# Nội dung Lý thuyết

1. **An toàn thông tin (Information Security)**

***1. Thông tin là gì?***“Information is an asset which, like other important business assets, has value to an organization and consequently needs to be suitably protected”

Trích dẫn từ tiêu chuẩn BS ISO 27002:2005 cho thấy rằng thông tin là một tài sản, giống như các tài sản kinh doanh quan trọng khác, có giá trị đối với một tổ chức và do đó cần được bảo vệ một cách phù hợp.

*(Vì thông tin có thể ảnh hưởng đến hoạt động kinh doanh, uy tín của tổ chức, hoặc cả tài sản vật lý và nguồn lực khác, nó cần được bảo vệ chính xác như các tài sản kinh doanh khác. Điều này có nghĩa là tổ chức cần có các biện pháp bảo mật phù hợp để đảm bảo rằng thông tin không bị rò rỉ, bị thất thoát hoặc bị tấn công, từ đó giữ cho giá trị và tính toàn vẹn của thông tin được bảo vệ.)*

***Information có thể được***Tạo, lưu, xóa, xử lý, chuyển giao, sử dụng (cho đúng mục đích, sai mục đích), hư hỏng, mất, đánh cắp, in hoặc viết lên giấy, lưu trữ chuyển giao bằng cách đăng lên hoặc dùng các phương tiện điện tử, đưa vào các video, hiển thị/xuất bản,…**‘… whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected”**

Trích dẫn từ tiêu chuẩn BS ISO 27002:2005 nhấn mạnh rằng bất kể thông tin được sử dụng dưới hình thức nào hoặc bằng phương tiện nào được chia sẻ hoặc lưu trữ, thông tin đó phải luôn được bảo vệ một cách thích hợp. Điều này ám chỉ rằng dù thông tin được truyền bằng cách nào, hay được lưu trữ trên bất kỳ phương tiện nào, thì nó cũng cần phải được bảo vệ chặt chẽ để đảm bảo tính toàn vẹn và bí mật của thông tin.

**2. An toàn thông tin là gì?**An toàn thông tin (Information Security) là tập hợp các biện pháp và quy trình được thực hiện để bảo vệ thông tin khỏi các mối đe dọa, đảm bảo tính liên tục của hoạt động kinh doanh, giảm thiểu tổn thất tài chính, tối ưu hóa lợi ích từ các đầu tư liên quan đến thông tin, và tăng cơ hội kinh doanh.

- Bảo vệ thông tin từ hàng loạt các mối đe dọa- Đảm bảo tính liên tục kinh doanh- Giảm thiểu tổn thất tài chính- Tối ưu hóa lợi tức đầu tư- Tăng cơ hội kinh doanhTiêu chuẩn ISO 27002:2005 định nghĩa (ATTT)Information Security là phải duy trì 3 yếu tố chính sau đây:- Tính bí mật (Confidentiality): Thông tin chỉ được phép truy cập (đọc) bởi những đối tượng (người, chương trình máy tính,…) được cấp phép (Ai có thể thấy được thông tin?) - Tính toàn vẹn (Integrity): Thông tin chỉ được phép xóa hoặc sửa bởi những đối tượng được phép và phải đảm bảo rằng thông tin vẫn còn chính xác khi được lưu trữ hay truyền đi (Thông tin có đúng không?)- Tính sẳn dùng (Availability): thông tin có thể được truy xuất bởi những người được phép vào bất cứ khi nào họ muốn (thông tin sẳn sàng và dùng được không?)Khi xây dựng hệ thống thông tin thì cần cân bằng 3 mục tiêu này để đảm bảo tính an toàn cho thông tin.Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, hình tam giác

Mô tả được tạo tự động

- Vi phạm bảo mật thông tin có thể dẫn đến các hậu quả nghiêm trọng như: + Uy tín bị mất+ Tổn thất về tài chính+ Mất mát tài sản trí tuệ+ Vi phạm pháp luật dẫn đến hàng động pháp lý (luật CNTT)+ Mất đi lòng tin cậy của khách hàng+ Chi phí gián đoạn kinh doanh+ ….- Information Security là “Organizational Problem” hơn là “IT Problem”. Tức là thông tin an ninh là một vấn đề của tổ chức hơn là chỉ là một vấn đề công nghệ thông tin. Điều này có nghĩa là an ninh thông tin không chỉ liên quan đến việc triển khai công nghệ và biện pháp bảo mật kỹ thuật, mà còn đòi hỏi sự tham gia và sự nhận thức từ mọi thành viên trong tổ chức. Dưới đây là một số lý do:- Hơn 70% các mối đe dọa là nội bộ (internal)- Hơn 60% các thủ phạm là kể lừa đảo lần đầu tiên (First Time fraudsters)- Mối nguy hiểm lớn nhất: con người- Tài sản lớn nhất: con người- Kỹ thuật “Social Engineering” là mối đe dọa chính

**3. Rủi ro, mối đe dọa, và lổ hỏng**- Vulnerability (lỗ hỏng): một điểm yếu trong tổ chức, hệ thống IT, hoặc mạng mà có thể được khám phá bởi mối đe dọa. - Threat (mối nguy/mối đe dọa): một cái gì đó mà có thể gây thiệt hại đến tổ chức, hệ thống IT hoặc hệ thống mạng. - Risk (rủi ro): một khả năng mà một mối đe dọa khai thác lỗ hỏng trong tài sản và gây ra nguy hại hoặc mất mát đến tài sản.

Mối quan hệ giữa lổ hỏng, mối đe dọa, rủi roẢnh có chứa văn bản, hàng, biểu đồ, ảnh chụp màn hình

Mô tả được tạo tự động

**Thread (mối đe dọa) xuất phát từ đâu?-** Nhân viên**-** Các bộ phận bên ngoài**-** Sự thiếu nhận thức về các vấn đề an toàn**-** Sự phát triển việc kết nối mạng và các máy tính phân tán **-** Sự phát triển trong mức độ phức tạp và hiệu suất của các công cụ tấng công và virus **-** Thảm họa tự nhiên như cháy, lũ lụt, động đất,…

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, số

Mô tả được tạo tự động

A screenshot of a computer

Description automatically generated

**Rủi ro xuất phát từ đâu?**

Hành vi của con người: Sự bất cẩn hoặc thiếu nhận thức của nhân viên về các biện pháp an ninh thông tin có thể dẫn đến rủi ro, bao gồm việc chia sẻ mật khẩu, mở cửa sổ máy tính không an toàn, hoặc rơi vào các kỹ thuật xâm nhập xã hội (social engineering).

