Chương IV

4

CHÍNH SÁCH AN TOÀN THÔNG TIN

(INFORMATION SECURITY POLICY)

Nội dung chính

1) Các khái niệm cơ bản
2) Các thành phần của chính sách ATTT
3) Tầm quan trọng của chính sách an toàn thông tin đối với doanh nghiệp/cá nhân
4) Vòng đời của chính sách an toàn thông tin
5) Xây dựng hoặc đưa ra các khuyến nghị về chính sách an toàn thông tin thích hợp.
6) Các bước triển khai một chính sách an toàn thông tin

https://www.sans.org/security-resources/policies/

Các khái niệm cơ bản

1) Chính sách

- **Chính sách** là một hệ thống nguyên tắc có chủ ý hướng dẫn các quyết định và đạt được các kết quả hợp lý. Một chính sách là một tuyên bố về ý định, và được thực hiện như một thủ tục hoặc giao thức.
- Các chính sách thường được cơ quan quản trị thông qua trong một tổ chức. Chính sách có thể hỗ trợ cả việc đưa ra quyết định chủ quan và khách quan.
- Ví dụ: chính sách cân bằng giữa công việc và cuộc sống.

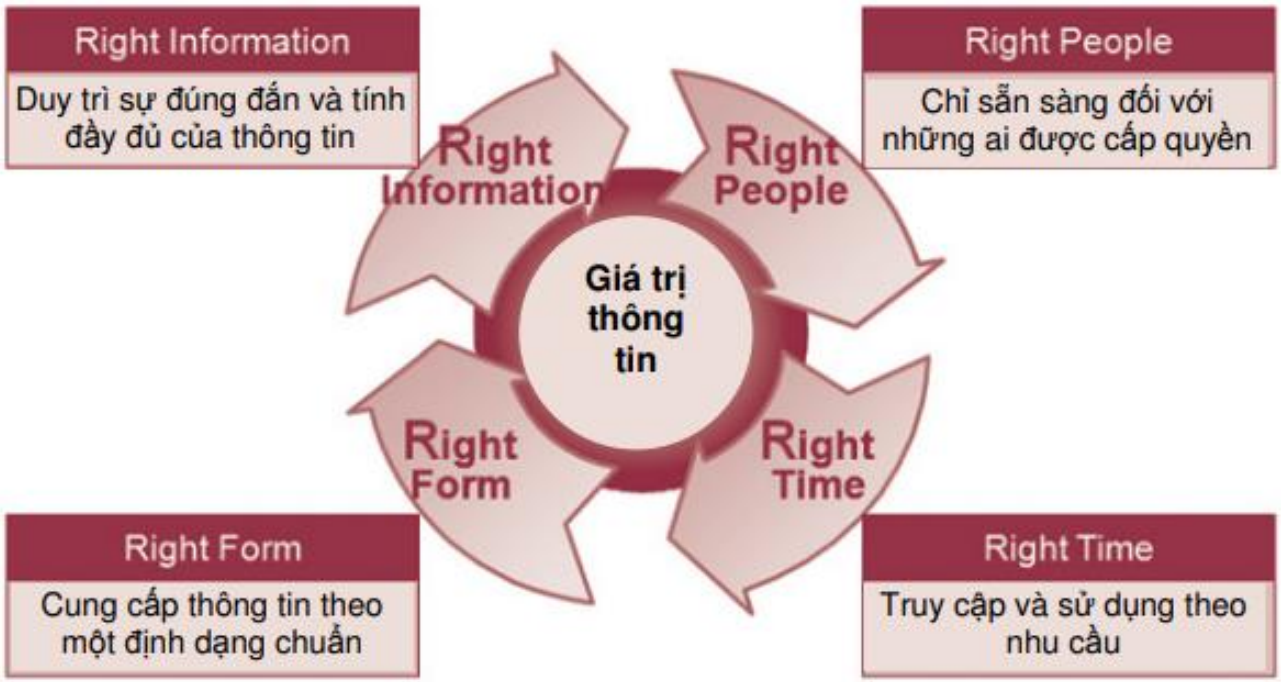
Các khái niệm cơ bản

1) Chính sách:

