# Lý thuyết 1: Xây dựng CSATTT cho một hệ thống cụ thể (1 hệ thống nhỏ hoặc 1 phần trong hệ thống, cần phải tuân thủ khuôn mẫu của CSATTT).

- Xây dựng chính sách an toàn thông tin (Information Security Policy) là một quá trình quan trọng giúp đảm bảo rằng các thông tin quan trọng của tổ chức được bảo vệ khỏi các mối đe dọa bảo mật. Dưới đây là các bước để xây dựng chính sách an toàn thông tin tuân thủ khuôn mẫu cho một hệ thống cụ thể:

- Tên chính sách và thông tin định danh:

1. Mục đích

2. Tổng quan

3. Phạm vi

4. Chính sách

5. Vai trò và trách nhiệm

6. Luật/Hướng dẫn áp dụng

7. Tính hiệu lực

8. Thông tin và hỗ trợ

9. Phê chuẩn

10.Tài liệu tham chiếu ./.

*Ví dụ như sau:*

Tên chính sách: CSATTT của công ty ABC

1. Mục đích: CSATTT của công ty ABC nhằm đảm bảo tính bảo mật và an toàn cho thông tin của công ty và khách hàng, tránh nguy cơ mất mát thông tin, ảnh hưởng đến hoạt động kinh doanh và danh tiếng của công ty.

2. Tổng quan: Chính sách này áp dụng cho tất cả các hoạt động liên quan đến thông tin của công ty ABC, bao gồm thông tin nội bộ, thông tin khách hàng, thông tin nhân viên, thông tin đối tác và các thông tin liên quan khác.

3. Phạm vi: Chính sách này bao gồm các quy định và hướng dẫn về việc quản lý, bảo mật và sử dụng thông tin, cũng như các biện pháp phòng chống các mối đe dọa về an ninh mạng và các cuộc tấn công mạng khác.

4. Chính sách: Công ty ABC cam kết thực hiện các biện pháp bảo mật thông tin bằng cách áp dụng các tiêu chuẩn và quy trình bảo mật thông tin hiện đại, đảm bảo tính bảo mật và an toàn cho thông tin của công ty và khách hàng.

5. Vai trò và trách nhiệm: Mỗi nhân viên và bộ phận trong công ty đều có trách nhiệm chung trong việc thực hiện chính sách an toàn thông tin. Công ty cũng có các chuyên gia bảo mật thông tin chịu trách nhiệm giám sát và đảm bảo thực hiện chính sách này.

6. Luật/Hướng dẫn áp dụng: Chính sách này tuân thủ các luật, quy định liên quan đến an ninh mạng và bảo mật thông tin.

7. Tính hiệu lực: CSATTT này có hiệu lực ngay khi được thông báo đến tất cả nhân viên trong công ty ABC.

8. Thông tin và hỗ trợ: Công ty ABC cung cấp các thông tin và hỗ trợ liên quan đến an ninh mạng và bảo mật thông tin cho nhân viên và khách hàng của mình.

9. Phê chuẩn: Chính sách này được phê chuẩn bởi Ban Giám đốc công ty ABC.

10. Tài liệu tham chiếu: Tài liệu tham chiếu cho chính sách an toàn thông tin của

công ty ABC bao gồm các hướng dẫn về bảo mật thông tin, quy định về sử dụng và truy cập thông tin, quy trình xử lý thông tin cá nhân, hướng dẫn về phát hiện và giải quyết các vấn đề an ninh mạng, cũng như các tài liệu liên quan khác.

Ngoài ra, CSATTT của công ty ABC còn bao gồm các biện pháp đảm bảo ATTT trong việc sử dụng các thiết bị di động, đảm bảo tính bảo mật của dữ liệu khi truyền qua mạng và các biện pháp xử lý các sự cố liên quan đến an ninh mạng và bảo mật thông tin.

Tất cả các nhân viên và bộ phận trong công ty ABC được yêu cầu thực hiện chính sách an toàn thông tin này trong quá trình làm việc của mình. Công ty cũng đảm bảo việc giáo dục và huấn luyện nhân viên về các quy định và biện pháp bảo mật thông tin liên quan đến công việc của họ.

Chính sách an toàn thông tin của công ty ABC được đánh giá và cập nhật định kỳ để đảm bảo tính hiệu lực và phù hợp với các thay đổi về an ninh mạng và bảo mật thông tin. Nếu có bất kỳ vấn đề an ninh mạng hay bảo mật thông tin nào xảy ra, công ty sẽ có các biện pháp khẩn cấp để đối phó và giải quyết vấn đề.

