QUẢN LÝ AN TOÀN THÔNG TIN

BÀI 4:
CHÍNH SÁCH AN TOÀN THÔNG TIN

Nguyên tắc quản lý ATTT

Các đặc điểm sau sẽ là trọng tâm của khóa học hiện tại (sáu chữ P):

1. Lập kế hoạch
2. Chính sách
3. Các chương trình
4. Sự bảo vệ
5. Con người
6. Quản lý dự án

http://csrc.nist.gov/publications/PubsTC.html

Nội dung chính:

I. Giới thiệu
II. Tại sao cần đến chính sách?
III. Chính sách, thủ tục và thông lệ
IV. Chính sách bảo mật thông tin doanh nghiệp
V. Chính sách bảo mật thông tin cho từng vấn đề cụ thể
VI. Chính sách bảo mật cho từng hệ thống cụ thể
VII. Các bước để xây dựng một chính sách hiệu quả
VIII. Các phương pháp tiếp cận thay thế

I. Giới thiệu

- Sự thành công của một chương trình bảo vệ tài nguyên thông tin phụ thuộc vào chính sách được tạo ra và thái độ của ban điều hành đối với việc bảo mật thông tin trên các hệ thống tự động (NIST Special Publication 500-169, 1989)

Chính sách là nền tảng thiết yếu cho một chương trình InfoSec hiệu quả.

II. Tại sao lại cần đến chính sách?

- Năm 2015, nghiên cứu State of the Endpoint thực hiện bởi viện Ponemon đưa ra một khảo sát với 703 nhân viên rằng:
  - 78% không tuân theo chính sách bảo mật, và đây là mối đe dọa lớn nhất với bảo mật điểm cuối.
  - 50% trong số đó không được đào tạo nâng cao nhận thức về an ninh hoặc chính sách.
  - 63% đồng ý rằng nhân viên làm việc tại nhà hay các địa điểm khác ngoài công ty làm tăng rủi ro về bảo mật điểm cuối.

TÌM HIỂU VỤ TẤN CÔNG TWITTER NĂM 2020

https://security-assignments.com/activities/case-twitter-2020.html

- Sinh viên xem video trên lớp
- Đọc và tìm hiểu, trả lời các câu hỏi: 15p

II. Tại sao cần đến chính sách?

- Về khảo sát trên, Chris Merritt, giám đốc tiếp thị tại Lumension, đơn vị đã tài trợ cho cuộc khảo sát nói rằng:

-”Tôi không muốn nói rằng họ hầu như không quan tâm, nhưng tôi cũng chỉ ra rằng công ty của họ có lẽ không làm tốt trong việc giúp họ hiểu tại sao họ cần quan tâm.”

- **Vậy chính sách ATTT là gì?**

- Chính sách ATTT là các hướng dẫn bằng văn bản, được cung cấp bởi cấp quản lý, thông báo tới nhân viên và những người khác tại nơi làm việc về các hành vi liên quan đến việc sử dụng thông tin và tài sản thông tin.

II. Tại sao cần đến chính sách?

- **Chính sách ATTT để làm gì?**

  - Cung cấp cấu trúc tại nơi làm việc, giải thích ý niệm của lãnh đạo về việc kiểm soát hành vi của nhân viên liên quan đến tài nguyên thông tin.

  - 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.

  - Cho phép chương trình ATTT hoạt động gần như liền mạch trong nơi làm việc.

II. Tại sao cần đến chính sách?

- **Một số quy tắc cơ bản cần tuân tủ khi xây dựng chính sách.**

  - Chính sách không bao giờ được xung đột với luật pháp. Tuân theo chính sách mà xung đột với luật pháp là phạm tội.

  - Chính sách phải có khả năng đứng trước tòa nếu bị phản đối.

  - Chính sách phải được hỗ trợ và quản lý phù hợp.

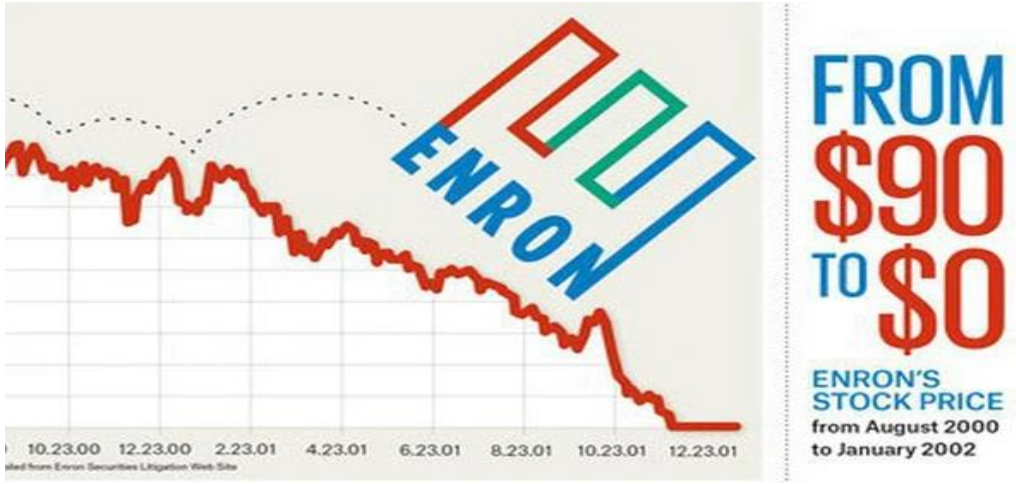
Vụ bê bối tài chính lớn nhất lịch sử:

- Vụ bê bối năm 2001 của Enron Corporation, một công ty năng lượng lớn của Mỹ có trụ sở tại Houston, Texas, và được coi là thất bại kiểm toán lớn nhất.