- Các chính sách tương phản để hỗ trợ việc ra quyết định khách quan thường hoạt động trong tự nhiên và có thể được kiểm tra khách quan, ví dụ: chính sách mật khẩu.
- Chính sách khác với các quy tắc hoặc luật pháp. Mặc dù luật pháp có thể buộc hoặc cấm hành vi (ví dụ: luật yêu cầu nộp thuế đối với thu nhập), chính sách chỉ hướng dẫn hành động đối với những hành vi có nhiều khả năng đạt được kết quả mong muốn nhất.

Các khái niệm cơ bản

2) An toàn thông tin: giá trị thông tin



Các khái niệm cơ bản

3) Chính sách bảo mật an toàn thông tin:

Information Security Policy (ISP)

ISP là một tập các quy tắc, hướng dẫn mà tổ chức đưa ra nhằm đảm bảo tính an toàn hệ thống thông tin và miễn nhiễm chống lại tấn công nguy hiểm.

Các khái niệm cơ bản

3) Chính sách an toàn thông tin:

- ISP cung cấp một ***môi trường để quản lý thông tin một cách an toàn trong toàn tổ chức.***
- ISP được viết ***cho tất cả các cấp nhân viên khác nhau.***
- ISP gồm ***các quy tắc chung về tất cả các chủ đề có liên quan đến an toàn thông tin và sử dụng máy tính hoặc các quy tắc riêng biệt về các chủ đề khác nhau***
- Ví dụ: quy tắc dùng e-mail, quyền hạn truy xuất dữ liệu, quy trình backup dữ liệu,....

RỦI RO KHI MẤT AN TOÀN THÔNG TIN

- **Đối với cá nhân:** Việc rò rỉ hay bị đánh cắp thông tin sẽ làm ảnh hưởng vô cùng nghiêm trọng đến tài chính, uy tín, các mối quan hệ của một cá nhân. Đặc biệt là các hành vi đánh cắp dữ liệu, tung lên mạng nhằm mục đích bôi xấu cá nhân và hack hệ thống tài khoản ngân hàng gây thiệt hại lớn.
- **Đối với doanh nghiệp:** Nếu chẳng may bị tin tặc tấn công, doanh nghiệp sẽ phải đối mặt với nguy cơ mất dữ liệu, thất thoát tài chính, gián đoạn hoạt động công ty, thiệt hại điện tử vật lý. Đó là còn chưa kể đến việc hình ảnh cũng như thương hiệu bị ảnh hưởng.

Mục đích của ISP - Tầm quan trọng của ISP

Các tổ chức đưa ra các ISP bởi nhiều lý do khác nhau:

- Thiết lập một cách tiếp cận chung đối với an toàn thông tin.
- Phát hiện và ngăn chặn sự thoả hiệp của an toàn thông tin như lạm dụng dữ liệu, mạng, hệ thống máy tính và các ứng dụng.
- Để bảo vệ danh tiếng của công ty đối với trách nhiệm đạo đức và pháp lý của công ty.
- Thực hiện các quyền của khách hàng; Cung cấp cơ chế hiệu quả để đáp ứng các khiếu nại và thắc mắc liên quan đến sự không tuân thủ chính sách thực tế hoặc không nhận thức được là một cách để đạt được mục tiêu này.