Phần mềm độc hại (Malware): Virus, ransomware, trojans và các loại phần mềm độc hại khác có thể lây lan qua email, các trang web không an toàn hoặc từ các thiết bị lưu trữ dữ liệu nhiễm virus.

Xâm nhập từ bên ngoài (External Intrusion): Hacker hoặc tổ chức tội phạm mạng có thể tìm cách xâm nhập vào hệ thống của một tổ chức để truy cập thông tin nhạy cảm hoặc gây hại.

Rủi ro từ bên trong (Insider Threats): Nhân viên, đối tác hoặc các bên thứ ba có quyền truy cập vào hệ thống có thể cố ý hoặc vô tình tiết lộ thông tin hoặc gây hại đến an ninh thông tin.

Thiết bị không an toàn: Sự sử dụng thiết bị không an toàn hoặc vi phạm chính sách bảo mật có thể tạo ra lỗ hổng trong hệ thống và dẫn đến việc rò rỉ thông tin.

Yếu điểm trong hệ thống và ứng dụng: Lỗ hổng bảo mật trong phần mềm hoặc hệ thống có thể bị lợi dụng để xâm nhập hoặc truy cập trái phép vào dữ liệu.

Tình trạng tự nhiên: Sự cố tự nhiên như sự cố hệ thống, hỏa hoạn, lụt lội, hoặc các sự kiện khác có thể gây mất mát dữ liệu hoặc gây ảnh hưởng đến hệ thống.

Sai phạm và vi phạm pháp luật: Vi phạm các quy định pháp luật liên quan đến bảo vệ dữ liệu cá nhân, bảo vệ quyền riêng tư và các quy định an ninh thông tin có thể dẫn đến hậu quả pháp lý và tài chính.

Các tổ chức cần nhận biết và đối phó với các nguồn rủi ro này thông qua việc triển khai các biện pháp bảo mật thích hợp và thường xuyên đánh giá và cập nhật các chiến lược an ninh thông tin của mình.

**Lỗ hổng xuất phát từ đâu?**

Lỗi phát triển phần mềm: Các lỗ hổng có thể tồn tại trong mã nguồn của phần mềm do các lỗi lập trình, thiếu sót hoặc không tuân thủ các nguyên tắc an toàn lập trình.

Cập nhật và bản vá thiếu: Việc sử dụng các phiên bản phần mềm cũ hoặc không cập nhật đúng cách có thể tạo điều kiện cho việc tấn công do các lỗ hổng đã được vá lấp trong các bản vá mới nhất.

Thiết kế không an toàn: Thiết kế hệ thống hoặc ứng dụng không đảm bảo an toàn từ ban đầu có thể tạo ra lỗ hổng bảo mật.

Quản lý quyền truy cập không chặt chẽ: Sự thiếu sót trong việc quản lý quyền truy cập có thể dẫn đến việc người dùng có quyền truy cập vào dữ liệu mà họ không nên có.

Phần mềm không được bảo trì đúng cách: Thiếu sót trong việc duy trì và bảo trì phần mềm, hệ điều hành hoặc các phần mềm bảo mật có thể tạo điều kiện cho việc tấn công.

Lỗ hổng trong hạ tầng mạng: Các thiết bị mạng, router, firewall hoặc switch không được cấu hình hoặc bảo trì đúng cách có thể tạo điều kiện cho việc tấn công.

Sử dụng phần mềm không an toàn: Sử dụng các phần mềm không được phát triển hoặc cung cấp bởi các nhà cung cấp đáng tin cậy có thể tạo ra lỗ hổng bảo mật.

Xâm nhập từ bên ngoài: Hacker hoặc kẻ tấn công có thể tìm ra lỗ hổng và khai thác nó để xâm nhập vào hệ thống.

Lỗi cấu hình và quản trị hệ thống: Cấu hình hệ thống không an toàn hoặc lỗi trong quản lý hệ thống có thể tạo ra lỗ hổng bảo mật.

Để ngăn chặn và giảm thiểu các lỗ hổng này, các tổ chức cần thực hiện các biện pháp bảo mật thích hợp, bao gồm kiểm tra mã nguồn, duy trì cập nhật, quản lý quyền truy cập, cấu hình hệ thống an toàn và giám sát liên tục.

**4. Giải pháp để an toàn thông tin**

**Thêm:**

- Chỉ định và thực thi chính sách an ninh thông tin (Information Security Policies): Xác định và triển khai các chính sách cụ thể về việc quản lý thông tin, truy cập dữ liệu, mật khẩu, và các biện pháp bảo vệ khác.

- Giáo dục và đào tạo nhân viên: Đào tạo nhân viên về các nguy cơ an ninh thông tin, biện pháp phòng ngừa, và cách xử lý thông tin một cách an toàn.

- Bảo vệ dữ liệu đầu vào và đầu ra: Kiểm tra và xác thực dữ liệu đầu vào từ các nguồn không tin cậy và kiểm tra dữ liệu đầu ra để đảm bảo tính toàn vẹn và an toàn.

- Sử dụng mã hóa: Mã hóa dữ liệu quan trọng để bảo vệ khỏi truy cập trái phép. Các công nghệ mã hóa cung cấp một lớp bảo vệ bổ sung cho dữ liệu.

- Quản lý danh sách kiểm tra an ninh (Security Checklist): Thực hiện các kiểm tra an ninh định kỳ để xác định và khắc phục các lỗ hổng an ninh.

- Bảo vệ hạ tầng mạng: Bao gồm việc sử dụng tường lửa (firewalls), phần mềm chống virus và malware, bộ lọc email, và các giải pháp bảo mật mạng.