# Câu 1. Anh/Chị hãy viết chính sách an toàn thông tin cho máy tính cá nhân của nhân viên trong một tổ chức bán hàng trực tuyến.

- Tên chính sách: CSATTT cho máy tính cá nhân của nhân viên trong một tổ chức bán hàng trực tuyến.

1. Mục đích: nhằm đảm bảo tính bảo mật và an toàn thông tin của cá nhân nhân viên đó nói riêng và tổ chức cùng khách hàng nói chung, tránh nguy cơ mất mát thông tin, ảnh hưởng đến hoạt động kinh doanh và danh tiếng của tổ chức.

2. Tổng quan: CS này sẽ có thể là một công cụ để đảm bảo các dữ liệu nhạy cảm/bí mật phải được an toàn và được khóa khi không sử dụng hoặc khi nhân viên rời khỏi chỗ làm. Đây là một trong những chiến lược hàng đầu được áp dụng để hạn chế rủi ro từ những vi phạm AT. Một CS như vậy cũng có thể nâng cao nhận thức của nhân viên về việc bảo vệ thông tin nhạy cảm.

3. Phạm vi: CS này áp dụng cho tất cả các nhân viên khi dùng máy tính cá nhân trong tổ chức bán hành trực tuyến

4. Chính sách:

a. Mọi máy tính cá nhân phải được bảo vệ bằng mật khẩu mạnh và chỉ được sử dụng bởi người sở hữu hoặc nhân viên được ủy quyền.

b. Việc cài đặt và cập nhật phần mềm bảo mật cần được thực hiện định kỳ để bảo vệ chống lại các mối đe dọa mới nhất.

c. Không được phép sử dụng phần mềm trái phép hoặc không rõ nguồn gốc trên máy tính cá nhân.

d. Máy tính cá nhân không được kết nối với các mạng không an toàn hoặc không được bảo mật.

e. ....

5. Vai trò và trách nhiệm: Tất cả nhân viên phải chịu trách nhiệm tuân thủ chính sách an toàn thông tin cho máy tính cá nhân của mình. Bộ phận IT phụ trách giám sát và hỗ trợ nhân viên trong việc thực hiện chính sách này.

6. Luật/Hướng dẫn áp dụng: Chính sách này tuân thủ các luật, quy định liên quan đến bảo mật, an toàn và an ninh mạng.

7. Tính hiệu lực: CSATTT này có hiệu lực ngay khi được thông báo đến tất cả nhân viên dùng máy tính cá nhân trong tổ chức bán hàng trực tuyến.

8. Thông tin và hỗ trợ: Tổ chức bán hàng trực tuyến cung cấp thông tin và hỗ trợ liên quan đến an ninh mạng và bảo mật thông tin cho nhân viên.

9. Phê chuẩn: Chính sách này được phê chuẩn bởi Ban Giám đốc tổ chức bán hàng trực tuyến.

10. Tài liệu tham chiếu: Tài liệu tham chiếu cho chính sách an toàn thông tin của tổ chức bán hàng trực tuyến bao gồm các hướng dẫn về an toàn thông tin, quy định về sử dụng và truy cập thông tin, quy trình xử lý thông tin cá nhân, hướng dẫn về phát hiện và giải quyết các vấn đề an ninh mạng, cũng như các tài liệu liên quan khác.

# Câu 2. Anh/chị hãy viết chính sách ATTT cho máy chủ ứng dụng web

Tên chính sách: Chính sách An toàn Thông tin cho Máy chủ Ứng dụng Web

1. **Mục đích:**

Mục đích của chính sách này là thiết lập các biện pháp an ninh nhằm bảo vệ máy chủ ứng dụng web khỏi các truy cập trái phép, sử dụng trái phép, thay đổi hoặc phá hủy thông tin, cũng như các mối đe dọa khác đối với an ninh thông tin.

1. Tổng quan:

CS này sẽ có thể là một công cụ để đảm bảo an toàn cho máy chủ web. Đây là một trong những chiến lược hàng đầu được áp dụng để hạn chế rủi ro từ những vi phạm AT.

1. **Phạm vi:**

Chính sách này áp dụng cho tất cả máy chủ ứng dụng web được sử dụng để lưu trữ hoặc xử lý dữ liệu của tổ chức.

1. Chính sách:

* Chỉ những người dùng được ủy quyền mới được phép truy cập vào máy chủ ứng dụng web.
* Mật khẩu người dùng phải mạnh và được thay đổi thường xuyên.
* Máy chủ ứng dụng web phải được đặt trong mạng riêng biệt và được bảo vệ bằng tường lửa.
* Phần mềm chống virus và phần mềm độc hại phải được cài đặt và cập nhật thường xuyên.
* Nhân viên phải được đào tạo để biết cách nhận dạng và báo cáo các sự cố an ninh thông tin.