Mục đích của ISP - Tầm quan trọng của ISP

- Giảm thiểu nguy cơ rò rỉ dữ liệu hoặc mất mát
- Bảo vệ tổ chức khỏi những người dùng bên trong và bên ngoài "độc hại“
- Thiết lập các hướng dẫn việc thực hiện và sử dụng chính sách để đảm bảo tuân thủ đúng.
- Thông báo các cá nhân, tổ chức bên trong và bên ngoài thông tin đó là tài sản, tài sản riêng của tổ chức, và được bảo vệ khỏi bị truy cập trái phép, sửa đổi, tiết lộ và hủy hoại.
- Đẩy mạnh lập trường chủ động cho tổ chức khi có vấn đề pháp lý phát sinh
- Cung cấp hướng nâng cấp các tiêu chuẩn an toàn trong và ngoài tổ chức

Đối tượng áp dụng ISP

- Người quản lý – tất cả các cấp độ
- Nhân viên kỹ thuật – người quản trị hệ thống, …
- Người dùng cuối – tất cả các người dùng dịch vụ của hệ thống

CÁC THÀNH PHẦN CỦA CHÍNH SÁCH ATTT

1) **Phạm vi**
2) **Phân loại thông tin**
3) **Mục tiêu quản lý**
4) **Bối cảnh**
5) **Tài Liệu hỗ trợ**
6) **Hướng dẫn cụ thể**
7) **Có trách nhiệm rõ ràng**
8) **Hậu quả và xử lý**

CÁC THÀNH PHẦN CỦA CHÍNH SÁCH ATTT

1) Phạm vi

Đảm bảo phạm vi cần giải quyết tất cả các thông tin trong hệ thống, các chương trình, dữ liệu, mạng nội bộ và tất cả nhân viên trong tổ chức của bạn. Ngoài ra, tổ chức có thể có những chính sách riêng về phạm vi cho từng phòng, bộ phận làm việc.

2) Phân loại thông tin

Người điều hành tổ chức cần cung cấp những định nghĩa, nội dung cụ thể về việc đảm bảo an ninh thông tin và những giải pháp bảo mật mạng thay vì "bí mật" hoặc "hạn chế".

CÁC THÀNH PHẦN CỦA CHÍNH SÁCH ATTT

3) Mục tiêu quản lý

Tổ chức cần phải đưa ra những mục tiêu rõ ràng trong quản lý và xử lý, khắc phục các sự cố liên quan tới an toàn thông tin trong từng phân loại (ví dụ các nghĩa vụ pháp lý, quy định và hợp đồng đối với việc đảm bảo an ninh).

4) Bối cảnh

Một chính sách an toàn thông tin phải được đặt trong trong bối cảnh cụ thể, có hướng dẫn quản lý và tài liệu bổ sung theo sát bối cảnh (ví dụ: được tất cả các cấp quản lý chấp thuận, tất cả các tài liệu xử lý thông tin khác phải phù hợp với nó).

CÁC THÀNH PHẦN CỦA CHÍNH SÁCH ATTT

5) Tài liệu hỗ trợ

Bao gồm các tài liệu hỗ trợ (ví dụ: vai trò và trách nhiệm, quá trình, tiêu chuẩn công nghệ, thủ tục, hướng dẫn, cách khắc phục và ứng cứu sự cố).

6) Hướng dẫn cụ thể

Bao gồm các tài liệu hướng dẫn về phương pháp an ninh cho hệ thống nội bộ, phương pháp sử dụng internet an toàn trên mạng xã hội hay những yêu cầu trong bảo mật cho toàn bộ tổ chức (ví dụ: tất cả quyền truy cập vào bất kỳ hệ thống máy tính đều phải yêu cầu xác minh danh tính và xác thực, không chia sẻ cơ chế xác thực cá nhân).

CÁC THÀNH PHẦN CỦA CHÍNH SÁCH ATTT

7) Có trách nhiệm rõ ràng

Bao gồm các tài liệu hướng dẫn về phương pháp an ninh cho hệ thống nội bộ, phương pháp sử dụng internet an toàn trên mạng xã hội hay những yêu cầu trong bảo mật cho toàn bộ tổ chức (ví dụ: tất cả quyền truy cập vào bất kỳ hệ thống máy tính đều phải yêu cầu xác minh danh tính và xác thực, không chia sẻ cơ chế xác thực cá nhân).