- Jeffrey Skilling - CEO của Enron, đã phát triển một ban điều hành che giấu hàng tỷ USD thua lỗ. Họ còn gây áp lực lên công ty kiểm toán Arthur Andersen(1 trong 5 cty kiểm toán lớn nhất thế giới) bỏ qua vấn đề này.

Vụ bê bối tài chính lớn nhất lịch sử:

- Bằng cách này, Enron không phải công khai các khoản nợ và che giấu được những khoản lỗ. Kết quả là Enron đã thổi phồng lợi nhuận của mình và giá cổ phiếu của công ty cũng theo đó tăng lên vun vút.
- Vụ việc vỡ lở vào tháng 10-2001, Enron chính thức tiết lộ một khoản lỗ hằng quý khổng lồ và cho biết họ đã phóng đại thu nhập một cách có hệ thống trong suốt ít nhất bốn năm.



Vụ bê bối tài chính lớn nhất lịch sử:

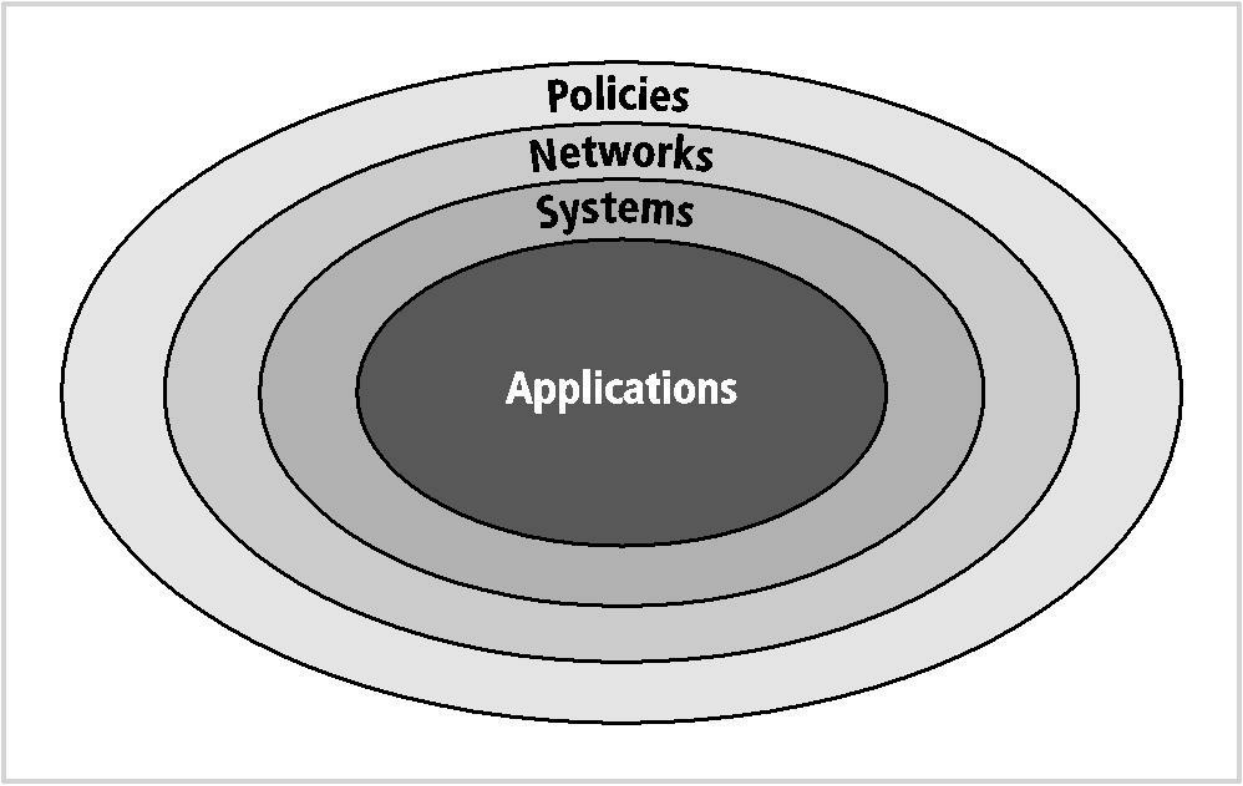
Bài học xương máu: **Một tổ chức phải tuân thủ chính sách của chính mình và chính sách đó phải được áp dụng một cách nhất quán.**

Mô hình Bulls-eye

- Chính sách phải được điều chỉnh cho phù hợp với các yêu cầu cụ thể của tổ chức.
- Mặc dù việc hoàn thiện và tuân thủ các chính sách là một mục tiêu khuyến khích được thực hiện, nhưng sự tồn tại của quá nhiều chính sách hoặc chính sách quá phức tạp có thể gây hoang mang và có thể làm mất tinh thần của nhân viên.
- Mô hình Bulleye - một mô hình triển khai chính sách trong chương trình InfoSec đã được chấp nhận rộng rãi.