…..

1. **Vai trò và Trách nhiệm:**

**Ban lãnh đạo:** Chịu trách nhiệm ban hành và thực thi chính sách này.

**Bộ phận IT:** Chịu trách nhiệm triển khai và duy trì các biện pháp an ninh cho máy chủ ứng dụng web.

**Người dùng:** Chịu trách nhiệm tuân thủ các quy định của chính sách này.

1. Luật/Hướng dẫn sử dụng: Chính sách này tuân thủ các luật, quy định liên quan đến bảo mật, an toàn và an ninh mạng
2. Tính hiệu lực: Chính sách này có hiệu lực ngay khi được thông báo đến tất cả các cá nhân dùng hệ thống
3. Thông tin và hỗ trợ: cung cấp thông tin và hỗ trợ liên quan đến an ninh mạng và bảo mật thông tin cho nhân viên
4. Phê chuẩn: Chính sách được phê duyệt bởi ban lãnh đạo
5. Tài liệu tham chiếu: Tài liệu tham chiếu cho chính sách an toàn thông tin bao gồm các hướng dẫn về an toàn thông tin, quy định về sử dụng và truy cập thông tin, quy trình xử lý thông tin cá nhân, hướng dẫn về phát hiện và giải quyết các vấn đề an ninh mạng, cũng như các tài liệu liên quan khác.

# Câu 3: Anh/chị hãy viết chính sách ATTT cho máy chủ cơ sở dữ liệu

Tên chính sách: Chính sách An toàn Thông tin cho Máy chủ cơ sở dữ liệu

1. **Mục đích:**

Mục đích của chính sách này là thiết lập các biện pháp an ninh nhằm bảo vệ máy chủ cơ sở dữ liệu khỏi truy cập trái phép, sử dụng trái phép, thay đổi hoặc phá hủy dữ liệu, cũng như các mối đe dọa khác đối với an ninh thông tin.

1. Tổng quan:

CS này sẽ có thể là một công cụ để đảm bảo an toàn cho máy chủ web. Đây là một trong những chiến lược hàng đầu được áp dụng để hạn chế rủi ro từ những vi phạm AT.

1. **Phạm vi:**

Chính sách này áp dụng cho tất cả máy chủ cơ sở dữ liệu được sử dụng để lưu trữ hoặc xử lý dữ liệu của tổ chức.

1. Chính sách:

* Chỉ những người dùng được ủy quyền mới được phép truy cập vào máy chủ cơ sở dữ liệu
* Phần mềm chống virus và phần mềm độc hại phải được cài đặt và cập nhật thường xuyên.
* Do tính chất nhạy cảm của dữ liệu được lưu trữ trên máy chủ cơ sở dữ liệu, phải được triển khai:Mã hóa dữ liệu, Ghi nhật ký và theo dõi,..
* Nhân viên phải được đào tạo để biết cách nhận dạng và báo cáo các sự cố an ninh thông tin.

…..

1. **Vai trò và Trách nhiệm:**

**Ban lãnh đạo:** Chịu trách nhiệm ban hành và thực thi chính sách này.

**Bộ phận IT:** Chịu trách nhiệm triển khai và duy trì các biện pháp an ninh cho máy chủ ứng dụng web.

**Người dùng:** Chịu trách nhiệm tuân thủ các quy định của chính sách này.

1. Luật/Hướng dẫn sử dụng: Chính sách này tuân thủ các luật, quy định liên quan đến bảo mật, an toàn và an ninh mạng
2. Tính hiệu lực: Chính sách này có hiệu lực ngay khi được thông báo đến tất cả các cá nhân dùng hệ thống
3. Thông tin và hỗ trợ: cung cấp thông tin và hỗ trợ liên quan đến an ninh mạng và bảo mật thông tin cho nhân viên
4. Phê chuẩn: Chính sách được phê duyệt bởi ban lãnh đạo
5. Tài liệu tham chiếu: Tài liệu tham chiếu cho chính sách an toàn thông tin bao gồm các hướng dẫn về an toàn thông tin, quy định về sử dụng và truy cập thông tin, quy trình xử lý thông tin cá nhân, hướng dẫn về phát hiện và giải quyết các vấn đề an ninh mạng, cũng như các tài liệu liên quan khác.