8) Hậu quả và xử lý

Bao gồm các hậu quả cho sự không tuân thủ theo chính sách an toàn thông tin của tổ chức (ví dụ sa thải hoặc chấm dứt hợp đồng làm việc).

NGUYÊN TẮC XÂY DỰNG CHÍNH SÁCH ATTT

- **Nguyên tắc CIA:** Là nguyên tắc đảm bảo đủ 3 tính chất của việc bảo vệ thông tin là tính bảo mật (Confidentiality); tính sẵn sàng (Availability); tính nguyên vẹn và tính không thể từ chối (Integrity and non – repudiation).
- **Nguyên tắc 3A (Authentication, Authorization, Accounting)**: cho phép các chuyên viên bảo mật biết được biết được các thông tin quan trọng về tình hình cũng như mức độ an toàn trong mạng, đồng thời có thể xác thực – phân quyền – tính toán;

NGUYÊN TẮC XÂY DỰNG HỆ THỐNG ATTT

- **Nguyên tắc giá trị thông tin:** Trong các hệ thống, bạn không thể đảm bảo rằng có thể bảo mật tuyệt đối tất cả các thông tin. Bởi thế, bạn cần phân chia cấp độ thông tin dựa trên mức độ quan trọng để có kế hoạch xây dựng hệ thống bảo mật phù hợp.
- **Nguyên tắc đặc quyền tối thiểu:** Nguyên tắc này quy định rằng một chủ thể chỉ nên có đặc quyền cần thiết để thực hiện nhiệm vụ của mình mà không nên được cấp các quyền bổ sung không cần thiết. Việc này sẽ giúp hạn chế sự rò rỉ thông tin không cần thiết.

Vòng đời của chính sách an toàn thông tin

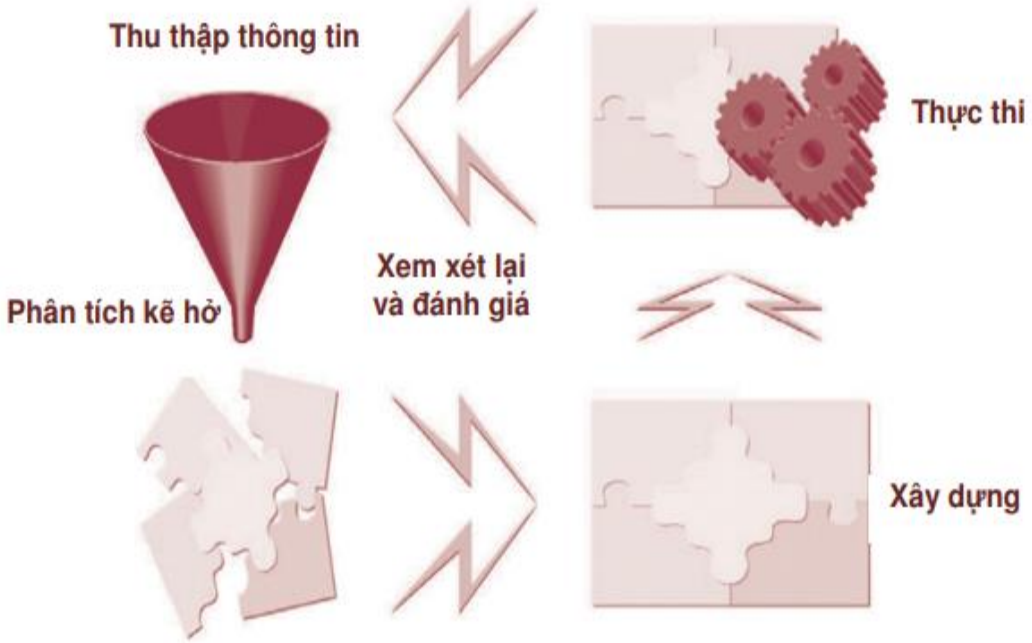
- Vòng đời của chính sách an toàn thông tin có thể được chia thành 4 giai đoạn:

