiệp**
- Phân loại CSATTT
- Quản lý và điều phối chính CSATTT
- Câu hỏi ôn tập

CSATTT trong doanh nghiệp…

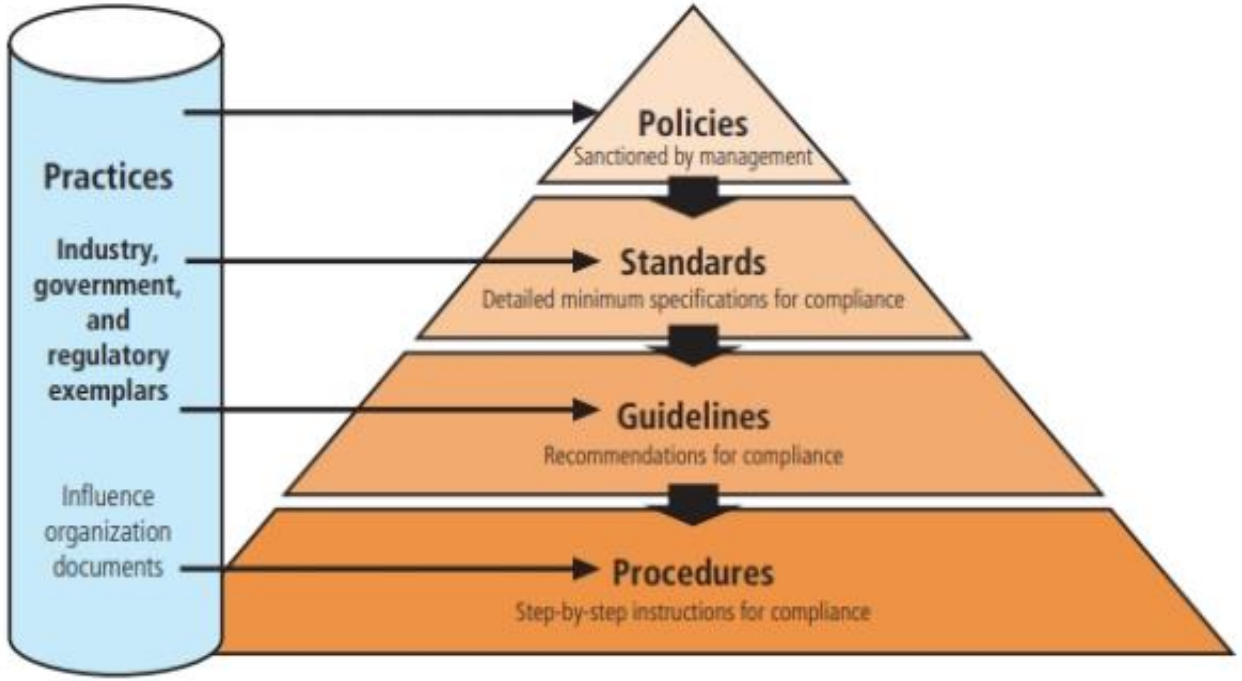
- phải được điều chỉnh cho phù hợp với các nhu cầu cụ thể của tổ chức.
- phải đáp ứng một số tiêu chí:
  - không bao giờ được xung đột với luật pháp.
  - phải có khả năng đứng trước tòa, nếu bị thách thức
  - phải được hỗ trợ và quản lý thích hợp.
- Nguyên tắc xây dựng CSATTT:
  - Chính sách phải đóng góp vào sự thành công của tổ chức.
  - Ban quản lý phải đảm bảo chia sẻ trách nhiệm một cách đầy đủ.
  - Người dùng cuối nên tham gia vào quá trình phát triển chính sách.

CSATTT trong doanh nghiệp…

- **Chính sách** là một tuyên bố về quan điểm của tổ chức nhằm tác động và xác định các quyết định và hành động, và được sử dụng để kiểm soát hành động của mọi người và sự phát triển của các thủ tục.
- không chỉ là một công cụ quản lý để đáp ứng các yêu cầu pháp lý
- để bảo vệ tổ chức và công việc của nhân viên.

CSATTT trong doanh nghiệp…

- có thể được xem như một tập hợp các quy tắc quy định hành vi được chấp nhận và không được chấp nhận trong một tổ chức.



- phải có thông tin về những gì được yêu cầu và những gì bị cấm, về các hình phạt khi vi phạm chính sách và về quy trình kháng cáo.
- Hướng dẫn hỗ trợ cho CS xuất phát từ các **tiêu chuẩn, thủ tục, thực hành và hướng dẫn.**

CSATTT trong doanh nghiệp…

- **Hướng dẫn:** Các khuyến nghị không bắt buộc mà nhân viên có thể sử dụng làm tài liệu tham khảo trong việc tuân thủ chính sách.
- **Thực hành:** Ví dụ về các hành động minh họa việc tuân thủ các chính sách.
- **Thủ tục:** Hướng dẫn từng bước được thiết kế để hỗ trợ nhân viên tuân theo các chính sách, tiêu chuẩn và hướng dẫn.
- **Tiêu chuẩn:** Tuyên bố chi tiết về những việc phải làm để tuân thủ chính sách, đôi khi được xem như các quy tắc chi phối việc tuân thủ chính sách.