Mô hình Bulls-eye

Trong mô hình này, các vấn đề được giải quyết bằng cách chuyển từ cái chung sang cái cụ thể, luôn bắt đầu từ chính sách



Mô hình Bulls-eye

- **Chính sách**
  - Đây là lớp ngoài cùng, là lớp bắt đầu mà hầu hết người dùng có khi tương tác với ATTT.
  - Nó có sẵn từ các tài liệu đã xuất bản thể hiện ý chí của ban quản lý và tìm cách hướng dẫn hành vi của người dùng.

- **Mạng**
  - Đây là môi trường mà các mối đe dọa từ các mạng công cộng và cơ sở hạ tầng mạng gặp nhau.

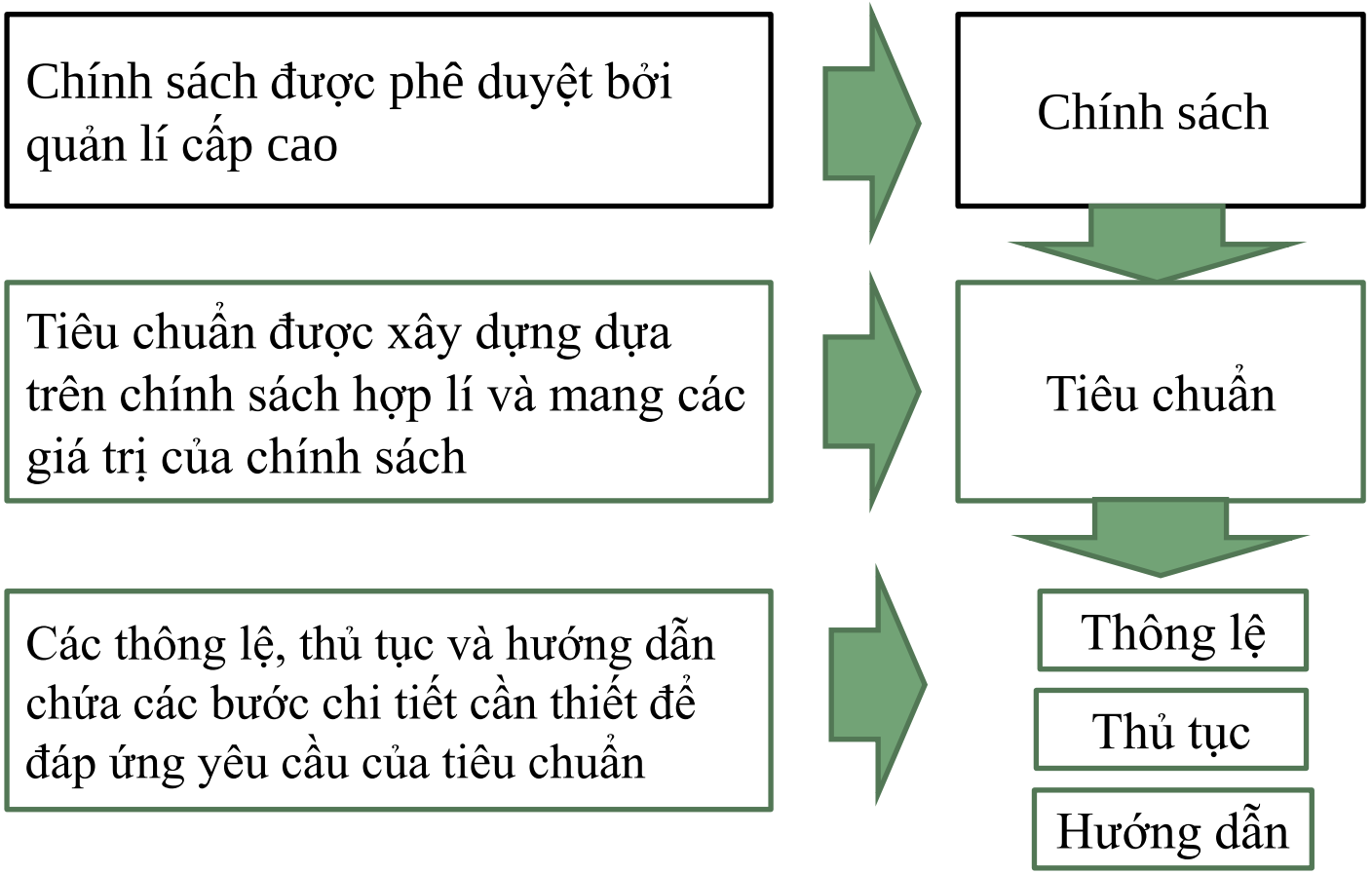
Mô hình Bulls-eye

- **Hệ thống**
  - Đây là những tập hợp phần cứng và phần mềm được sử dụng làm máy chủ hoặc máy tính để bàn cũng như những hệ thống được dùng để kiểm soát các quá trình

- **Ứng dụng**
  - Đây là các hệ thống ứng dụng, từ các ứng dụng đóng gói, chẳng hạn như các chương trình e-mail và tự động hóa văn phòng, phần mềm ứng dụng tùy chỉnh

III. Chính sách, thông lệ và thủ tục

- Hình sau cho ta thấy mối tương quan giữa chính sách, tiêu chuẩn và thông lệ, thủ tục và hướng dẫn:



Chính sách

- **Chính sách là gì?**
  - Chính sách là một kế hoạch hoặc quá trình hoạt động của một chính phủ, đảng phái chính trị hoặc doanh nghiệp, nhằm tác động và xác định các quyết định, hành động và các vấn đề khác.
  - Chính sách thể hiện một tuyên bố chính thức về triết lý quản lý của tổ chức.