# Câu 4: Anh/chị hãy viết chính sách ATTT cho máy chủ ứng dụng tác nghiệp nội bộ của tổ chức. ( tương tự câu 1)

# Câu 5: Chính sách cho bàn làm việc sạch sẽ cho các nhân viên trong công ty

Tên chính sách: Chính sách bàn làm việc sạch sẽ trong công ty ABC

1. **Mục đích:**

Mục đích của chính sách này là thiết lập các tiêu chuẩn và quy trình để duy trì một môi trường làm việc sạch sẽ, an toàn và hiệu quả cho tất cả nhân viên.

1. Tổng quan:

Chính sách này đẩm bảo việc thiết lập quy định để duy trì môi trường làm việc sạch sẽ. Nâng cao nhận thức của nhân viên về việc bảo vệ môi trường

1. **Phạm vi:**

Chính sách này áp dụng cho tất cả nhân viên trong công ty

1. Chính sách:

* Bàn làm việc phải được dọn dẹp gọn gàng vào cuối mỗi ngày làm việc.
* Tất cả rác thải phải được vứt vào thùng rác.
* Bàn làm việc phải được lau chùi bằng chất khử trùng ít nhất một lần mỗi tuần.
* Sàn nhà xung quanh bàn làm việc phải được quét và lau chùi sạch sẽ.
* Các vật dụng cá nhân phải được cất giữ trong tủ hoặc ngăn kéo.
* Thức ăn và đồ uống không được phép để trên bàn làm việc.
* Khuyến khích nhân viên cá nhân hóa bàn làm việc của họ bằng cách thêm một vài bức ảnh hoặc cây cảnh nhỏ.

…..

1. **Vai trò và Trách nhiệm:**

**Tất cả nhân viên phải có trách nhiệm**  giữ cho bàn làm việc của mình sạch sẽ và ngăn nắp.

1. Luật/Hướng dẫn sử dụng: Chính sách này tuân thủ các luật, quy định liên quan đến bảo mật, an toàn và an ninh mạng
2. Tính hiệu lực: Chính sách này có hiệu lực ngay khi được thông báo đến tất cả các nhân viên trong công ty
3. Thông tin và hỗ trợ:
4. Phê chuẩn: Chính sách được phê duyệt bởi ban lãnh đạo
5. Tài liệu tham chiếu:

# Câu 6: Chính sách mật khẩu mạnh

-Tên chính sách: Chính sách mật khẩu mạnh cho hệ thống

1. Mục đích: nhằm thiết lập các yêu cầu tối thiểu về độ mạnh của mật khẩu để bảo vệ tài khoản người dùng và hệ thống khỏi truy cập trái phép.

2. Tổng quan

Chính sách áp dụng cho tất cả các hoạt động liên quan đến hệ thống. Chính sách sẽ là công cụ đảm bảo việc an toàn mật khẩu giúp đảm bảo rủi ro vi phạm AT

3. Phạm vi: Chính sách này áp dụng cho tất cả người dùng hệ thống, bao gồm nhân viên, nhà thầu và khách hàng.

* 4.Chính sách
* Mật khẩu phải dài ít nhất 12 ký tự.
* Mật khẩu phải chứa ít nhất một chữ cái viết hoa, một chữ cái viết thường, một số và một ký tự đặc biệt.
* Mật khẩu không được dựa trên từ điển hoặc chuỗi ký tự dễ đoán.
* Mật khẩu không được sử dụng cho nhiều tài khoản.
* Thay đổi mật khẩu thường xuyên, ít nhất mỗi 6 tháng một lần.
* Không bao giờ chia sẻ mật khẩu với bất kỳ ai khác.
* Cẩn thận với các email lừa đảo yêu cầu bạn nhập mật khẩu của mình.

5. Vai trò và trách nhiệm: Tất cả người dùng hệ thống đều phải chịu trách nhiệm tuân thủ chính sách mật khẩu mạnh. Bộ phận IT Sử dụng trình quản lý mật khẩu để tạo và lưu trữ mật khẩu mạnh.

6. Luật/ hướng dẫn áp dụng: Chính sách này tuân thủ các luật, quy định liên quan đến bảo mật, an toàn và an ninh mạng

7. Tính hiệu lực: Chính sách này có hiệu lực ngay khi được thông báo đến tất cả các cá nhân dùng hệ thống

8. Thông tin và hỗ trợ: cung cấp thông tin và hỗ trợ liên quan đến an ninh mạng và bảo mật thông tin cho nhân viên

9. Phê chuẩn: Chính sách được phê chuẩn bởi ban giám đốc

10. Tài liệu tham chiếu:

# Câu 7. Chính sách về bảo mật thông tin khách hàng trong giao dịch thương mại điện tử

Tên chính sách: Chính sách bảo mật thông tin khách hàng trong giao dịch thương mại điện tử

1. **Mục đích:**

Mục đích của chính sách này là thiết lập các nguyên tắc và quy trình để bảo vệ thông tin cá nhân của khách hàng trong các giao dịch thương mại điện tử, đảm bảo quyền riêng tư và an toàn cho khách hàng khi sử dụng các dịch vụ thương mại điện tử do tổ chức cung cấp

1. Tổng quan:

CS này sẽ có thể là một công cụ để đảm bảo các dữ liệu nhạy cảm/bí mật phải được an toàn cho dữ liệu người dùng. Đây là một trong những chiến lược hàng đầu được áp dụng để hạn chế rủi ro từ những vi phạm AT.