CHÍNH SÁCH AN TOÀN THÔNG TIN

- Tầm quan trọng của CSATTT
- CSATTT trong doanh nghiệp
- **Phân loại CSATTT**
- Quản lý và điều phối chính CSATTT
- Câu hỏi ôn tập

Phân loại CSATTT…

- Ba loại CSATTT (NIST SP 800-14):
  - CSATTT doanh nghiệp (Enterprise information security policy - EISP), đặt ra định hướng chiến lược, phạm vi và tư tưởng cho tất cả các nỗ lực an toàn; EISP phải dựa trên và hỗ trợ các tuyên bố về tầm nhìn và sứ mệnh của tổ chức.
  - CSATTT vấn đề cụ thể (Issue-specific security policies - ISSP), cung cấp hướng dẫn cho tất cả các thành viên của tổ chức về việc sử dụng CNTT.
  - CSATTT hệ thống cụ thể (System-specific security policies - SysSP), hướng dẫn việc quản lý và các thông số kỹ thuật của các công nghệ và hệ thống cụ thể.
- Quy trình thông thường:
  - Thứ nhất - tạo ra EISP - chính sách cấp cao nhất
  - Tiếp theo - các chính sách chung được đáp ứng bằng cách phát triển các ISSP và SysSP.

CSATTT doanh nghiệp (Enterprise information security policy - EISP)…

- Hay CS chương trình an toàn, CSAT chung, CSAT IT, CS lnfoSec cấp cao hoặc đơn giản là CS lnfoSec.
- phân công trách nhiệm đối với các lĩnh vực khác nhau của ATTT, bao gồm việc duy trì các CSATTT cũng như các thực hành và trách nhiệm của người dùng cuối.
- hướng dẫn các yêu cầu phát triển, triển khai và quản lý của chương trình ATTT, các yêu cầu này phải được quản lý ATTT và các chức năng an toàn cụ thể khác đáp ứng.

CSATTT doanh nghiệp…

- phải hỗ trợ trực tiếp cho các tuyên bố về tầm nhìn và sứ mệnh của tổ chức.
- là tài liệu cấp điều hành, thường do giám đốc ATTT (CISO) soạn thảo với sự tham vấn của giám đốc thông tin (CIO) và các giám đốc điều hành khác.
- tương đối ngắn gọn, thường dài từ 2 đến 10 trang, nhưng định hình triết lý AT trong toàn bộ môi trường tổ chức.
- thường không yêu cầu sửa đổi thường xuyên
- việc tạo và quản lý CSATTT không phải là tĩnh mà nên được coi là động

CSATTT doanh nghiệp…

- Tích hợp Sứ mệnh và Mục tiêu của Tổ chức vào EISP:
- **Các nội dung trong EISP:**
  - Tổng quan triết lý doanh nghiệp về an toàn
  - Thông tin về cấu trúc của tổ chức ATTT và các cá nhân thực hiện vai trò ATTT
  - Tất cả các thành viên của tổ chức (nhân viên, nhà thầu, nhà tư vấn, đối tác và khách) đều phải chịu trách nhiệm rõ ràng về ATTT.
  - Các trách nhiệm được quy định rõ ràng về an toàn dành riêng cho từng vai trò trong tổ chức.

CSATTT doanh nghiệp…

- **Các thành phần của EISP**:
  - **Mục đích:** Trả lời câu hỏi 'Chính sách nhằm mục đích gì?‘
  - **Các phần tử:** xác định toàn bộ chủ đề ATTT trong tổ chức cũng như các thành phần quan trọng của nó.
  - **Sự cần thiết:** Biện minh cho sự cần thiết của tổ chức phải có một chương trình ATTT
  - **Vai trò và trách nhiệm:** Xác định cấu trúc nhân sự được thiết kế để hỗ trợ InfoSec trong tổ chức
  - **Tham chiếu:** Liệt kê các tiêu chuẩn khác ảnh hưởng và chịu ảnh hưởng của chính sách này (các luật và các chính sách khác).

CSATTT doanh nghiệp…

- Các phần tử (chủ đề ATTT) EISP mẫu…:

Table 4-2 Sample EISP Document Elements

1. Protection of Information	
Policy:	Information must be protected in a manner commensurate with its sensitivity, value, and criticality.
Commentary:	This policy applies regardless of the media on which information is stored, the locations where the information is stored, the systems technology used to process the information, or the people who handle the information. This policy encourages examining the ways information flows through an organization. The policy also points to the scope of Information Security management's work throughout, and often even outside, an organization.
Audience:	Technical staff
2. Use of Information	
Policy:	Company X information must be used only for the business purposes expressly authorized by management.
Commentary:	This policy states that all nonapproved uses of Company X information are prohibited.
Audience:	All

CSATTT doanh nghiệp…

- Các phần tử (chủ đề ATTT) EISP mẫu:
  - Protection of Information
  - Use of Information
  - Information Handling, Access, and Usage
  - Data and Program Damage Disclaimers
  - Legal Conflicts
  - Exceptions to Policies
  - Policy Nonenforcement
  - Violation of Law
  - Revocation of Access Privileges
  - Industry-Specific Information Security Standards
  - Use of Information Security Policies and Procedures
  - Security Controls Enforceability

Bảng 4-2 trang 180-183, Michael E. Whitman, Herbert J. Mattord - Management of Information Security-Cengage Learning (2018)