- Các chính sách bao gồm một tập hợp các quy tắc quy định hành vi được chấp nhận và không được chấp nhận trong một tổ chức.

Chính sách

- Các chính sách hướng dẫn cách giải quyết các vấn đề cần được giải quyết và các công nghệ nên được sử dụng.

- Các chính sách cũng phải nêu rõ các hình phạt đối với hành vi không được chấp nhận và xác định quy trình kháng nghị.
  - Ví dụ, một tổ chức cấm xem các trang Web không phù hợp tại nơi làm việc phải thực hiện một bộ tiêu chuẩn làm rõ và xác định chính xác nghĩa của từ “không phù hợp” và tổ chức sẽ làm gì để ngăn chặn hành vi đó.

Chính sách

- **Các loại chính sách:**
  - Chính sách bảo mật thông tin doanh nghiệp(EISP)
  - Chính sách bảo mật cho từng vấn đề cụ thể(ISSP)
  - Chính sách bảo mật cho một hệ thống cụ thể(SysSP)
- Mỗi loại chính sách này được tìm thấy trong hầu hết các tổ chức.
- Thủ tục thông thường trước tiên là tạo EISP - cấp chính sách cao nhất. Sau đó, các nhu cầu về chính sách bảo mật của tổ chức được đáp ứng bằng cách phát triển các chính sách ISSP và SysSP

Tiêu chuẩn

- **Tiêu chuẩn là gì?**
  - Tiêu chuẩn là những tuyên bố chi tiết về việc phải làm gì để tuân thủ một chính sách nhất định.
- Mỗi loại chính sách này được tìm thấy trong hầu hết các tổ chức.
- Việc sử dụng các tiêu chuẩn là một cách để thực hiện các chính sách.
- Ví dụ: Khi thực hiện chính sách: Cấm các hành vi không phù hợp khi làm việc, tổ chức có thể tạo ra một tiêu chuẩn chứa tất cả nội dung không phù hợp sẽ bị chặn và liệt kê những tài liệu được coi là không phù hợp.

Tiêu chuẩn

- **Vậy chính sách khác tiêu chuẩn như nào?**
  - Chính sách là các kế hoạch hoặc các hành động cụ thể nhằm gây ảnh hưởng, quyết định hay hành động về 1 vấn đề nào đó
  - Tiêu chuẩn là những tuyên bố chi tiết về việc phải làm để tuân thủ một chính sách nhất định. Việc sử dụng các tiêu chuẩn là một cách để thực hiện chính sách.

- **Một số quy định về tiêu chuẩn:**
  - Được sử dụng để chỉ định hành vi người theo mong đợi. Ví dụ: chữ ký email của công ty phải được nhất quán.
  - Có thể chỉ định những giải pháp phần cứng và phần mềm nào sẵn có và được hỗ trợ.
  - Bắt buộc và phải được thực thi để có hiệu lực (điều này cũng áp dụng cho các chính sách).

Thông lệ, thủ tục và hướng dẫn

- Các thông lệ, thủ tục và hướng dẫn bao gồm các bước chi tiết cần thiết để đáp ứng các yêu cầu của tiêu chuẩn.
- Thủ tục có thể tích hợp:
  - Một danh sách các bước được thực hiện để hoàn thành mục tiêu cuối cùng.
  - Đủ chi tiết và không quá khó để chỉ một nhóm nhỏ (hoặc một người duy nhất) có thể hiểu.
  - Cách để bảo vệ tài nguyên.
  - Chỉ định cấu trúc để thực thi chính sách và cung cấp tài liệu tham khảo nhanh chóng.

Thông lệ, thủ tục và hướng dẫn

- Hướng dẫn:
  - Hướng dẫn là các khuyến nghị cho người dùng khi các tiêu chuẩn cụ thể không được áp dụng.
  - Về bản chất, các hướng dẫn nên được giải thích và không cần phải tuân theo quy định khắt khe về từ ngữ
  - Có thể thay đổi thường xuyên dựa trên môi trường làm việc và cần được xem xét thường xuyên hơn tiêu chuẩn và chính sách.

IV. Chính sách bảo vệ thông tin doanh nghiệp(EISP)

Tổng quan:

- EISP là một tài liệu cấp điều hành, do giám đốc an toàn thông tin (CISO) soạn thảo với sự tham vấn của giám đốc thông tin (CIO) và các giám đốc điều hành khác. Thường dài từ 2–10 trang, nó định hình triết lý bảo mật trong môi trường CNTT của tổ chức.
- Dùng để xác định định hướng chiến lược, tầm nhìn cho 1 công ty và tất cả các chủ đề bảo mật bên trong.
- Chính sách này phải trực tiếp phản ánh các mục tiêu và sứ mệnh của công ty.

IV. Chính sách bảo vệ thông tin doanh nghiệp(EISP)

Vài trò của EISP với tổ chức:

- Nêu rõ tầm quan trọng của InfoSec đối với sứ mệnh và mục tiêu của tổ chức.
- Lập kế hoạch chiến lược InfoSec bắt nguồn từ các chính sách chiến lược khác của tổ chức.
- Làm cho chính sách chung của công ty dễ hiểu hơn.