(1) Thu thập thông tin và phân tích kẽ hở;

(2) Xây dựng chính sách;

(3) Thực thi chính sách;

(4) Kiểm soát và tiếp nhận phản hồi



Vòng đời của chính sách an toàn thông tin

(1) Thu thập thông tin

Thu thập thông tin sau từ nước ngoài:

- Mức độ an toàn thông tin của các quốc gia
- Định hướng xây dựng chính sách của các quốc gia
- Hệ thống hạ tầng của các quốc gia

Vòng đời của chính sách an toàn thông tin

(1) Thu thập thông tin

- Thu thập các dữ liệu trong nước: tiến hành thu thập, phân tích và đánh giá tất cả những luật pháp, quy định và chính sách có liên quan đến an toàn thông tin.

Vòng đời của chính sách an toàn thông tin

(1) Thu thập thông tin

- Thông tin về việc xây dựng và vận hành của các tổ chức liên quan đến an toàn thông tin.
- Thông tin về các chính sách, luật pháp, và các quy định về an toàn.
- Phương pháp an toàn thông tin được sử dụng trên phạm vi quốc tế.
- Các xu hướng đe dọa và những biện pháp đối phó hay kiểm soát theo các loại hình tấn công.
- Các biện pháp đối phó cho việc bảo vệ bí mật riêng tư.

Vòng đời của chính sách an toàn thông tin

(1) Phân tích kẽ hở;

- Phân tích kẽ hở có thể được chia thành hai giai đoạn:

1. Nắm bắt được các năng lực và khả năng của quốc gia – ví dụ như các nguồn lực con người và tổ chức, cũng như cơ sở hạ tầng thông tin và truyền thông – trong lĩnh vực an toàn thông tin;

2. Xác định các mối đe dọa từ bên ngoài đối với an toàn thông tin. Những nhà hoạch định chính sách cần biết rõ các nguồn lực con người và tổ chức an toàn thông tin – ví dụ các cơ quan tư nhân và công cộng trong các lĩnh vực liên quan đến an toàn thông tin.

Vòng đời của chính sách an toàn thông tin

(1) Phân tích kẽ hở;

- Xác định các mối đe dọa bên ngoài đối với an toàn thông tin.
  - Tốc độ thâm nhập của các mối đe dọa đối với an toàn thông tin
  - Các loại hình tấn công hiện tại và phổ biến nhất
  - Các loại hình đe dọa và mức độ phát triển của chúng trong tương lai.
  - Tìm ra những nguyên nhân từ các yếu tố có thể bị tấn công.

Vòng đời của chính sách an toàn thông tin

(1) Thu thập thông tin và phân tích kẽ hở;

- Việc xác định có thể được thực hiện thông qua kiểm tra những vấn đề sau đây:
  - Hiện trạng của hệ thống ATTT và khả năng đối phó của nó
  - Hiện trạng của các chuyên gia về an toàn thông tin
  - Mức độ xây dựng và sức mạnh của hệ thống an toàn thông tin
  - Quy phạm pháp luật bảo vệ chống lại sự xâm phạm tài sản thông tin
  - Môi trường vật lý cho việc bảo vệ các tài sản thông tin

Mục tiêu của việc phân tích kẽ hở là nhằm có thể xác định các biện pháp đối phó thực tiễn cần được thực hiện. Cần nhấn mạnh rằng đây là bước cơ bản nhất trong việc hoạch định chính sách an toàn thông tin.

Vòng đời của chính sách an toàn thông tin

(2) Xây dựng chính sách an toàn thông tin: Việc xây dựng một chính sách an toàn thông tin liên quan tới:

(1) Vạch ra định hướng chính sách;

(2) Thiết lập tổ chức an toàn thông tin và xác định trách nhiệm cũng như vai trò của nó;

(3) Kết nối khuôn khổ chính sách an toàn thông tin;

(4) Xây dựng và/hoặc sửa lại luật pháp giúp tạo cho chúng sự thích hợp với chính sách;

(5) Phân bổ một nguồn ngân sách cho việc thực hiện chính sách thông tin.