Phân loại CSATTT…

- Ba loại CSATTT (NIST SP 800-14):
  - CSATTT doanh nghiệp (Enterprise information security policy - EISP)
  - **CSATTT vấn đề cụ thể (Issue-specific security policies - ISSP)**
  - CSATTT hệ thống cụ thể (System-specific security policies - SysSP)

CSATTT vấn đề cụ thể (ISSP)…

- Cung cấp hướng dẫn chi tiết => hướng dẫn tất cả các thành viên của tổ chức sử dụng tài nguyên.
- Nên bắt đầu bằng cách giới thiệu triết lý sử dụng nguồn lực cơ bản của tổ chức: nhằm bảo vệ cả nhân viên và tổ chức khỏi sự kém hiệu quả và mơ hồ.
- Mục đích: hoạt động như một tiêu chuẩn dễ tiếp cận để tuân thủ các chính sách được xác định rộng hơn trong EISP.

CSATTT vấn đề cụ thể (ISSP)…

- ISSP hiệu quả:
  - Thể hiện rõ những mong đợi của tổ chức về cách sử dụng các nguồn lực dựa trên công nghệ của tổ chức.
  - Ghi lại cách thức kiểm soát tài nguyên dựa trên công nghệ, xác định các quá trình và cơ quan có thẩm quyền cung cấp sự kiểm soát này.
  - Quy trách nhiệm cho tổ chức đối với việc nhân viên sử dụng tài nguyên không phù hợp hoặc bất hợp pháp.

CSATTT vấn đề cụ thể (ISSP)…

- ISSP có hiệu lực là một thỏa thuận ràng buộc giữa các bên (tổ chức và các thành viên của tổ chức) và cho thấy rằng tổ chức đã nỗ lực trung thực để đảm bảo rằng công nghệ của mình sẽ không bị sử dụng theo cách không phù hợp.
- ISSP có ba đặc điểm:
  - Giải quyết các tài nguyên dựa trên công nghệ cụ thể.
  - Yêu cầu cập nhật thường xuyên.
  - Chứa một tuyên bố giải thích quan điểm của tổ chức về một vấn đề cụ thể.

CSATTT vấn đề cụ thể (ISSP)...

- Các chủ điểm ISSP...:
  - Sử dụng e-mail, nhắn tin tức thời và các ứng dụng liên lạc điện tử khác
  - Sử dụng Internet, Web và mạng công ty bằng thiết bị của công ty
  - Yêu cầu bảo vệ trước phần mềm độc hại
  - Cài đặt và sử dụng phần mềm hoặc phần cứng không do tổ chức phát hành trên các tài sản của tổ chức
  - Xử lý và/hoặc lưu trữ TT tin tổ chức trên các máy tính không thuộc sở hữu của tổ chức

CSATTT vấn đề cụ thể (ISSP)...

- Các chủ điểm ISSP...:
  - Các quy định cấm hack hoặc kiểm tra các biện pháp kiểm soát AT của tổ chức hoặc cố gắng sửa đổi hoặc leo thang các đặc quyền kiểm soát truy cập
  - Cá nhân và/hoặc gia đình sử dụng các thiết bị máy tính thuộc sở hữu của công ty
  - Xóa thiết bị của tổ chức khỏi tài sản của tổ chức
  - Sử dụng thiết bị cá nhân trên mạng công ty
  - Sử dụng công nghệ cá nhân trong giờ làm việc

CSATTT vấn đề cụ thể (ISSP)…

- Các chủ điểm ISSP:
  - Sử dụng các công nghệ và mạng viễn thông của tổ chức
  - Sử dụng thiết bị photocopy và scan
  - Yêu cầu về lưu trữ và truy cập TT công ty khi ở bên ngoài các cơ sở của công ty
  - Đặc điểm kỹ thuật cho các phương pháp, lập lịch, tiến hành và thử nghiệm sao lưu dữ liệu
  - Yêu cầu đối với việc thu thập, sử dụng và tiêu hủy tài sản TT
  - Các yêu cầu và quyền đối với việc lưu trữ TT xác thực kiểm soát truy cập của người dùng.

CSATTT vấn đề cụ thể (ISSP)…

- Các thành phần của ISSP…:

1. **Tuyên bố về Mục đích**
   a) Phạm vi và khả năng áp dụng
   b) Định nghĩa về công nghệ được khắc phục
   c) Trách nhiệm
2. **Sử dụng được Cấp phép**
   a) Quyền truy cập của người dùng
   b) Sử dụng hợp lý và có trách nhiệm
   c) Bảo vệ quyền riêng tư

CSATTT vấn đề cụ thể (ISSP)…

- Các thành phần của ISSP…:

3. **Việc sử dụng bị cấm**
   a) Sử dụng gây gián đoạn hoặc sử dụng sai mục đích
   b) Sử dụng tội phạm
   c) Tài liệu xúc phạm hoặc quấy rối
   d) Sở hữu trí tuệ có bản quyền, được cấp phép hoặc khác
   e) Các hạn chế khác

4. **Quản lý hệ thống**
   a) Quản lý tài liệu lưu trữ
   b) Giám sát nhà tuyển dụng
   c) Phòng ngừa vi-rút
   d) An toàn vật lý
   e) Mã hóa