IV. Chính sách bảo vệ thông tin doanh nghiệp(EISP)

EISP cần cung cấp:

- Tổng quan về triết lý của tổ chức về an ninh.
- Thông tin về vai trò của tổ chức với InfoSec:
  - Trách nhiệm bảo mật được chia sẻ bởi tất cả các thành viên của tổ chức
  - Trách nhiệm bảo mật đối với mỗi vai trò của tổ chức

Các thành phần của EISP

- Tổng quan triết lý doanh nghiệp về bảo mật:
  - Mục đích:
    - Xác định các yếu tố của một chính sách bảo mật tốt
    - Giải thích nhu cầu bảo mật thông tin
    - Chỉ định các loại bảo mật thông tin khác nhau
    - Xác định các trách nhiệm và vai trò bảo mật thông tin
    - Xác định các mức độ bảo mật thích hợp thông qua các tiêu chuẩn và hướng dẫn

Các thành phần của EISP

- Tổng quan triết lý doanh nghiệp về bảo mật:
  - Các thành phần:
    - Xác định toàn bộ chủ đề an toàn thông tin trong tổ chức cũng như các thành phần quan trọng của nó
    - Ví dụ: chính sách có thể nêu: “Bảo vệ tính bí mật, tính toàn vẹn và tính sẵn dùng của thông tin trong quá trình xử lý, truyền tải và lưu trữ, thông qua việc sử dụng chính sách, giáo dục và đào tạo và công nghệ” và sau đó xác định vị trí và cách thức các phần tử được sử dụng.
    - Phần này cũng có thể đưa ra các định nghĩa hoặc triết lý bảo mật để làm rõ chính sách

Các thành phần của EISP

- Tổng quan triết lý doanh nghiệp về bảo mật:
  - Sự cần thiết:
    - Chứng mịnh cho sự cần thiết của tổ chức phải có một chương trình bảo mật thông tin.
  - Vai trò và trách nhiệm:
    - Xác định cấu trúc nhân sự và thiết kế chính sách phù hợp với từng bộ phận
  - Các chính sách, tiêu chuẩn và hướng dẫn khác:
    - Liệt kê các tiêu chuẩn khác có ảnh hưởng và bị ảnh hưởng bởi tài liệu chính sách này

Các thành phần của EISP

- Thông tin về tổ chức an toàn thông tin và vai trò của an toàn thông tin:
  - Tất cả các thành viên của tổ chức (nhân viên, nhà thầu, nhà tư vấn, đối tác và khách tham quan) đều phải chịu trách nhiệm rõ ràng về bảo mật.
  - Các trách nhiệm được quy định rõ ràng về bảo mật dành riêng cho từng vai trò trong tổ chức

Chính sách bảo mật cho từng vấn đề cụ thể(ISSP)

- Chính sách bảo mật phù hợp với vấn đề cụ thể (ISSP) cung cấp hướng dẫn chi tiết, có mục tiêu để hướng dẫn tất cả các thành viên của tổ chức sử dụng tài nguyên
- Cung cấp sự hiểu biết chung về mục đích mà nhân viên bị giới hạn quyền truy cập tài nguyên
- Chính sách này nhằm bảo vệ cả nhân viên và tổ chức khỏi sự kém hiệu quả và mơ hồ
- Bồi thường cho tổ chức về trách nhiệm pháp lý đối với việc sử dụng hệ thống không phù hợp hoặc bất hợp pháp của nhân viên

Chính sách bảo mật cho từng vấn đề cụ thể(ISSP)

- Chính sách ISSP hiệu quả sẽ thực hiện được những điều sau:
  - Nêu rõ những kỳ vọng của tổ chức về cách sử dụng hệ thống dựa trên công nghệ của tổ chức.
  - Ghi lại cách hệ thống công nghệ được kiểm soát và xác định các điểm chuyên nghiệp và các cơ quan có thẩm quyền cung cấp sự kiểm soát này.
  - Quy trách nhiệm cho tổ chức đối với việc sử dụng hệ thống không phù hợp hoặc không hợp pháp của nhân viên

Các lĩnh vực có thể áp dụng ISSP

- Sử dụng e-mail và các ứng dụng liên lạc điện tử khác
- Yêu cầu bảo vệ khỏi các phần mềm độc hại
- Sử dụng tại nhà thiết bị máy tính thuộc sở hữu của công ty
- Sử dụng thiết bị cá nhân trên mạng công ty
- Sử dụng công nghệ viễn thông (fax, điện thoại, điện thoại di động)
- Sử dụng thiết bị photocopy và quét

Các thành phần của ISSP

- Mục đích
  - Nêu rõ mục đích ngay từ đầu giải quyết các câu hỏi sau:
    - Mục đích của chính sách này là gì?
    - Ai chịu trách nhiệm và chịu trách nhiệm về việc áp dụng chính sách?
    - Tài liệu chính sách đề cập đến những công nghệ và vấn đề nào?
- Các hành vi được phép:
  - Giải thích ai có thể sử dụng công nghệ và cho những mục đích nào
  - Yêu cầu "sử dụng hợp lý và có trách nhiệm" đối với thiết bị và các tài sản khác của tổ chức, đồng thời giải quyết các vấn đề pháp lý quan trọng, chẳng hạn như bảo vệ thông tin cá nhân và quyền riêng tư