- Sao lưu và khôi phục dữ liệu: Thực hiện việc sao lưu dữ liệu định kỳ và kiểm tra tính toàn vẹn của sao lưu. Đảm bảo có kế hoạch khôi phục dữ liệu hiệu quả trong trường hợp xảy ra sự cố.

- Quản lý quyền truy cập: Hạn chế quyền truy cập vào dữ liệu nhạy cảm chỉ đến những người cần thiết và theo nguyên tắc lấy ít nhất làm nguyên tắc.

- Theo dõi và phản ứng với sự cố: Triển khai hệ thống giám sát liên tục để phát hiện các hành vi không bình thường và sự xâm nhập. Phản ứng nhanh chóng và hiệu quả khi phát hiện sự cố.

- Tuân thủ các quy định và tiêu chuẩn: Đảm bảo tuân thủ các quy định và tiêu chuẩn an ninh thông tin áp dụng, chẳng hạn như GDPR (General Data Protection Regulation) ở châu Âu hoặc HIPAA (Health Insurance Portability and Accountability Act) ở Hoa Kỳ.

- Liên tục cải thiện: Xác định và triển khai các biện pháp bảo mật mới để ứng phó với các mối đe dọa và thách thức an ninh thông tin mới phát triển.

1. **Chính sách an toàn thông tin (Information Security Policy)**
2. **Chính sách ATTT là gì ?**

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 nhiểm chống lại tấng công nguy hiểm.

- 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 ninh thông tin và sử dụng máy tính hoặc các quy tắc riêng biệt về các chủ đề khác nhauVí dụ: quy tắc dùng e-mail, quyền hạn truy xuất dữ liệu, quy trình backup dữ liệu,....Ảnh có chứa văn bản, ảnh chụp màn hình, biểu đồ, Phông chữ

Mô tả được tạo tự động

## **2. Mục tiêu 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 ninh thông tin.- Phát hiện và ngăn chặn sự thoả hiệp của an ninh 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.

## **3. Phạm vi của ISP**ISP thường nhắm vào tất cả:+ Các dữ liệu+ Chương trình+ Hệ thống+ Phương tiện+ Cấu trúc hạ tầng cơ sở+ Các người dùng, các bên tham gia thứ 3 + Các nhóm bên ngoài (third parties) tổ chức+ Không có trường hợp ngoại lệ.ISP được dùng để hỗ trợ việc bảo vệ, điều khiển và quản lý các tài sản thông tin của tổ chức. ISP được yêu cầu là bao hàm tất cả các thông tin bên trong tổ chức mà có thể bao gồm dữ liệu và thông tin như sau: + Lưu trữ trong các CSDL, trong máy tính ở các đĩa cứng cố định+ Truyền qua mạng nội bộ và công cộng+ In hoặc viết tay trên giấy, bảng trắng ...+ Gửi qua fax, telex hoặc các phương tiện truyền thông khác+ Lưu trữ trên phương tiện di động như CD-ROM, đĩa cứng, băng và các phương tiện tương tự khác+ Tổ chức trên phim, các trang trình chiếu, máy chiếu, sử dụng phương tiện nghe nhìn và âm thanh+ Phát biểu trong các cuộc gọi điện thoại và các cuộc họp được chuyển tải bằng bất kỳ phương pháp nào khác

## **4. Tầm quan trọng ISP**- Giảm thiểu nguy cơ rò rỉ dữ liệu hoặc mất mát- Bảo vệ tổ chức khỏi những người dùng nội bộ và bên ngoài "độc hại“- Thiết lập các hướng dẫn, thực tiễn tốt nhất về sử dụng và đảm bảo tuân thủ đúng.- Thông báo nội bộ 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 ninh trong và ngoài tổ chức

## **5. Ai là người dùng ISP** Người quản lý – tất cả các cấp độNhân viên kỹ thuật – người quản trị hệ thống, …Người dùng cuối – tất cả các người dùng dịch vụ của hệ thống

## **6. Các bước triển khai ISP**1. Thu thập thông tin cơ bản2. Thực hiện đánh giá nguy cơ3. Tạo bức tranh tổng quan chính sách4. Triển khai kế hoạch bảo toàn thông tin5. Triển khai ch1nh sách an toàn thông tin6. Thực hiện chính sách và chuẩn7. Nhận thức và huấn luyện8. Theo dõi sự hài long9. Đánh giá tính hiệu lực10. Hiệu chỉnh chính sách

## Ảnh có chứa biểu đồ, văn bản, hàng, ảnh chụp màn hình Mô tả được tạo tự động

Ảnh có chứa văn bản, vòng tròn, đĩa nén, Đồ họa

Mô tả được tạo tự động

## **7. Xác định được vấn đề cần ISP**- Các nguồn tài nguyên và thông tin cần truy suất có thẩm quyền - Không tiết lộ hoặc không được phép tiết lộ thông tin- Quy trình cần tuân theo- Lỗi và lỗi người dùng

Quan tâm đến an toàn dữ liệu

- Xử lý dữ liệu:+ Chính sách: Cách dữ liệu được xử lý như thế nào và cách duy trì tính bí mật và toàn vẹn của dữ liệu. + Sự tồn tại của dữ liệu bên thứ ba+ Dữ liệu cá nhân+ Dữ liệu nhân sự+ Bảo vệ sự riêng tư+ Chi phí giấy phép phần mềm

- Sao lưu (Backups)+ Dữ liệu nào cần sao lưu+ Tần suất sao lưu+ Kiểm soát các quy trình sao lưu+ Lưu trữ dữ liệu tại chỗ hoặc ngoài nơi lưu trữ dữ liệu

- Tiêu hủy dữ liệu+ Xem xét các ổ cứng cũ+ Dumpster diving: kỹ thuật được dùng để lấy ra thông tin từ các dữ liệu đã bị xóa- Các quyền và chính sách về sở hữu trí tuệ+ Ai là chủ quyền đối với các tài sản trí tuệ+ Ghi nhãn để thực thi quyền sở hữu trí tuệ