1. **Phạm vi:**

Chính sách này áp dụng cho tất cả các hoạt động thu thập, sử dụng, lưu trữ và truyền tải thông tin cá nhân của khách hàng trong các giao dịch thương mại điện tử trên website và ứng dụng di động của tổ chức.

1. Chính sách:

+ Thu thập thông tin cá nhân của khách hàng một cách hợp pháp, minh bạch và chính đáng.

+ Lưu trữ thông tin cá nhân của khách hàng an toàn và bảo mật.

+ Không tiết lộ thông tin cá nhân của khách hàng cho bên thứ ba mà không có sự đồng ý của khách hàng.

+ Tổ chức chỉ thu thập thông tin cá nhân của khách hàng cần thiết cho mục đích cung cấp dịch vụ thương mại điện tử.

+ Khách hàng có quyền từ chối cung cấp thông tin cá nhân, tuy nhiên việc này có thể ảnh hưởng đến khả năng sử dụng một số dịch vụ nhất định.

1. **Vai trò và Trách nhiệm:**

Tất cả người dùng phải chịu trách nhiệm tuân thủ chính sách an toàn thông tin cho thông tin của mình mình. Bộ phận IT phụ trách giám sát và hỗ trợ nhân người dùng trong việc thực hiện chính sách này.

1. Luật/Hướng dẫn sử dụng: Chính sách này tuân thủ các luật, quy định liên quan đến bảo mật, an toàn và an ninh mạng
2. Tính hiệu lực: Chính sách này có hiệu lực ngay khi được thông báo đến tất cả các cá nhân dùng giao dịch thương mại diện tử
3. Thông tin và hỗ trợ: cung cấp thông tin và hỗ trợ liên quan đến an ninh mạng và bảo mật thông tin cho người dùng
4. Phê chuẩn: Chính sách được phê duyệt bởi ban lãnh đạo
5. Tài liệu tham chiếu: Tài liệu tham chiếu cho chính sách an toàn thông tin bao gồm các hướng dẫn về an toàn thông tin, quy định về sử dụng và truy cập thông tin, quy trình xử lý thông tin cá nhân, hướng dẫn về phát hiện và giải quyết các vấn đề an ninh mạng, cũng như các tài liệu liên quan khác.

# Câu 8. Chính sách về sử dụng email trong tổ chức

Tên chính sách: Chính sách An toàn sử dụng email trong tổ chức

1. **Mục đích:**

Mục đích của chính sách này là thiết lập các nguyên tắc và quy định về việc sử dụng email trong tổ chức, đảm bảo hiệu quả hoạt động, an ninh thông tin và tuân thủ các quy định pháp luật liên quan.

1. Tổng quan:

CS này sẽ có thể là một công cụ để đảm bảo an toàn việc sử dụng email trong tổ chức. Đây là một trong những chiến lược hàng đầu được áp dụng để hạn chế rủi ro từ những vi phạm AT.

1. **Phạm vi:**

Chính sách này áp dụng cho tất cả cán bộ, nhân viên, cộng tác viên đang làm việc tại tổ chức và sử dụng hệ thống email của tổ chức.

1. Chính sách:

* **Sử dụng email cho mục đích công việc:**
* Cán bộ, nhân viên phải bảo mật thông tin cá nhân, thông tin của tổ chức và khách hàng khi sử dụng email.
* Sử dụng mật khẩu mạnh và giữ bí mật mật khẩu email.
* Cẩn trọng khi mở tệp đính kèm, nhấp vào liên kết trong email từ người lạ hoặc nguồn không xác định.
* Cẩn trọng khi mở tệp đính kèm, nhấp vào liên kết trong email từ người lạ hoặc nguồn không xác định.
* Tổ chức có thể tổ chức các khóa đào tạo về sử dụng email hiệu quả cho cán bộ, nhân viên.
* Tổ chức có thể triển khai các công cụ quản lý email để kiểm soát việc sử dụng email và bảo mật thông tin.

…..