Các thành phần của ISSP

- Các hành vi bị cấm
  - Nêu rõ hành vi hoặc công nghệ bị cấm sử dụng
  - Trình bày rõ ràng các giả định và sau đó viết ra các trường hợp ngoại lệ
  - Có thể gộp các hành vi được phép và các hành vi bị cấm lại thành một phần
- Quản lý hệ thống
  - Tập trung vào mối quan hệ của người dùng với quản lý hệ thống
  - Chỉ định trách nhiệm của người dùng và hệ thống quản lý, để tất cả các bên biết họ phải chịu trách nhiệm gì

Các thành phần của ISSP

- Vi phạm chính sách
  - Phần này nêu rõ các hình phạt và hậu quả của việc vi phạm chính sách người quản lý hệ thống và sử dụng. Hình phạt cần được đặt ra cho mỗi vi phạm
- Rà soát và sửa đổi chính sách
  - Mọi chính sách phải có các thủ tục và thời gian biểu để xem xét định kỳ.
  - Phần này cần phác thảo một phương pháp luận cụ thể để xem xét và sửa đổi ISSP, để đảm bảo rằng người dùng luôn có quyền phản ảnh các công nghệ và nhu cầu hiện tại của tổ chức

Các thành phần của ISSP

- Giới hạn trách nhiệm về pháp lý
  - Đưa ra một tuyên bố chung về trách nhiệm pháp lý hoặc một tập hợp các tuyên bố từ chối trách nhiệm
  - Nếu nhân viên vi phạm chính sách của công ty hoặc bất kỳ luật nào bằng cách sử dụng công nghệ của công ty, công ty sẽ không bảo vệ họ và công ty không chịu trách nhiệm về hành động của họ

Triển khai ISSP

Có thể thực hiện một số cách triển khai để tạo và quản lý ISSP. Ba trong số những cách phổ biến nhất là:

- Tạo một số tài liệu ISSP độc lập, 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 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

Chính sách cá nhân

Ưu điểm:

- Phân công rõ ràng cho một bộ phận có trách nhiệm
- Được viết bởi những người có chuyên môn cao về chủ đề cho các hệ thống công nghệ cụ thể

Nhược điểm:

- Thường tạo ra kết quả ảnh chụp 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

Ưu điểm:

- 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 được xây dựng riêng lẻ
- Thường xác định các quy trình phổ biến, thực thi và xem xét

Nhược điểm:

- Có thể tổng quát hóa quá mức các vấn đề và bỏ qua các lỗ hổng bảo mật
- Có thể được viết bởi những người có chuyên môn về chủ đề kém hoàn chỉnh hơn

Chính sách mô-đun

Ưu điểm:

- Là sự cân bằng tối ưu giữa ISSP cá nhân và các cách tiếp cận ISSP toàn diện
- 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

Nhược điểm:

- Chi phí đắt
- Việc triển khai có thể khó quản lý

Chính sách bảo mật hệ thống cụ thể (SysSP)

- SysSP thường hoạt động như các tiêu chuẩn hoặc thủ tục được sử dụng khi định cấu hình hoặc bảo trì hệ thống
- SysSP có thể được tách thành hai nhóm chung, hướng dẫn quản lý và thông số kỹ thuật hoặc chúng có thể kết hợp hai loại thành một tài liệu SysSP thống nhất

Chính sách bảo mật hệ thống cụ thể

- Hướng dẫn quản lý SysSPs
  - Hướng dẫn quản lý Tài liệu SysSP được ban quản lý tạo ra để hướng dẫn việc triển khai và cấu hình công nghệ cũng như giải quyết hành vi của mọi người trong tổ chức nhằm hỗ trợ việc bảo mật thông tin.

Ví dụ:

- Trong khi cấu hình cụ thể của tường lửa thuộc thông số kỹ thuật SysSP, thì quá trình xây dựng và triển khai tường lửa phải tuân theo các nguyên tắc do ban quản lý thiết lập. Tại sao? Trong trường hợp không có hướng dẫn này, quản trị viên tường lửa có thể định cấu hình tường lửa khi họ thấy phù hợp, có thể trùng khớp hoặc không với ý định của tổ chức.

Chính sách bảo mật hệ thống cụ thể

- Hướng dẫn quản lý SysSPs
  - Áp dụng cho bất kỳ công nghệ nào ảnh hưởng đến tính bảo mật, tính toàn vẹn hoặc tính sẵn có của thông tin.
  - SysSP có thể được phát triển cùng lúc với ISSP, hoặc chúng có thể được chuẩn bị trước các ISSP liên quan của chúng.

Thông số kỹ thuật SysSPs

- Mặc dù người quản lý có thể làm việc với quản trị viên hệ thống để tạo chính sách quản lý, như được mô tả trong phần trước, người quản trị hệ thống có thể cần tạo một loại chính sách khác để thực hiện chính sách quản lý.

Ví dụ:

  - ISSP có thể yêu cầu thay đổi mật khẩu người dùng hàng quý; quản trị viên hệ thống có thể triển khai kiểm soát kỹ thuật trong một ứng dụng cụ thể để thực thi chính sách này.

- Các phương pháp chung để thực hiện các biện pháp kiểm soát kỹ thuật:
  - Danh sách kiểm soát truy cập.
  - Quy tắc cấu hình

Thông số kỹ thuật SysSPs

- Danh sách kiểm soát truy cập (ACL):
  - Danh sách kiểm soát truy cập (ACL) bao gồm danh sách truy cập của người dùng, ma trận và bảng khả năng chi phối các quyền và đặc quyền của người dùng.
  - Cho phép quản trị hạn chế quyền truy cập theo người dùng, máy tính, thời gian, thời lượng hoặc thậm chí một tệp cụ thể.