CSATTT vấn đề cụ thể (ISSP)…

- Các thành phần của ISSP:

5. **Vi phạm Chính sách**
   a) Thủ tục Báo cáo Vi phạm
   b) Hình phạt cho các vi phạm
6. **Rà soát và sửa đổi chính sách**
   a) Đánh giá chính sách theo lịch trình
   b) Thủ tục sửa đổi
7. **Hạn chế của Trách nhiệm pháp lý**
   a) Tuyên bố về trách nhiệm
   b) Tuyên bố từ chối trách nhiệm khác

CSATTT vấn đề cụ thể (ISSP)…

- **Triển khai ISSP:**
  - Tạo một số tài liệu ISSP, mỗi tài liệu phù hợp với một vấn đề cụ thể.
  - Tạo một tài liệu ISSP toàn diện duy nhất bao gồm tất cả các vấn đề.
  - Tạo một tài liệu ISSP mô-đun thống nhất việc tạo và quản lý chính sách trong khi vẫn duy trì các yêu cầu của từng vấn đề cụ thể.

CSATTT vấn đề cụ thể (ISSP)

PP tiếp cận	Ưu điểm	Nhược điểm
Chính sách Cá nhân	• Phân công rõ ràng cho một bộ phận có trách nhiệm • Được viết bởi những người có chuyên môn cao về chủ đề đối với các hệ thống cụ thể về công nghệ	• Thường mang lại kết quả phân tán không bao gồm tất cả các vấn đề cần thiết • Có thể gặp khó khăn do phổ biến, thực thi và rà soát chính sách kém
Chính sách Toàn diện	• Được kiểm soát tốt bởi các thủ tục được quản lý tập trung đảm bảo phạm vi chủ đề hoàn chỉnh • Thường cung cấp các thủ tục chính thức tốt hơn so với khi các chính sách công thức riêng	• Có thể tổng quát hóa các vấn đề và bỏ qua các lỗ hổng an toàn • Có thể được viết bởi những người có chuyên môn về chủ đề kém hoàn thiện hơn • Thường xác định các quy trình phổ biến, thực thi và kiểm tra lại
Chính sách Mô-đun	• Thường được coi là sự cân bằng tối ưu giữa các cá nhân • Được kiểm soát tốt bởi các thủ tục được quản lý tập trung, đảm bảo phạm vi chủ đề hoàn chỉnh • Phân công rõ ràng cho một bộ phận chịu trách nhiệm • Được viết bởi những người có chuyên môn cao về chủ đề cho các hệ thống công nghệ cụ thể	• Có thể đắt hơn các giải pháp ISSP thay thế khác và các phương pháp tiếp cận ISSP toàn diện • Việc triển khai có thể khó quản lý

Phân loại CSATTT…

- Ba loại CSATTT (NIST SP 800-14):
  - CSATTT doanh nghiệp (Enterprise information security policy - EISP)
  - CSATTT vấn đề cụ thể (Issue-specific security policies - ISSP)
  - **CSATTT hệ thống cụ thể (System-specific security policies - SysSP)**

CSAT hệ thống cụ thể (SysSP)…

- Cung cấp hướng dẫn và thủ tục để định cấu hình các hệ thống, công nghệ và ứng dụng cụ thể
- Thường mang tính chất kỹ thuật nhất, nhưng cũng có thể mang tính chất quản lý
  - Hướng dẫn ứng dụng công nghệ để thực thi chính sách cấp cao hơn (ví dụ: tường lửa để hạn chế truy cập Internet)
- Thường hoạt động như các tiêu chuẩn hoặc thủ tục được sử dụng khi định cấu hình hoặc duy trì hệ thống
- Khung chính sách đảm bảo rằng việc tạo và sử dụng ISSP hoặc SysSP được kích hoạt bởi EISP về các lĩnh vực chủ đề đó.

CSAT hệ thống cụ thể (SysSP)…

- Có thể được tách thành:
  - Hướng dẫn quản lý
  - Thông số kỹ thuật
  - Kết hợp trong một tài liệu chính sách duy nhất.