1. **Vai trò và Trách nhiệm:**

Ban lãnh đạo: Chịu trách nhiệm ban hành, tuyên truyền và thực thi chính sách này.

Bộ phận IT: Chịu trách nhiệm quản lý hệ thống email, cung cấp hướng dẫn sử dụng và hỗ trợ kỹ thuật cho người dùng.

Cán bộ, nhân viên: Chịu trách nhiệm tuân thủ các quy định của chính sách này trong việc sử dụng email.

1. Luật/Hướng dẫn sử dụng: Chính sách này tuân thủ các luật, quy định liên quan đến bảo mật, an toàn và an ninh mạng
2. Tính hiệu lực: Chính sách này có hiệu lực ngay khi được thông báo đến tất cả các nhân viên sử dụng email
3. Thông tin và hỗ trợ: cung cấp thông tin và hỗ trợ liên quan đến an ninh mạng và bảo mật thông tin cho nhân viên
4. Phê chuẩn: Chính sách được phê duyệt bởi ban lãnh đạo
5. Tài liệu tham chiếu: Tài liệu tham chiếu cho chính sách an toàn thông tin bao gồm các hướng dẫn về an toàn thông tin, quy định về sử dụng và truy cập thông tin, quy trình xử lý thông tin cá nhân, hướng dẫn về phát hiện và giải quyết các vấn đề an ninh mạng, cũng như các tài liệu liên quan khác.

# Câu 9. Chính sách về sao lưu phục hồi

Tên chính sách: Chính sách An toàn về sao lưu phục hồi

1. **Mục đích:**

Mục đích của chính sách này là thiết lập các quy trình và thủ tục để sao lưu và phục hồi dữ liệu một cách hiệu quả, đảm bảo tính sẵn sàng, an toàn và bảo mật cho dữ liệu của tổ chức.

1. Tổng quan:

CS này sẽ có thể là một công cụ để đảm bảo an toàn việc sử dụng sao lưu phục hồi dữ liệu trong tổ chức. Đây là một trong những chiến lược hàng đầu được áp dụng để hạn chế rủi ro từ những vi phạm AT.

1. **Phạm vi:**

Chính sách này áp dụng cho tất cả dữ liệu điện tử được tạo ra, sử dụng và lưu trữ trong hệ thống thông tin của tổ chức, bao gồm dữ liệu ứng dụng, dữ liệu hệ thống và dữ liệu cá nhân.

1. Chính sách:
   * Lập lịch sao lưu dữ liệu thường xuyên theo tần suất phù hợp với mức độ quan trọng của dữ liệu và nhu cầu sử dụng.
   * Nên kết hợp sử dụng nhiều phương pháp sao lưu để đảm bảo an toàn chodữ liệu:  sao lưu cục bộ, sao lưu ngoại tuyến, sao lưu đám mây.
   * Lưu trữ bản sao lưu dữ liệu ở nơi an toàn, tránh xa các mối nguy hiểm tiềm ẩn như hỏa hoạn, lũ lụt, trộm cắp.
   * Thực hiện thử nghiệm phục hồi dữ liệu định kỳ để đảm bảo hệ thống sao lưu và phục hồi hoạt động hiệu quả.
   * Tổ chức có thể đầu tư vào các giải pháp sao lưu và phục hồi dữ liệu tự động để tiết kiệm thời gian và công sức cho cán bộ, nhân viên.
   * Tổ chức có thể tổ chức các khóa đào tạo về sao lưu và phục hồi dữ liệu cho cán bộ, nhân viên để nâng cao nhận thức và kỹ năng sử dụng hệ thống.

…..

1. **Vai trò và Trách nhiệm:**

Ban lãnh đạo: Chịu trách nhiệm ban hành, tuyên truyền và thực thi chính sách này.

Bộ phận IT: Chịu trách nhiệm triển khai, vận hành và duy trì hệ thống sao lưu và phục hồi dữ liệu.

Cán bộ, nhân viên: Chịu trách nhiệm tuân thủ các quy định của chính sách này trong việc sử dụng hệ thống sao lưu và phục hồi dữ liệu.

1. Luật/Hướng dẫn sử dụng: Chính sách này tuân thủ các luật, quy định liên quan đến bảo mật, an toàn và an ninh mạng
2. Tính hiệu lực: Chính sách này có hiệu lực ngay khi được thông báo đến tất cả các nhân viên về việc sao lưu phục hồi dữ liệu
3. Thông tin và hỗ trợ: cung cấp thông tin và hỗ trợ liên quan đến an ninh mạng và bảo mật thông tin cho nhân viên
4. Phê chuẩn: Chính sách được phê duyệt bởi ban lãnh đạo
5. Tài liệu tham chiếu: Tài liệu tham chiếu cho chính sách an toàn thông tin bao gồm các hướng dẫn về an toàn thông tin, quy định về sử dụng và truy cập thông tin, quy trình xử lý thông tin cá nhân, hướng dẫn về phát hiện và giải quyết các vấn đề an ninh mạng, cũng như các tài liệu liên quan khác.