Thông số kỹ thuật SysSPs

- Danh sách kiểm soát truy cập:
  - ACL quy định các khía cạnh sau của quyền truy cập:
    - Ai có thể sử dụng hệ thống.
    - Người dùng được ủy quyền có thể truy cập những gì.
    - Khi người dùng được ủy quyền có thể truy cập vào hệ thống.
    - Người dùng được ủy quyền có thể truy cập hệ thống từ đâu.
    - Người dùng được ủy quyền có thể truy cập hệ thống như thế nào.

Thông số kỹ thuật SysSPs

- Danh sách kiểm soát truy cập:
  - ACL có thể hạn chế sự truy cập 1 cách tự do của người dùng bằng cách cấp quyền.
  - Các quyền mà quản trị viên cấp cho người dùng:
    - Đọc
    - Ghi
    - Thực thi
    - Xóa

Thông số kỹ thuật SysSPs

- Quy tắc cấu hình:
  - Các quy tắc cấu hình là các mã hướng dẫn hướng dẫn việc thực thi hệ thống khi thông tin đi qua nó.
  - Các chính sách dựa trên quy tắc cụ thể hơn đối với hoạt động của hệ thống so với ACL và chúng có thể giải quyết trực tiếp hoặc không với người dùng.
  - Nhiều hệ thống bảo mật yêu cầu các tập lệnh cấu hình cụ thể chỉ định hành động nào cần thực hiện trên mỗi tập thông tin mà chúng xử lý.

VII. Các bước để xây dựng một chính sách hiệu quả

- Chính sách chỉ có thể thực thi nếu nó được thiết kế, phát triển và thực hiện đúng cách bằng cách sử dụng một quy trình đảm bảo các kết quả có thể lặp lại.

Các bước để xây dựng một chính sách hiệu quả

- Để các chính sách có hiệu lực, chúng phải được thực hiện đúng 6 bước:
  - Phát triển: Được phát triển bằng cách sử dụng các thông lệ được ngành công nghiệp chấp nhận.
  - Phổ biến: Được phổ biến bằng các phương pháp thích hợp hợp cho nhân viên.
  - Đọc: Được tất cả nhân viên đọc.
  - Hiểu: Được tất cả nhân viên hiểu.
  - Tuân thủ: Được nhân viên tuân thủ bằng hành động hoặc sự cam kết.
  - Thực thi thống nhất: Được nhân viên áp dụng và thực thi 1 cách thống nhất.

1. Phát triển chính sách bảo mật thông tin

- Nên xem việc phát triển chính sách là một dự án gồm 2 phần.
  - ❿ Thiết kế và phát triển chính sách (hoặc tái thiết kế và tái phát triển một chính sách đã lỗi thời.
  - ❿ Củng cố quy trình quản lý để duy trì chính sách trong tổ chức
- Dự án phát triển chính sách cần có:
  - Bản kế hoạch tốt
  - Được cấp vốn hợp lý
  - Được quản lý sát sao để đảm bảo rằng nó được hoàn thành đúng thời hạn và mục tiêu
- Dự án phát triển chính sách có thể được xây dựng theo mô hình SecSDLC

Mô hình SecSDLC cho dự án phát triển chính sách

- Giai đoạn điều tra:
  - Có hỗ trợ từ quản lý cấp cao
  - Trình bày rõ ràng các mục tiêu
  - Có quản lý đủ năng lực
  - Xây dựng bản phác thảo chi tiết về phạm vi của dự án phát triển chính sách và các ước tính hợp lý về chi phí và lịch trình của dự án.

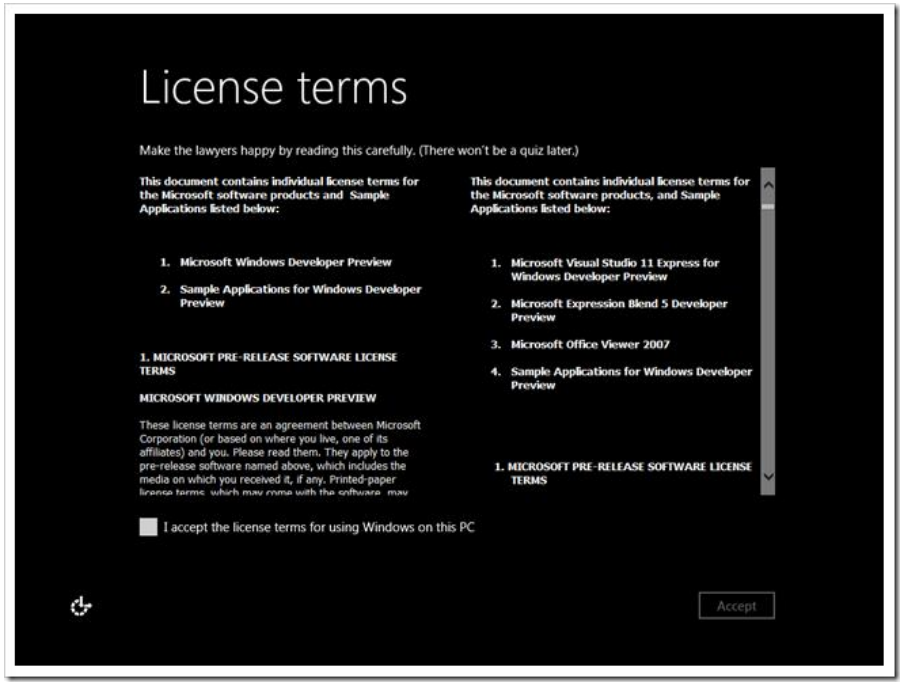
Mô hình SecSDLC cho dự án phát triển chính sách