## **8. Nội dung có trong 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

1. **Tại sao nhân viên ngành CNTT nắm rõ về Chính sách an toàn thông tin tại nơi làm việc**

Là một kỹ sư Công nghệ Thông tin (CNTT), em nghĩ việc nắm rõ và tuân thủ chính sách an toàn thông tin tại nơi làm việc là vô cùng quan trọng. Nó không chỉ là yêu cầu mà còn là một chiến lược quan trọng để đảm bảo an ninh thông tin trong môi trường làm việc. Dưới đây là ba lý do mà em nghĩ là kỹ sư CNTT cần nắm rõ:

*Bảo vệ Dữ liệu Quan trọng và Nhạy cảm:* Thông tin và dữ liệu đóng vai trò quan trọng. Chúng ta thường xử lý các dữ liệu nhạy cảm như: thông tin cá nhân của khách hàng, thông tin tài khoản người dùng, mã nguồn phần mềm, và nhiều loại dữ liệu khác. Chính sách an toàn thông tin giúp đảm bảo rằng các biện pháp bảo mật được thiết lập để bảo vệ dữ liệu quan trọng này khỏi sự truy cập trái phép, thất lạc, hay thậm chí là tấn công mạng.

*Ngăn Chặn Các Mối Đe Dọa An Ninh Thông Tin:* Tấn công mạng, virus, phần mềm độc hại, và thậm chí là nguy cơ từ bên trong do sự cẩu thả hoặc hành vi không an toàn của nhân viên là điều khó tránh khỏi. Chính sách an toàn thông tin giúp nhận diện, đánh giá và ngăn chặn những mối đe dọa này bằng cách đưa ra hướng dẫn cụ thể về cách ứng phó và ngăn chặn chúng.

*Tuân Thủ Pháp Luật và Nâng Cao Danh Tiếng:* Trong nhiều quốc gia, tổ chức phải tuân thủ quy định và luật lệ về bảo vệ thông tin. Việc không tuân thủ có thể đưa đến hậu quả pháp lý và tổn thất uy tín. Chính sách an toàn thông tin giúp xây dựng hệ thống an toàn thông tin mạnh mẽ, đảm bảo tuân thủ pháp luật và bảo vệ danh tiếng của tổ chức.

*Duy Trì Hiệu Suất Hệ Thống:* Điều này đảm bảo rằng hoạt động kinh doanh không bị ảnh hưởng do sự cố an ninh, đồng thời hỗ trợ trong việc duy trì hiệu suất tối ưu của hệ thống. Chính sách an toàn thông tin có thể cung cấp hướng dẫn về cách duy trì hiệu suất và ổn định của hệ thống trong môi trường an toàn.

1. **Ví dụ về chính sách an toàn thông tin**

Mobile Device Acceptable Use Policy (Chính sách Sử dụng Thiết bị Di động): Đây là một chính sách quy định các nguyên tắc và hướng dẫn cho nhân viên về việc sử dụng thiết bị di động của công ty, bao gồm điện thoại di động, máy tính bảng và các thiết bị di động khác. Chính sách này thường bao gồm các hạn chế về việc cài đặt ứng dụng không an toàn, quản lý mật khẩu và mã hóa dữ liệu trên các thiết bị, cũng như các biện pháp bảo mật khác để bảo vệ thông tin của tổ chức.

Sample Password Policy (Chính sách Mật khẩu Mẫu): Đây là một tài liệu quy định các yêu cầu và nguyên tắc cho việc tạo, quản lý và sử dụng mật khẩu trong tổ chức. Chính sách này thường bao gồm các yêu cầu về độ dài mật khẩu, sự đa dạng của ký tự, thời hạn hết hạn và các biện pháp bảo mật khác để ngăn chặn tấn công qua mật khẩu.

Wireless Security Access Policy (Chính sách Truy cập Bảo mật Không Dây): Chính sách này quy định các biện pháp an ninh cần được thực hiện khi sử dụng mạng không dây trong tổ chức. Nó bao gồm các yêu cầu về việc cài đặt mã hóa, xác thực và quản lý quyền truy cập để đảm bảo an toàn khi kết nối với mạng không dây.

IT Computer Equipment Security Policy (Chính sách Bảo mật Thiết bị Máy tính): Chính sách này tập trung vào bảo vệ các thiết bị máy tính và thiết bị điện tử khác trong tổ chức. Nó quy định các biện pháp bảo mật như khóa màn hình, mã hóa ổ cứng, kiểm soát truy cập và bảo vệ vật lý để ngăn chặn truy cập không được ủy quyền vào thiết bị và dữ liệu.

Software Installation Policy (Chính sách Cài đặt Phần mềm): Chính sách này quy định các quy định và hướng dẫn cho việc cài đặt và quản lý phần mềm trên các máy tính và thiết bị trong tổ chức. Nó có thể bao gồm các yêu cầu về sự phê duyệt trước khi cài đặt, sự tuân thủ giấy phép và các biện pháp bảo mật khác để ngăn chặn việc cài đặt phần mềm không an toàn hoặc không ủy quyền.

Responsible Use of Information and Technology Resources (Chính sách Sử dụng Trách nhiệm Tài nguyên Thông tin và Công nghệ): Chính sách này quy định các nguyên tắc và hướng dẫn cho việc sử dụng trách nhiệm các tài nguyên thông tin và công nghệ trong tổ chức. Nó bao gồm các hạn chế về việc sử dụng cá nhân, đạo đức sử dụng và các biện pháp bảo mật để bảo vệ tài nguyên thông tin của tổ chức.

Sample Internet Usage Policy (Chính sách Sử dụng Internet Mẫu): Chính sách này quy định các quy định và hướng dẫn cho việc sử dụng Internet trong tổ chức. Nó bao gồm các hạn chế về việc truy cập vào các trang web không an toàn, việc sử dụng email và truyền thông điện tử, và các biện pháp bảo mật để ngăn chặn việc xâm nhập từ Internet vào mạng của tổ chức.