CSAT hệ thống cụ thể (SysSP)…

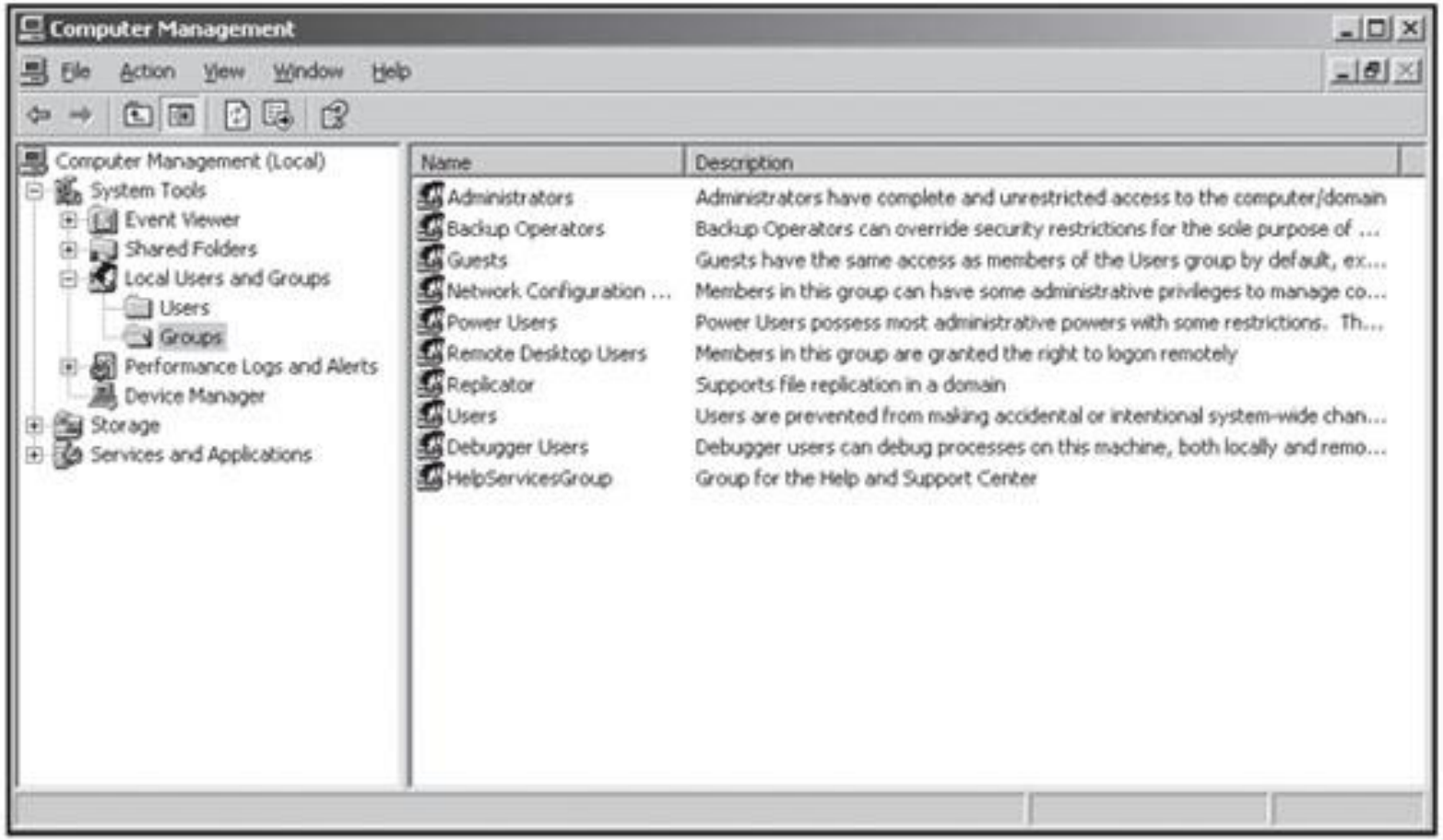
- SysSP hướng dẫn quản lý:
  - Có thể được phát triển cùng lúc với ISSP hoặc có thể được chuẩn bị trước các ISSP liên quan.
  - Do ban quản lý tạo ra để hướng dẫn việc triển khai và cấu hình công nghệ
  - Áp dụng cho bất kỳ công nghệ nào ảnh hưởng đến tính bảo mật, tính toàn vẹn hoặc tính sẵn có của thông tin, ví dụ: cấu hình tường lửa
  - Thông báo cho các nhà công nghệ về ý định quản lý

CSAT hệ thống cụ thể (SysSP)…

- SysSPs đặc điểm kỹ thuật :
  - Hướng dẫn của quản trị viên HT về việc triển khai CS quản lý
  - Mỗi loại thiết bị có các chính sách riêng
  - Các phương pháp chung để thực hiện các biện pháp kiểm soát kỹ thuật
    - Danh sách kiểm soát truy cập (Quản trị viên thiết lập đặc quyền người dùng)
    - Quy tắc cấu hình