Vòng đời của chính sách an toàn thông tin

2. **Thiết lập khuôn khổ cho chính sách an toàn thông tin**

- Khuôn khổ an toàn thông tin đề ra những tham số đối với chính sách an toàn thông tin.
- Nó đảm bảo rằng chính sách đưa vào các tài nguyên IT (con người, tài liệu thông tin, phần cứng, phần mềm, các dịch vụ); phản ánh các quy tắc và pháp luật quốc tế; và thỏa mãn các nguyên tắc về tính sẵn sàng, tính bí mật, tính toàn vẹn, trách nhiệm giải trình và sự đảm bảo của thông tin.

Vòng đời của chính sách an toàn thông tin

2. Thiết lập khuôn khổ cho chính sách an toàn thông tin

Khuôn khổ an toàn thông tin

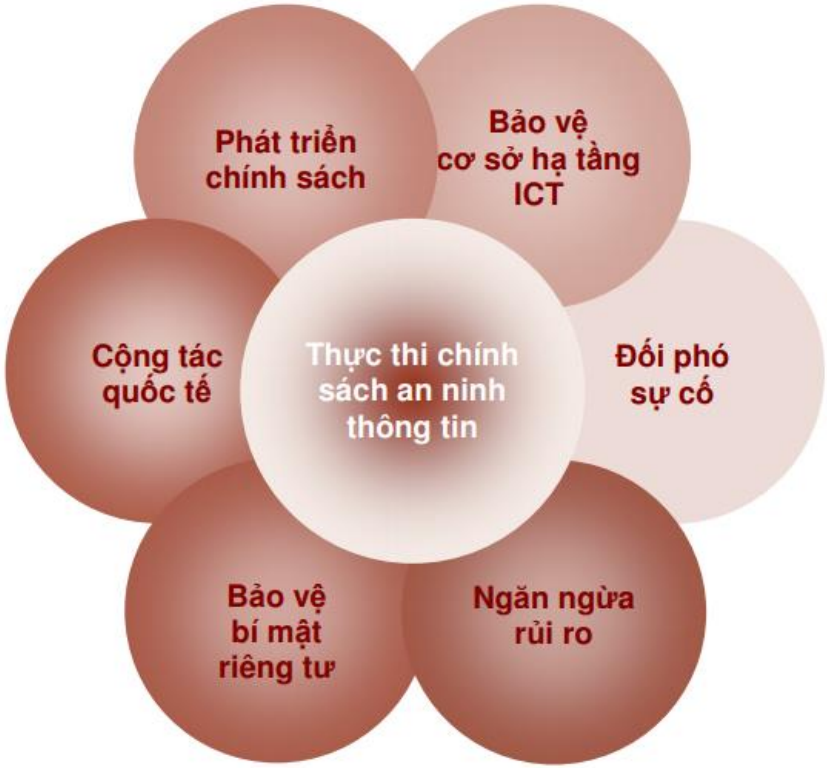
Vòng đời của chính sách an toàn thông tin

Chính sách ATTT bao gồm 5 lĩnh vực:

a. Kế hoạch và tổ chức
b. Thu nhận và thực thi: Khía cạnh này bao gồm an toàn nguồn nhân lực, thu nhận các hệ thống an toàn và phát triển an toàn.
c. Bảo vệ bí mật riêng tư
d. Hoạt động và hỗ trợ
e. Giám sát và đánh giá

Vòng đời của chính sách an toàn thông tin

3. Thực hiện/thực thi chính sách: Việc thực thi suôn sẻ chính sách an toàn thông tin đòi hỏi sự cộng tác giữa chính phủ, tư nhân và các tổ chức quốc tế