**Thêm:**

Chính sách Mật khẩu Mạnh: Yêu cầu người dùng sử dụng mật khẩu mạnh bao gồm các ký tự chữ cái, số và ký tự đặc biệt, cũng như thay đổi mật khẩu định kỳ.

Chính sách Phòng Chống Virus và Phần Mềm Độc Hại: Yêu cầu cài đặt và duy trì phần mềm chống virus, cập nhật định kỳ và quét hệ thống để phát hiện và ngăn chặn các phần mềm độc hại.

Chính sách Quản lý Thiết bị và Phần Mềm: Xác định quy trình để kiểm soát việc cài đặt và sử dụng phần mềm trên các thiết bị trong mạng, bao gồm việc phê duyệt và giám sát các ứng dụng được cài đặt.

Chính sách Đào tạo An toàn Thông tin: Cung cấp đào tạo định kỳ cho nhân viên về các nguy cơ an ninh thông tin, phương pháp phòng chống và quy trình ứng phó với các vấn đề an ninh.

1. **Hệ thống quản lý ATTT (ISMS)**

- Bên cạnh những rủi ro về ATTT do bị tấn công phá hoại có chủ đích, tổ chức cũng có thể gặp phải những rủi ro đối với thông tin nếu: Các quy trình quản lý, vận hành không đảm bảo; Việc quản lý quyền truy cập chưa được kiểm tra và xem xét định kỳ; Nhận thức của nhân viên trong việc sử dụng và trao đổi thông tin chưa đầy đủ…. - Do đó, ngoài các biện pháp kỹ thuật, tổ chức cần xây dựng và áp dụng các chính sách, quy định, quy trình vận hành phù hợp để giảm thiểu rủi ro. - Tùy vào quy mô và lĩnh vực hoạt động, mỗi tổ chức có thể có các phương thức tiếp cần khác nhau để xây dựng hệ thống quản lý ATTT phù hợp**1. Hệ thống quản lý ATTT là gì?**

**Information Security Management System – ISMS**là công cụ để các nhà lãnh đạo quản lý thực hiện giám sát, quản lý hệ thống thông tin, tăng cường mức độ an toàn, bảo mật, giảm thiểu rủi ro cho hệ thống thông tin, đáp ứng được mục tiêu của doanh nghiệp, tổ chức.Thiết kế và triển khai Hệ thống ISMS phụ thuộc vào mục tiêu, các yêu cầu về ATTT cần phải đạt được, các quy trình đang vận hành, quy mô và cơ cấu của tổ chức... - Hệ thống ISMS cũng đòi hỏi phải luôn được xem xét, cập nhật để phù hợp với những thay đổi của tổ chức và nâng cao mức độ an toàn với Hệ thống lưu trữ, xử lý thông tin. - Tổ chức cũng cần cân nhắc chi phí đầu tư xây dựng và triển khai ISMS phù hợp với nhu cầu đảm bảo ATTT.- Sau khi xây dựng hệ thống ISMS thì doanh nghiệp sẽ nhận được Chứng chỉ An toàn bảo mật thông tin

## - Việc áp dụng ISMS là quyết định mang tính chiến lược của một tổ chức. Hệ thống quản lý an toàn thông tin (ISMS) duy trì tính bảo mật, tính toàn vẹn và tính sẵn sàng của thông tin bằng cách áp dụng một quá trình quản lý rủi ro và mang lại sự tin cậy cho các bên quan tâm rằng các rủi ro đã được quản lý đầy đủ.**2. Lợi ích khi áp dụng ISMS**

- Đảm bảo ATTT của tổ chức, đối tác và khách hàng, giúp cho hoạt động của tổ chức luôn thông suốt và an toàn.- Giúp nhân viên tuân thủ việc đảm bảo ATTT trong hoạt động nghiệp vụ thường ngày; Các sự cố ATTT do người dùng gây ra sẽ được hạn chế tối đa khi nhân viên được đào tạo, nâng cao nhận thức ATTT.- Giúp hoạt động đảm bảo ATTT luôn được duy trì và cải tiến. Các biện pháp kỹ thuật và chính sách tuân thủ được xem xét, đánh giá, đo lường hiệu quả và cập nhật định kỳ.- Đảm bảo hoạt động nghiệp vụ của tổ chức không bị gián đoạn bởi các sự cố liên quan đến ATTT.- Nâng cao uy tín của tổ chức, tăng sức cạnh tranh, tạo lòng tin với khách hàng, đối tác, thúc đẩy quá trình toàn cầu hóa và tăng cơ hội hợp tác quốc tế.

**3. Tiêu chuẩn ISO/IEC 27001:2013**- ISO/IEC 27001 là tiêu chuẩn quốc tế về Hệ thống quản lý an ninh thông tin (ISMS). - ISO/IEC 27001 là tiêu chuẩn quy định các yêu cầu đối với việc xây dựng và áp dụng hệ thống quản lý ATTT nhằm đảm bảo tính bảo mật (confidentiality), tính nguyên vẹn (integrity) và tính sẵn sàng (availability) đối với tài sản thông tin của các tổ chức. - Là một tiêu chuẩn trong bộ tiêu chuẩn ISO/IEC 27000 về quản lý ATTT, được xây dựng dựa trên các tiêu chuẩn về quản lý an toàn thông tin BS 7799 của Viện Tiêu chuẩn Anh (British Standards Institute - BSI). -Năm 2005, tiêu chuẩn này được ban hành lần 1 tiêu chuẩn ISO/IEC 27001:2005, đến năm 2013 ban hành tiêu chuẩn lần 2 ISO/IEC 27001:2013