SysSPs đặc điểm kỹ thuật…

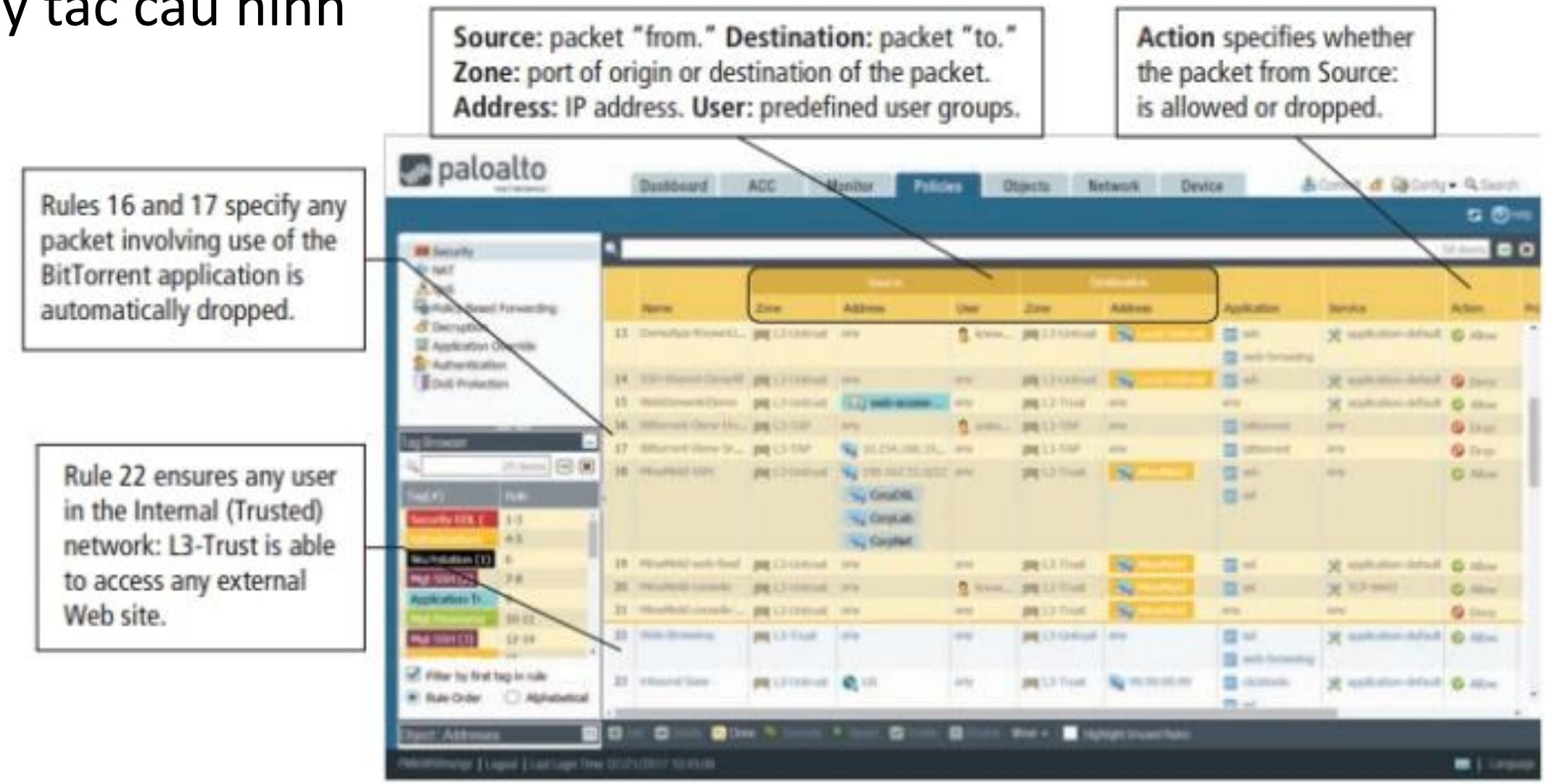
- Danh sách kiểm soát truy cập



The list of "built-in" groups specifies which rights individual users have to and within a particular system.

SysSPs đặc điểm kỹ thuật

- Quy tắc cấu hình



CHÍNH SÁCH AN TOÀN THÔNG TIN

- Tầm quan trọng của CSATTT
- CSATTT trong doanh nghiệp
- Phân loại CSATTT
- **Quản lý và điều phối CSATTT**
- Câu hỏi ôn tập

Quản lý và điều phối CSATTT

1. **Quản lý CSATTT**
2. Điều phối CSATTT
3. Cách tiếp cận phát triển CSATTT

Quản lý chính sách…

- Cần phải được quản lý và thường xuyên thay đổi
- Để duy trì tính khả thi, các CSAT phải có:
  - Một cá nhân chịu trách nhiệm đánh giá (Quản trị viên chính sách)
  - Một lịch trình đánh giá
  - Các thủ tục và thực hành đánh giá
  - Ngày sửa đổi và ban hành chính sách cụ thể.

Quản lý chính sách…

- **Quản trị viên Chính sách**
  - Nhân viên cấp trung chịu trách nhiệm về việc tạo, sửa đổi, phân phối và lưu trữ CS.
  - Chỉ yêu cầu một nền tảng kỹ thuật vừa phải
  - Trưng cầu ý kiến cả từ các chuyên gia ATTT lão luyện (kỹ thuật) và các nhà quản lý
  - Thông báo cho các thành viên bị ảnh hưởng của tổ chức khi CS được sửa đổi
  - Đảm bảo tài liệu CS và các bản sửa đổi tiếp theo được phân phối một cách thích hợp
  - Phải được xác định rõ ràng trên tài liệu CS là người liên hệ chính để cung cấp thông tin bổ sung hoặc khi đề xuất sửa đổi CS.

Quản lý chính sách…

- **Lịch trình đánh giá**
  - Bất kỳ tài liệu CS nào cũng phải chứa một lịch trình xem xét lại được tổ chức hợp lý
  - Một CS nên được xem xét lại ít nhất hàng năm
  - Nên lấy ý kiến đóng góp từ đại diện của tất cả các bên bị ảnh hưởng, ban quản lý và nhân viên, sau đó sử dụng thông tin đầu vào này để sửa đổi tài liệu cho phù hợp.