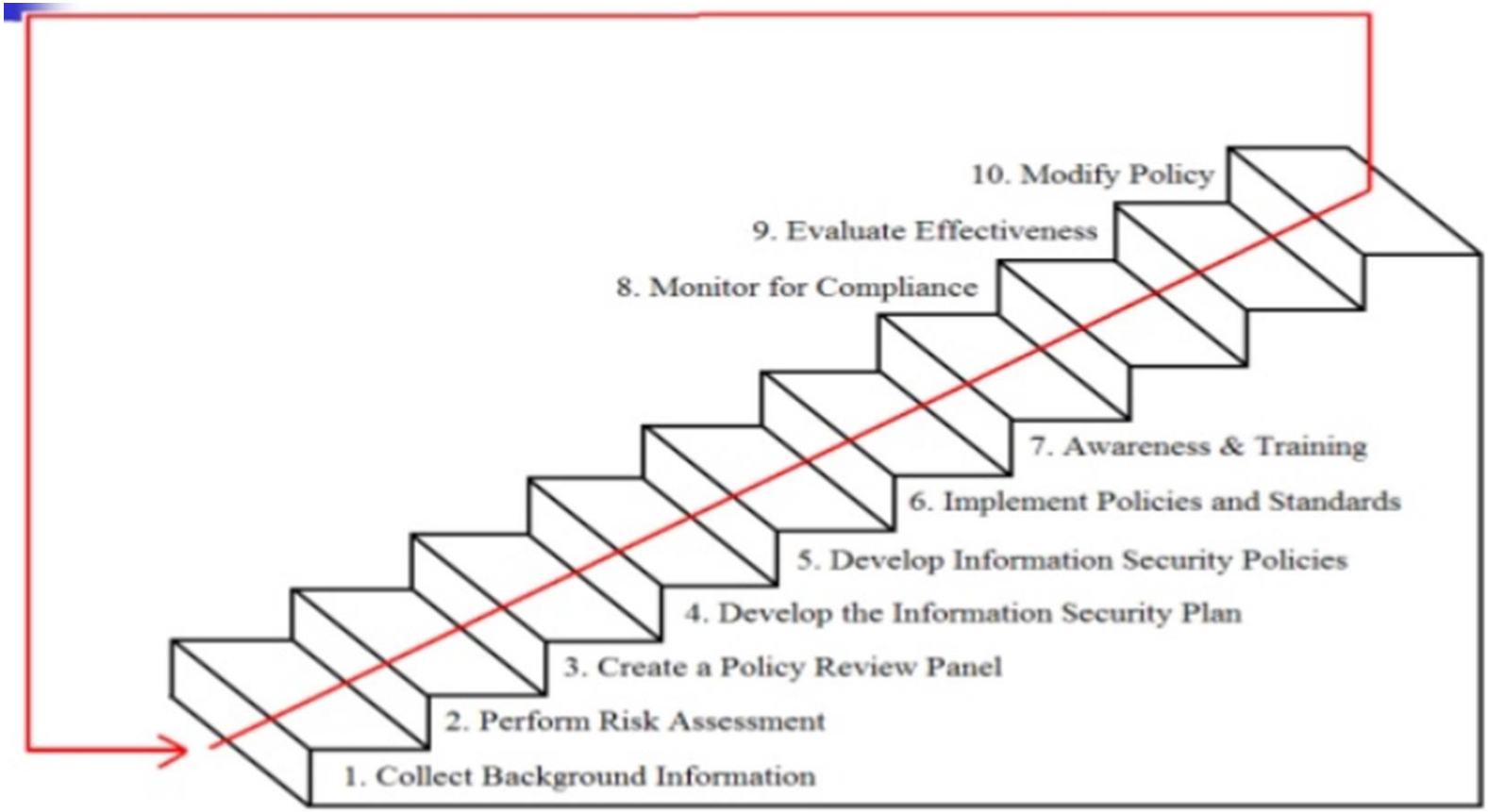


Vòng đời của chính sách an toàn thông tin

4. **Xem xét lại và đánh giá Chính sách an toàn thông tin**

- Việc sửa đổi chính sách là cần thiết sau khi hiệu quả của một chính sách an toàn thông tin được xác định. Một phương pháp đánh giá chính sách trong nước có thể được thực hiện để xác định hiệu quả của chính sách an toàn thông tin quốc gia.