# Câu 10. Chính sách về trao đổi thông tin

Tên chính sách: Chính sách An toàn trao đổi thông tin

1. **Mục đích:**

Mục đích của chính sách này là thiết lập các nguyên tắc và quy trình để trao đổi thông tin một cách hiệu quả, minh bạch và chính xác trong tổ chức, đảm bảo sự phối hợp, hợp tác và ra quyết định hiệu quả.

1. Tổng quan:

CS này sẽ có thể là một công cụ để đảm bảo an toàn trao đổi thông tintrong tổ chức. Đây là một trong những chiến lược hàng đầu được áp dụng để hạn chế rủi ro từ những vi phạm AT.

1. **Phạm vi:**

Chính sách này áp dụng cho tất cả cán bộ, nhân viên, cộng tác viên đang làm việc tại tổ chức và tham gia vào các hoạt động trao đổi thông tin..

1. Chính sách:

* **Trao đổi thông tin một cách cởi mở và minh bạch:**
* Sử dụng các kênh giao tiếp nội bộ như email, tin nhắn nội bộ, bảng tin, hội nghị trực tuyến,... để trao đổi thông tin nội bộ.
* Sử dụng các biện pháp bảo mật phù hợp để bảo vệ thông tin khỏi truy cập trái phép, sử dụng hoặc tiết lộ.
* Sử dụng hệ thống lưu trữ thông tin an toàn và tin cậy.
* Tổ chức có thể tổ chức các khóa đào tạo về kỹ năng giao tiếp và trao đổi thông tin cho cán bộ, nhân viên để nâng cao hiệu quả trao đổi thông tin.

…..

1. **Vai trò và Trách nhiệm:**

Ban lãnh đạo: Chịu trách nhiệm ban hành, tuyên truyền và thực thi chính sách này.

Bộ phận Truyền thông: Chịu trách nhiệm quản lý hệ thống thông tin nội bộ, website và các kênh truyền thông của tổ chức.

Cán bộ, nhân viên: Chịu trách nhiệm tuân thủ các quy định của chính sách này trong việc trao đổi thông tin.

1. Luật/Hướng dẫn sử dụng: Chính sách này tuân thủ các luật, quy định liên quan đến bảo mật, an toàn và an ninh mạng
2. Tính hiệu lực: Chính sách này có hiệu lực ngay khi được thông báo đến tất cả các nhân viên về việc trao đổi thông tin
3. Thông tin và hỗ trợ: cung cấp thông tin và hỗ trợ liên quan đến an ninh mạng và bảo mật thông tin cho nhân viên
4. Phê chuẩn: Chính sách được phê duyệt bởi ban lãnh đạo
5. Tài liệu tham chiếu: Tài liệu tham chiếu cho chính sách an toàn thông tin bao gồm các hướng dẫn về an toàn thông tin, quy định về sử dụng và truy cập thông tin, quy trình xử lý thông tin cá nhân, hướng dẫn về phát hiện và giải quyết các vấn đề an ninh mạng, cũng như các tài liệu liên quan khác.

# Câu 11. Chính sách bảo mật nhân sự

Tên chính sách: Chính sách An toàn bảo mật nhân sự

1. **Mục đích:**

Mục đích của chính sách này là thiết lập các nguyên tắc và quy trình để bảo vệ thông tin nhân sự của cán bộ, nhân viên, đảm bảo quyền riêng tư và an toàn cho dữ liệu cá nhân của họ, phù hợp với các quy định của pháp luật lao động và luật bảo mật thông tin.

1. Tổng quan:

CS này sẽ có thể là một công cụ để đảm bảo an toàn việc bảo mật thông tin nhân sự. Đây là một trong những chiến lược hàng đầu được áp dụng để hạn chế rủi ro từ những vi phạm AT.

1. **Phạm vi:** CS này áp dụng cho tất cả các nhân viên trong tổ chức
2. Chính sách:
   * Thu thập thông tin nhân sự một cách hợp pháp, minh bạch và chính đáng, với sự đồng ý của cán bộ, nhân viên.
   * Chỉ sử dụng thông tin nhân sự cho mục đích đã được thu thập và đồng ý.
   * Lưu trữ thông tin nhân sự an toàn và bảo mật, áp dụng các biện pháp kỹ thuật và vật lý tiên tiến nhất để bảo vệ dữ liệu.
   * Hạn chế truy cập vào thông tin nhân sự chỉ dành cho những người có thẩm quyền.
   * Nâng cao nhận thức về bảo mật thông tin cho cán bộ, nhân viên.