Quản lý chính sách…

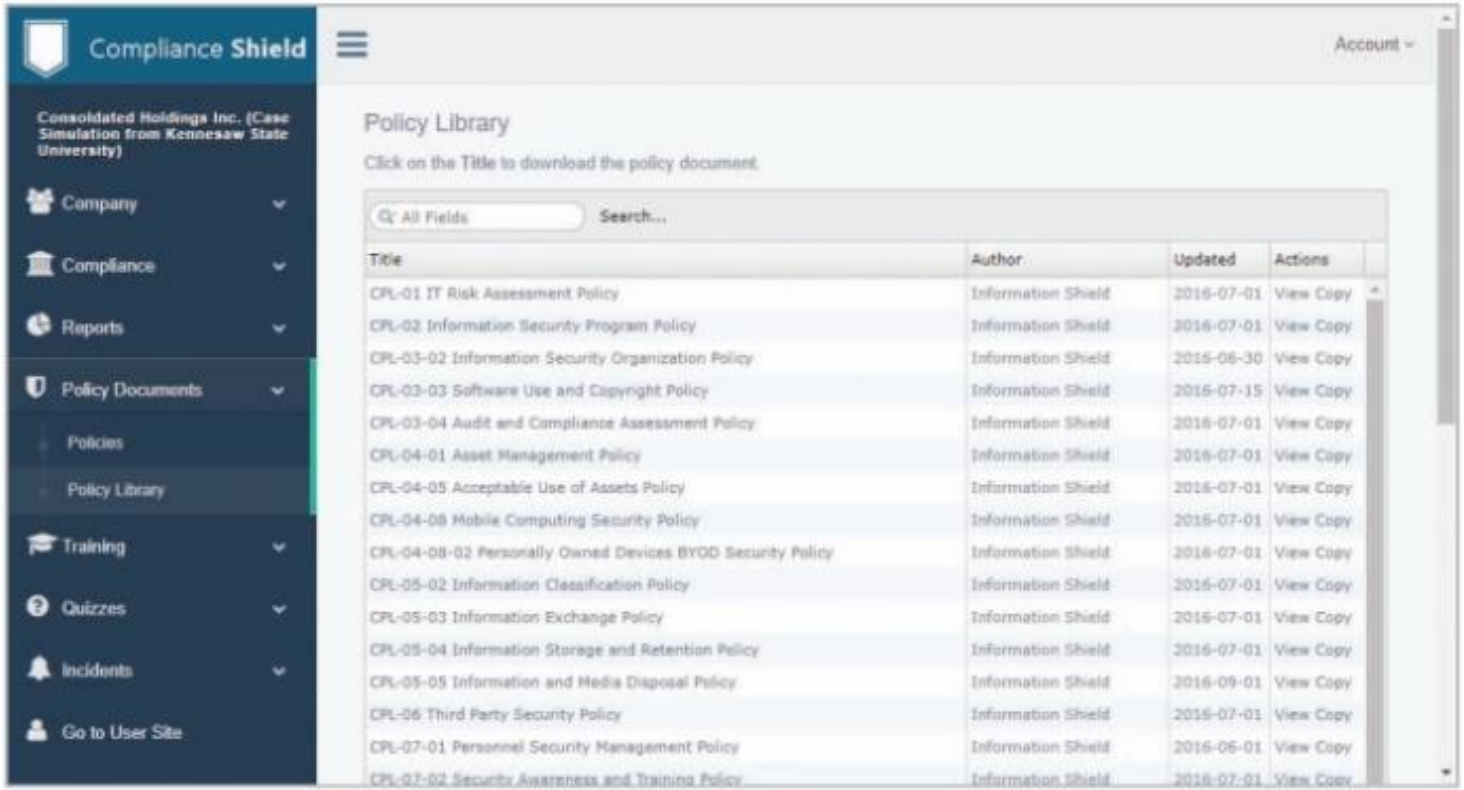
- **Các thủ tục và thực hành đánh giá**
  - Nhà quản lý CS nên thực thi một cơ chế mà các cá nhân có thể dễ dàng đưa ra các đề xuất sửa đổi CS và các tài liệu liên quan khác (e-mail, thư văn phòng hoặc một biểu mẫu Web ẩn danh)
  - Khi CS đã được đưa ra để xem xét, tất cả các ý kiến cần được xem xét và thực hiện các thay đổi đã được cấp quản lý phê duyệt.

Quản lý chính sách

- **Ngày sửa đổi và ban hành chính sách cụ thể**
  - Nên bao gồm ngày xuất bản, cùng với ngày sửa đổi (nếu có).
  - Một số chính sách có thể cần "điều khoản ngừng hoạt động“ (ngày hết hạn).

Phần mềm hỗ trợ cho quản lý chính sách

- Quản lý CS có thể đạt được bằng các công cụ phần mềm hỗ trợ phát triển, thực hiện và duy trì chính sách.
- Kết hợp việc xuất bản và theo dõi chính sách với các video đào tạo và câu hỏi về tuân thủ: Compliance Shield của Information Shield



Quản lý và điều phối CSATTT

1. Quản lý CSATTT
2. **Điều phối CSATTT**
3. Cách tiếp cận phát triển CSATTT

Điều phối CSATTT…

- Trừ khi tổ chức có thể chứng minh rằng CS đã thực sự đến được với người dùng cuối, nếu không, CS đó không thể được thực thi.
- Những CS có chứa TT nội bộ bí mật: đòi hỏi các cấp độ kiểm soát bổ sung (*ghi nhãn tài liệu, phổ biến và lưu trữ CS mới, thu thập và tiêu hủy các phiên bản cũ)* để đảm bảo tính bí mật của TT chứa trong chính các tài liệu CS.
- Các phương pháp:
  - Phân phối bản cứng
  - Phân phối điện tử