Các bước triển khai IS



Nội dung của một tài liệu ISP

- Giới thiệu
- Mục đích
- Phạm vi
- Chính sách
- Vài trò và trách nhiệm
- Vi phạm và xử lý
- Lịch sửa đổi và cập nhật
- Thông tin liên hệ
- Định nghĩa/thuật ngữ

Nội dung của một tài liệu ISP

Ví dụ về chính sách an toàn thông tin

- https://www.sans.org/security-resources/policies/

Ví dụ về chính sách an toàn thông tin

Ví dụ về chính sách an toàn thông tin

Ví dụ về chính sách an toàn thông tin

Ví dụ về chính sách an toàn thông tin

Ví dụ về chính sách an toàn thông tin

Ví dụ về chính sách an toàn thông tin

Ví dụ về chính sách an toàn thông tin

Ví dụ về chính sách an toàn thông tin

THẢO LUẬN NHÓM

1. Tại sao nhân viên cần nắm rõ về Information Security Policy tại nơi làm việc?
2. Những chính sách an toàn thông tin nào ở nơi làm việc cần nắm rõ? Nêu lý do tại sao
3. Hãy viết một chính sách an toàn thông tin dành cho các sinh viên có tham gia sử dụng các trang thiết bị, phần mềm ở phòng thực hành, chính sách cài đặt các phần mềm ứng dụng, phần phòng chống mã độc cho máy tính.
4. Hãy viết một chính sách sử dụng Wifi trong một phòng ban có khoảng 20 nhân viên

Câu hỏi & Bài tập

1. Chính sách an toàn thông tin là gì? Tầm quan trọng của chính sách an toàn thông tin?
2. Là nhân viên, tại sao bạn cần nắm rõ những chính sách an toàn thông tin tại nơi bạn làm việc?
3. Hãy viết một chính sách an toàn thông tin dành cho các sinh viên có tham gia sử dụng các trang thiết bị, phần mềm ở phòng thực hành, chính sách cài đặt các phần mềm ứng dụng, phần phòng chống mã độc cho máy tính.
4. Hãy viết một chính sách sử dụng Wifi trong một phòng ban có khoảng 20 nhân viên

Câu hỏi & Bài tập

5. Chính sách an toàn thông tin (ISP) của một doanh nghiệp là gì? Trình bày và giải thích được ít nhất 3 lý do tại sao một doanh nghiệp cần có một ISP?
6. “Theo dõi sự tuân thủ (monitor for compliance)” là một trong 10 bước triển khai ISP. Bạn hãy phân tích để thấy được tại sao cần có “theo dõi sự tuân thủ” trong khi triển khai ISP của một doanh nghiệp.
7. “Hiệu chỉnh chính sách (modify policy)” là một trong 10 bước triển khai ISP. Bạn hãy phân tích để thấy được tại sao cần có “hiệu chỉnh chính sách” trong khi triển khai ISP của một doanh nghiệp.

Câu hỏi & Bài tập

Bài tập về nhà (làm theo nhóm)

- Hãy viết một chính sách an toàn thông tin/thiết bị dành cho các sinh viên/giao viên có tham gia sử dụng các trang thiết bị, phần mềm ở phòng thực hành, chính sách cài đặt các phần mềm ứng dụng, phần mềm phòng chống mã độc cho máy tính trong phòng thực hành.

Kiểm tra 15 phút

- An toàn thông tin của một doanh nghiệp là gì?
- Doanh nghiệp cần phải làm gì để đạt được an toàn thông tin và duy trì an toàn thông tin đó một cách bền vững?

THANKS YOU