- Giai đoạn phân tích
  - Đánh giá rủi ro mới hoặc gần đây hoặc đánh giá việc ghi lại các nhu cầu an toàn thông tin hiện tại của tổ chức
  - Tổng hợp các tài liệu tham khảo - bao gồm mọi chính sách hiện có

Mô hình SecSDLC cho dự án phát triển chính sách

- Giai đoạn thiết kế

  Phải lập một kế hoạch để phân phối và xác minh việc phân phối các chính sách.



Mô hình SecSDLC cho dự án phát triển chính sách

- Giai đoạn thực hiện
  - Viết chính sách
  - Phân bổ chính sách
- Giai đoạn bảo trì
  - Giám sát, duy trì và sửa đổi chính sách nếu cần
  - Cơ chế báo cáo tích hợp
  - Rà soát tích hợp

2. Phân phối chính sách an toàn thông tin

- Các lựa chọn phổ biến:
  - Phân bố bản cứng: các bản in, bảng thông báo ...
  - Phân bố điện tử: E-mail, mạng nội bộ ...

3. Việc đọc chính sách

- Các rào cản đối với đọc hiểu chính sách của nhân viên có thể xuất phát từ các vấn đề về đọc viết hoặc ngôn ngữ.
- Các tổ chức đa quốc gia cũng phải đối phó với những thách thức trong việc đánh giá mức độ đọc của công dân nước ngoài. Bản dịch đơn giản của các tài liệu chính sách, mặc dù là yêu cầu tối thiểu, nhưng cần phải theo dõi cẩn thận. Các vấn đề về dịch thuật từ lâu đã tạo ra những thách thức cho các tổ chức.

4. Việc hiểu chính sách

- Để chắc chắn rằng nhân viên hiểu chính sách, tài liệu phải được viết ở mức độ dễ đọc, với các thuật ngữ quản lý và thuật ngữ kỹ thuật giảm ở mức tối thiểu.
- Bước tiếp theo là sử dụng một số hình thức đánh giá để đánh giá mức độ hiểu biết của nhân viên về các vấn đề cơ bản của chính sách. Các câu đố và các hình thức kiểm tra khác có thể được sử dụng để đánh giá một cách định lượng xem nhân viên nào hiểu chính sách bằng cách đạt điểm tối thiểu (ví dụ: 70%) và nhân viên nào cần được đào tạo thêm và nỗ lực nâng cao nhận thức trước khi chính sách có thể được thực thi. Các câu hỏi có thể được phân phối dưới dạng bản cứng hoặc dạng điện tử.

5. Việc tuân thủ chính sách

- Tuân thủ chính sách có nghĩa là nhân viên phải đồng ý với chính sách.
- Nếu nhân viên không đồng ý với chính sách có nghĩa là từ chối làm việc và do đó có thể là căn cứ để chấm dứt hợp đồng. Các tổ chức có thể tránh được tình thế tiến thoái lưỡng nan này bằng cách kết hợp các xác nhận chính sách vào hợp đồng lao động, bản định giá niên kim hoặc các tài liệu khác cần thiết cho việc tiếp tục làm việc của cá nhân.

6. Việc thực thi chính sách

- Thực thi đồng bộ và theo từng vị trí
- Việc thực thi chính sách phải có khả năng chịu được sự giám sát kỹ lưỡng từ bên ngoài.

VIII. Các phương pháp tiếp cận thay thế

- Phương pháp xây dựng chính sách của Charles Cresson Wood
- Kế hoạch phát triển bảo mật cho Liên bang

Phương pháp xây dựng chính sách của Charles Cresson Wood

- Thu thập các tài liệu tham khảo chính
- Xác định khuôn khổ cho các chính sách
- Chuẩn bị một ma trận bảo hiểm
- Đưa ra các quyết định thiết kế hệ thống cốt yếu
- Cấu trúc quy trình xem xét, phê duyệt và thực thi

Kế hoạch phát triển bảo mật cho HTTT Liên bang

- "Special Publication 800-18, Rev. 1" của NIST củng cố cách tiếp cận lấy quy trình kinh doanh làm trung tâm để quản lý chính sách.

- Các chính sách là tài liệu sống

- Các thông lệ quản lý tốt để xây và duy trì chính sách giúp cho một tổ chức linh hoạt.

Kế hoạch phát triển bảo mật cho HTTT Liên bang

- Yêu cầu:
  - Một cá nhân có trách nhiệm
  - Một lịch trình đánh giá
  - Một phương pháp để đưa ra đề xuất cho các bài đánh giá
  - Một dấu hiệu về chính sách và ngày sửa đổi.

Một lưu ý cuối cùng về chính sách

Bạn có thể tin rằng lý do duy nhất để có chính sách là tránh kiện tụng, điều quan trọng là phải nhấn mạnh bản chất phòng ngừa của chính sách.