- Đối tượng áp dụng: cho nhiều loại hình tổ chức (thương mại, cơ quan nhà nước, phi lợi nhuận...). Đặc biệt là các tổ chức mà các hoạt động phụ thuộc nhiều vào CNTT, máy tính, mạng máy tính, sử dụng CSDL như ngân hàng, tài chính, viễn thông, ...- Một hệ thống ISMS theo tiêu chuẩn ISO/IEC 27001:2013 sẽ đem lại sự tin tưởng của các bên liên quan như đối tác, khách hàng,... của tổ chức.- Doanh nhiệp sẽ được cấp Chứng chỉ An toàn bảo mật thông tin ISO 27001:2013 - Tiêu chuẩn này được xây dựng nhằm cung cấp các yêu cầu cho việc thiết lập, triển khai, duy trì và cải tiến liên tục Hệ thống quản lý an toàn thông tin (ISMS). - ISO/IEC 27001 đặc tả các yêu cầu cần thiết cho việc thiết lập, vận hành và giám sát hoạt động của ISMS; đưa ra các nguyên tắc cơ bản cho việc khởi tạo, thực thi, duy trì và cải tiến ISMS. -Tiêu chuẩn này đưa ra các quy tắc bảo mật thông tin và đánh giá sự tuân thủ đối với các bộ phận bên trong tổ chức, xây dựng các yêu cầu bảo mật thông tin mà đối tác, khách hàng cần phải tuân thủ khi làm việc với tổ chức.

## **4. Cấu trúc Tiêu chuẩn ISO 27001: 2013**

## Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, biểu đồ Mô tả được tạo tự động

- Gồm có 07 điều khoản chính (từ phần 4 đến phần 10 của Tiêu chuẩn)- Các điều khoản đưa ra yêu cầu bắt buộc về các công việc cần thực hiện trong việc thiết lập, vận hành, duy trì, giám sát và nâng cấp Hệ thống ISMS của các tổ chức. - Bất kỳ vi phạm nào của tổ chức so với các quy định nằm trong 07 điều khoản này đều được coi là không tuân thủ theo tiêu chuẩn.  
- Điều khoản 4 - Phạm vi tổ chức: Đưa ra các yêu cầu cụ thể để tổ chức căn cứ trên quy mô, lĩnh vực hoạt động và các yêu cầu, kỳ vọng của các bên liên quan thiết lập phạm vi Hệ thống quản lý ATTT phù hợp. - Điều khoản 5 - Lãnh đạo: Quy định các vấn đề về trách nhiệm của Ban lãnh đạo mỗi tổ chức trong Hệ thống ISMS, bao gồm các yêu cầu về sự cam kết, quyết tâm của Ban lãnh đạo trong việc xây dựng và duy trì hệ thống; các yêu cầu về việc cung cấp nguồn lực, tài chính để vận hành hệ thống.   
- Điều khoản 6 - Lập kế hoạch: Tổ chức cần định nghĩa và áp dụng các quy trình đánh giá rủi ro, từ đó đưa ra các quy trình xử lý. Điều khoản này cũng đưa ra các yêu cầu về việc thiết lập mục tiêu ATTT và kế hoạch để đạt được mục tiêu đó.- Điều khoản 7 - Hỗ trợ: yêu cầu đối với việc tổ chức đào tạo, truyền thông, nâng cao nhận thức cho toàn thể cán bộ, nhân viên của tổ chức về lĩnh vực ATTT và ISMS, số hóa thông tin.- Điều khoản 8 - Vận hành hệ thống: Tổ chức cần có kế hoạch vận hành và quản lý để đạt được các mục tiêu đã đề ra. Đồng thời cần định kỳ thực hiện đánh giá rủi ro ATTT và có kế hoạch xử lý.- Điều khoản 9 - Đánh giá hiệu năng hệ thống: Quy định trách nhiệm của Ban lãnh đạo trong việc định kỳ xem xét, đánh giá Hệ thống ISMS của tổ chức. Phần này đưa ra yêu cầu đối với mỗi kỳ xem xét hệ thống, đảm bảo đánh giá được toàn bộ hoạt động của hệ thống, đo lường hiệu quả của các biện pháp thực hiện và có kế hoạch khắc phục, nâng cấp hệ thống cho phù hợp với những thay đổi trong hoạt động của tổ chức.- Điều khoản 10 - Cải tiến hệ thống: Giữ vững nguyên tắc Kế hoạch - Thực hiện - Kiểm tra - Hành  động (P-D-C-A), tiêu chuẩn cũng đưa ra các yêu cầu đảm bảo Hệ thống ISMS không ngừng được cải tiến trong quá trình hoạt động. Gồm các quy định trong việc áp dụng các chính sách mới, các hoạt động khắc phục, phòng ngừa các điểm yếu đã xảy ra và tiềm tàng để đảm bảo hiệu quả của Hệ thống ISMS.- Phụ lục A: Các mục tiêu và biện pháp kiểm soát: đưa ra 14 lĩnh vực kiểm soát nhằm cụ thể hóa các vấn đề mà tổ chức cần xem xét, thực hiện khi xây dựng và duy trì Hệ thống ISMS.

Ảnh có chứa văn bản, ảnh chụp màn hình

Mô tả được tạo tự động

## **5. Triển khai ISMS ở Việt Nam**

## Bước 1: Khảo sát và lập kế hoạchBước 2: Xác định phương pháp quản lý rủi ro ATTTBước 3: Xây dựng hệ thống đảm bảo ATTT tại đơn vịBước 4: Triển khai áp dụng: các biện pháp đã lựa chọn, đáp ứng chính sách, quy định, quy trình đã xây dựng và yêu cầu của tiêu chuẩn ISO 27001.Bước 5: Đánh giá nội bộ: khắc phục các điểm không phù hợp với các quy định của tổ chức và yêu cầu của tiêu chuẩn. Sau khi thực hiện xong bước 5, tổ chức mời các đơn vị độc lập để đánh giá và cấp Chứng nhận phù hợp với tiêu chuẩn ISO 2701:2013 cho Hệ thống quản lý ATTT đã xây dựng.**6. DN nhận CC ATTT theo tiêu chuẩn ISO/IEC 27001:2013** - Công ty Cổ phần Dịch vụ Công nghệ Tin học HPT – 12/05/2014- Ngân hàng VIETCOMBANK - 12/12/2014 (NH đầu tiên)- Tập đoàn Bảo Việt – 23/1/2016- Trung tâm Internet Việt Nam (VNNIC) - 02/7/2015- Ngân hàng TMCP Sài Gòn - Hà Nội (SHB) - 20/11/2015- Trung tâm dữ liệu của VNPT (VNPT Data) – 1/9/2016- Ngân hàng TMCP Quân đội (MB) - 04/2017