…..

1. **Vai trò và Trách nhiệm:**

Ban lãnh đạo: Chịu trách nhiệm ban hành, tuyên truyền và thực thi chính sách này.

Bộ phận Nhân sự: Chịu trách nhiệm quản lý, lưu trữ và bảo mật thông tin nhân sự.

Cán bộ, nhân viên: Chịu trách nhiệm tuân thủ các quy định của chính sách này trong việc cung cấp, sử dụng và bảo mật thông tin nhân sự.

1. Luật/Hướng dẫn sử dụng: Chính sách này tuân thủ các luật, quy định liên quan đến bảo mật, an toàn và an ninh mạng
2. Tính hiệu lực: Chính sách này có hiệu lực ngay khi được thông báo đến tất cả các nhân viên về việc bảo mật nhân sự
3. Thông tin và hỗ trợ: cung cấp thông tin và hỗ trợ liên quan đến an ninh mạng và bảo mật thông tin cho nhân viên
4. Phê chuẩn: Chính sách được phê duyệt bởi ban lãnh đạo
5. Tài liệu tham chiếu: Tài liệu tham chiếu cho chính sách an toàn thông tin bao gồm các hướng dẫn về an toàn thông tin, quy định về sử dụng và truy cập thông tin, quy trình xử lý thông tin cá nhân, hướng dẫn về phát hiện và giải quyết các vấn đề an ninh mạng, cũng như các tài liệu liên quan khác.

# Lý thuyết 2: Ước lượng rủi ro cho một hệ thống

- Chú thích các chữ viết tắt:

* V: Giá trị tài sản
* P: Khả năng xuất hiện 1 điểm yếu
* RR: Rủi ro
* R: Mức độ rủi ro được giảm thiểu do các kiểm soát an toàn
* U: Mức độ rủi ro do sự không chắc chắn của các tri thức hiện tại về
* điểm yếu

**- Bước 1:** Xác định các giá trị sau:

* Giá trị của V, P và tính P\*V
* Tiếp theo tính: R = (sự kiểm soát mức độ đạt được là x%) \* PV
* Nếu mức độ không đạt được thì lấy (100% - x%)\*PV
* Không có sự kiểm soát nào thì lấy 0%\*PV
* U = (độ ước lượng không chắc chắn y%) \* PV
* Nếu độ ước lượng chắc chắn thì lấy (100% - y%)\*PV

**- Bước 2:** Tính RR cho từng điểm yếu theo công thức

RR = PV-R+U

**- Bước 3:** Thứ tự ưu tiên

Cái nào RR càng cao thì viết đầu, vd: ĐY3,ĐY1,ĐY2,...

MỤC LỤC

[Lý thuyết 1: Xây dựng CSATTT cho một hệ thống cụ thể (1 hệ thống nhỏ hoặc 1 phần trong hệ thống, cần phải tuân thủ khuôn mẫu của CSATTT). 1](#_Toc164866568)

[Câu 1. Chính sách an toàn thông tin cho máy tính cá nhân của nhân viên trong một tổ chức bán hàng trực tuyến. 3](#_Toc164866569)

[Câu 2. Chính sách ATTT cho máy chủ ứng dụng web 4](#_Toc164866570)

[Câu 3: chính sách ATTT cho máy chủ cơ sở dữ liệu 5](#_Toc164866571)

[Câu 4: Chính sách ATTT cho máy chủ ứng dụng tác nghiệp nội bộ của tổ chức. ( tương tự câu 1) 7](#_Toc164866572)

[Câu 5: Chính sách cho bàn làm việc sạch sẽ cho các nhân viên trong công ty 7](#_Toc164866573)

[Câu 6: Chính sách mật khẩu mạnh 8](#_Toc164866574)

[Câu 7. Chính sách về bảo mật thông tin khách hàng trong giao dịch thương mại điện tử 9](#_Toc164866575)

[Câu 8. Chính sách về sử dụng email trong tổ chức 10](#_Toc164866576)

[Câu 9. Chính sách về sao lưu phục hồi 12](#_Toc164866577)

[Câu 10. Chính sách về trao đổi thông tin 13](#_Toc164866578)

[Câu 11. Chính sách bảo mật nhân sự 15](#_Toc164866579)

[Lý thuyết 2: Ước lượng rủi ro cho một hệ thống 16](#_Toc164866580)