Điều phối CSATTT

- Chính sách trao tay cho nhân viên
- Đăng chính sách trên bảng thông báo công khai
- E-mail
- Intranet
- Hệ thống quản lý tài liệu

Quản lý và điều phối CSATTT

1. Quản lý CSATTT
2. Điều phối CSATTT
3. **Cách tiếp cận phát triển CSATTT**

Cách tiếp cận để phát triển CSATTT…

- 3 cách:
  - **Cách tiếp cận quản lý dự án giống như của SDLC**
  - **Information Security Policies Made Easy:** *Wood, Charles Cresson. Information Security Policies Made Easy, 12th ed. Houston, TX: Information Shield, Inc., 2012: 9.*
  - **NIST SP 800-18**: *https:llwww.nist.gov/publications/information-security-handbook-guide-managers.*

Cách tiếp cận để phát triển CSATTT…

- Cách tiếp cận quản lý dự án giống SDLC:
  - Phải được lập kế hoạch, cấp vốn hợp lý và quản lý chặt chẽ để đảm bảo được hoàn thành đúng thời hạn và trong ngân sách
  - Giai đoạn khảo sát: nhận được sự hỗ trợ từ ban lãnh đạo cấp cao và đạt được sự mô tả rõ ràng về các mục tiêu
  - Giai đoạn phân tích: thu thập các tài liệu tham khảo chính, gồm cả các CS hiện hành
  - Giai đoạn thiết kế: tài liệu CS thực tế được tạo.
  - Giai đoạn thực hiện: tổ chức phải phân phối và đạt được sự thừa nhận về CS
  - Giai đoạn duy trì: đảm bảo CS hiệu quả đáp ứng các mối đe dọa đang thay đổi.

Lưu ý

- Các chính sách là một biện pháp đối phó để bảo vệ tài sản khỏi các mối đe dọa
- Thông báo cho nhân viên về hành vi có thể chấp nhận được (không thể chấp nhận được)
- Cải thiện năng suất của nhân viên và ngăn ngừa các tình huống xấu có thể xảy ra
- Thông báo các hình phạt cho việc không tuân thủ
- Ba nguyên nhân chung dẫn đến hành vi phi đạo đức và bất hợp pháp: thiếu hiểu biết, tai nạn và ý định.
- Sự răn đe có thể được tạo ra khi có đủ ba điều kiện: sợ bị phạt, khả năng bị bắt và khả năng bị áp dụng hình phạt.

CHÍNH SÁCH AN TOÀN THÔNG TIN

- Tầm quan trọng của CSATTT
- CSATTT trong doanh nghiệp
- Phân loại CSATTT
- Quản lý và điều phối CSATTT
- **Câu hỏi ôn tập**

Câu hỏi cuối chương…

- Câu 1. Chính sách an toàn thông tin là gì? Tại sao nó lại quan trọng đối với sự thành công của chương trình An toàn thông tin?
- Câu 2. Trong số các biện pháp kiểm soát hoặc biện pháp đối phó được sử dụng để kiểm soát rủi ro ATTT biện pháp nào được xem là ít tốn kém nhất? Các chi phí chính của loại kiểm soát này là gì?
- Câu 3. Liệt kê và mô tả ba thách thức trong việc định hình chính sách.

Câu hỏi cuối chương…

- Câu 4. Phân biệt các khái niệm: chính sách, tiêu chuẩn, thủ tục.
- Câu 5. Để một chính sách có hiệu lực, sau khi được cấp quản lý chấp thuận tổ chức cần phải làm gì? Một số cách để thực hiện điều này là gì?
- Câu 6. Chính sách được coi là tĩnh hay động? Yếu tố nào có thể xác định trạng thái này?
- Câu 7. Liệt kê và mô tả ba loại chính sách An toàn thông tin như được mô tả bởi NIST SP 800-14.

Câu hỏi cuối chương…

- Câu 8. Mục đích của EISP là gì?
- Câu 9. Mục đích của ISSP là gì?
- Câu 10. Mục đích của SysSP là gì?
- Câu 11. Các giá trị, sứ mệnh và mục tiêu của tổ chức nên được tích hợp vào các văn bản chính sách ở mức độ nào?
- Câu 12. Liệt kê và mô tả bốn chủ đề cần có trong EISP.
- Câu 13. Liệt kê và mô tả ba chức năng của ISSP trong tổ chức.

Câu hỏi cuối chương

- Câu 14. Thành phần đầu tiên của ISSP khi nó được trình bày là gì? Tại sao? Thành phần chính thứ hai nên là gì? Tại sao?
- Câu 15. Liệt kê và mô tả ba cách phổ biến trong đó các tài liệu ISSP được tạo và/hoặc quản lý.
- Câu 16. Liệt kê và mô tả hai nhóm tài liệu chung có trong hầu hết các tài liệu SysSP.
- Câu 17. Liệt kê và mô tả ba cách tiếp cận để xây dựng CS. Theo bạn, cái nào là phù hợp nhất để sử dụng cho một tổ chức nhỏ và tại sao? Nếu tổ chức mục tiêu lớn hơn rất nhiều, thì cách tiếp cận nào sẽ phù hợp hơn và tại sao?

HỌC VIỆN KỸ THUẬT MẬT MÃ
AN TOÀN THÔNG TIN

Thank You!