## **7. Một số lưu ý của tiêu chuẩn ISO 27001:2013**

- Hệ thống ISMS là nhu cầu thiết yếu của tổ chức, đảm bảo ATTT một cách toàn diện.- Xây dựng hệ thống ISMS theo tiêu chuẩn ISO/IEC 27001: 2013 sẽ giúp hoạt động đảm bảo ATTT của tổ chức được quản lý chặt chẽ. - Do tiêu chuẩn ISO/IEC 27001:2013 xem xét đảm bảo ATTT trên nhiều khía cạnh. Nên việc xây dựng và áp dụng hệ thống đòi hỏi phải có sự quyết tâm của lãnh đạo tổ chức. Và sự phối hợp đồng bộ các bộ phận của tổ chức trong việc xây dựng và duy trì hệ thống.- Những vấn đề khó khăn, cần lưu ý khi tổ chức bắt tay vào xây dựng hệ thống ISMS là:+ Nhận thức của người dùng trong tổ chức về việc đảm bảo ATTT.  Đánh giá lợi ích mang lại khi áp dụng hệ thống ISMS chưa cao.+ Trách nhiệm xây dựng, duy trì hệ thống được phân công không phù hợp. Đơn vị được giao không nhận được sự phối hợp, cộng tác của các đơn vị khác trong tổ chức.+ Việc xây dựng và nâng cấp hệ thống cần sự quan tâm của lãnh đạo và đầu tư nguồn lực thích đáng.

1. **Lợi ích khi áp dụng ISMS**

- Đảm bảo ATTT của tổ chức, đối tác và khách hàng, giúp cho hoạt động của tổ chức luôn thông suốt và an toàn.- Giúp nhân viên tuân thủ việc đảm bảo ATTT trong hoạt động nghiệp vụ thường ngày; Các sự cố ATTT do người dùng gây ra sẽ được hạn chế tối đa khi nhân viên được đào tạo, nâng cao nhận thức ATTT.- Giúp hoạt động đảm bảo ATTT luôn được duy trì và cải tiến. Các biện pháp kỹ thuật và chính sách tuân thủ được xem xét, đánh giá, đo lường hiệu quả và cập nhật định kỳ.- Đảm bảo hoạt động nghiệp vụ của tổ chức không bị gián đoạn bởi các sự cố liên quan đến ATTT.- Nâng cao uy tín của tổ chức, tăng sức cạnh tranh, tạo lòng tin với khách hàng, đối tác, thúc đẩy quá trình toàn cầu hóa và tăng cơ hội hợp tác quốc tế

**Thêm:**

- Bảo vệ Dữ liệu và Thương hiệu: ISMS giúp đảm bảo rằng dữ liệu quan trọng của tổ chức được bảo vệ khỏi mất mát, sửa đổi trái phép hoặc tiết lộ. Điều này giúp bảo vệ thương hiệu của tổ chức trước các mối đe dọa liên quan đến việc rò rỉ thông tin hoặc sự cố an ninh.

- Tuân thủ Pháp luật và Tiêu chuẩn: Áp dụng ISMS giúp tổ chức tuân thủ các yêu cầu pháp luật liên quan đến bảo vệ thông tin cá nhân, như GDPR, HIPAA, hoặc các tiêu chuẩn an ninh thông tin như ISO 27001. Điều này giúp tránh phạt và trách nhiệm pháp lý đối với việc vi phạm.

- Giảm Thiểu Rủi ro: ISMS giúp xác định, đánh giá và quản lý các rủi ro an ninh thông tin một cách hệ thống. Việc phát hiện và giảm thiểu rủi ro giúp giảm nguy cơ phát sinh sự cố an ninh, từ đó giảm thiểu tác động tiêu cực lên hoạt động kinh doanh.

- Tăng Credibility: Việc áp dụng ISMS thể hiện cam kết của tổ chức đối với việc bảo vệ thông tin và dữ liệu khách hàng. Điều này tạo ra niềm tin và uy tín từ phía khách hàng, đối tác và cơ quan quản lý.

- Tối ưu Hóa Quản lý Rủi ro: ISMS cung cấp một phương pháp hệ thống để quản lý rủi ro, từ đó giúp tổ chức hiểu rõ hơn về các rủi ro mà họ đang đối mặt và ra quyết định thông minh về việc đầu tư và ưu tiên.

- Tiết kiệm Chi phí: Bằng cách giảm thiểu các sự cố an ninh thông tin và tối ưu hóa quản lý rủi ro, ISMS có thể giúp giảm chi phí liên quan đến xử lý sự cố, phạt pháp lý, và phục hồi sau sự cố.

- Nâng cao Hiệu suất và Năng suất: Việc có một môi trường an ninh thông tin được quản lý tốt giúp tăng cường hiệu suất làm việc và năng suất của nhân viên. Sự tự tin và an tâm trong việc làm việc với dữ liệu cũng tạo điều kiện cho một môi trường làm việc tích cực hơn.

Tóm lại, việc áp dụng ISMS không chỉ là một nhu cầu pháp lý mà còn là một đầu tư thông minh giúp tăng cường bảo vệ dữ liệu, tăng cường uy tín và hiệu suất của tổ chức.

1. **Vì sao Doanh nghiệp phải xây dựng Hệ thống ISMS (**Tương tự V.2, VI**)**
2. **Hãy kể thêm 2 Tiêu chuẩn Quốc tế cũng là ISMS**

- ISO/IEC 27001: Đây là một trong những tiêu chuẩn quốc tế phổ biến nhất về bảo mật thông tin. ISO/IEC 27001 cung cấp các yêu cầu cho việc thiết lập, triển khai, duy trì và cải thiện liên tục một Hệ thống Quản lý An ninh Thông tin (ISMS) trong một tổ chức. Tiêu chuẩn này không chỉ xác định các yêu cầu cần thiết để bảo vệ thông tin một cách hiệu quả mà còn đề xuất một phương pháp hệ thống để quản lý an ninh thông tin trong toàn bộ tổ chức.

- ISO/IEC 27002: Tiêu chuẩn này cung cấp hướng dẫn về các biện pháp bảo mật thông tin, bao gồm các chính sách, thủ tục, cơ chế kiểm soát và các biện pháp kỹ thuật. ISO/IEC 27002 không phải là một tiêu chuẩn đánh giá như ISO/IEC 27001, mà nó cung cấp một khung nhất định cho việc triển khai các biện pháp bảo mật thông tin trong tổ chức, dựa trên các nguyên tắc và phương pháp thực tiễn.

🡪 Cả hai tiêu chuẩn này cung cấp các hướng dẫn và phương pháp cho việc thiết lập, triển khai và duy trì một hệ thống an ninh thông tin hiệu quả trong tổ chức. Việc tuân thủ các tiêu chuẩn này giúp tổ chức tăng cường bảo vệ thông tin, giảm thiểu rủi ro và đảm bảo tuân thủ các quy định pháp luật và tiêu chuẩn ngành.

1. **Em hãy trình bày 5 Tiêu chuẩn Đạo đức Nghề nghiệp của Nhân viên, viên chức chuyên ngành CNTT Theo thông tư 45. Là Nhân viên Ngành Công nghệ Thông tin Em sẽ thực hiện trao dồi 5 tiêu chuẩn này như thế nào?**

Ngày 29/12/2017, Bộ Thông tin và Truyền thông ban hành Thông tư 45/2017/TT-BTTTT quy định tiêu chuẩn chức danh nghề nghiệp viên chức chuyên ngành công nghệ thông tin.- Chấp hành các chủ trương, đường lối, chính sách của Đảng, pháp luật của Nhà nước, các quy định của ngành và địa phương về thông tin và truyền thông.- Nắm vững quan điểm, đường lối, chủ trương chính sách, chỉ thị, nghị quyết của Đảng và pháp luật Nhà nước về lĩnh vực chuyên ngành;- Trung thực, khách quan, có tinh thần trách nhiệm cao đối với công việc được giao; thực hiện đúng và đầy đủ các nghĩa vụ của người viên chức trong hoạt động nghề nghiệp.- Có ý thức trau dồi đạo đức, giữ gìn phẩm chất, danh dự, uy tín nghề nghiệp; không lạm dụng vị trí công tác, nhiệm vụ được phân công để trục lợi; đoàn kết, sáng tạo, sẵn sàng tiếp thu, học hỏi cái mới, tự nâng cao trình độ; có ý thức phối hợp, giúp đỡ đồng nghiệp, chia sẻ kinh nghiệm trong công tác; tích cực tham gia nghiên cứu đề tài khoa học, sáng kiến cải tiến kỹ thuật để phát triển nghề nghiệp và nâng cao trình độ.- Tuân thủ pháp luật về bảo vệ bí mật nhà nước; đảm bảo an toàn, bí mật thông tin và an ninh, quốc phòng.

### **Là Nhân viên Ngành Công nghệ Thông tin Em sẽ thực hiện trao dồi 5 tiêu chuẩn này như thế nào?**

Là nhân viên ngành CNTT em sẽ thực hiện và trao dồi 5 tiêu chuẩn này theo cách:

-Cần có ý thức, trách nhiệm với công việc của mình. Biết thực hiện công việc một cách trung thực, không gian dối, gian lận, đặt chữ tín lên hàng đầu.Làm việc gì cũng cần đảm bảo tính minh bạch, chính xác, rõ ràng.

-Chịu trách nhiệm với việc mình làm, đảm bảo hoàn thành trách nhiệm đúng thời hạn và đảm bảo chất lượng. Tôn trọng quyền lợi sở thích của người khác, không xâm phạm quyền riêng tư và phải bảo vệ thông tin người dung

-Luôn có tinh thần học hỏi, đoàn kết, sáng tạo, tiếp thu kiến thức, công nghệ mới

-Làm việc phải có tinh thần đoàn kết, có ý thức phối hợp, giúp đỡ đồng nghiệp và chia sẻ những gì mình biết cho đồng nghiệp.

-Nếu có cơ hội hãy thử sức với các cuộc thi quốc tế, tham gia vào các cuộc nghiên cứu đề tài khoa học công nghệ, cải tiến kỹ thuật, phát triển công nghệ để nâng cao trình độ.

-Cần tuân thủ các quy định nguyên tắc đạo đức nghề nghiệp, không tham nhũng, tham ô, vi phạm pháp luật và đạo đức trong công việc

-Chấp hành các chủ trương, đường lối, chính sách của Đảng, pháp luật của Nhà nước.

-Tâm huyết với nghề, trung thực, khách quan, làm việc khoa học, có chính kiến rõ rang, thực hành tiết kiệm chi phí, chống lãng phí.

1. **Tóm tắc ACM**

Nếu đề kêu tóm tắt chép từ đây

Tổ chức ACM (Association for Computing Machinery) là một tổ chức quốc tế hàng đầu trong lĩnh vực nghiên cứu và giáo dục về Khoa học Máy tính và Tin học. Được thành lập từ năm 1947, ACM có hơn 100.000 hội viên tính đến năm 2011 và đã đóng góp đáng kể vào sự phát triển của ngành công nghiệp này.

Bộ quy tắc đạo đức của ACM được thiết kế để hướng dẫn hành vi đạo đức của các chuyên gia máy tính, bao gồm cả giảng viên, sinh viên và người sử dụng công nghệ máy tính. Bộ quy tắc này bao gồm các nguyên tắc cơ bản về trách nhiệm và công bằng, dựa trên sự hiểu biết rằng lợi ích công cộng luôn là yếu tố chính.

Các nguyên tắc chính trong Bộ quy tắc đạo đức của ACM bao gồm:

Đóng góp cho xã hội và làm cho con người hạnh phúc: Tầm quan trọng của việc đảm bảo rằng công nghệ máy tính không chỉ cải thiện cuộc sống mà còn giảm thiểu các hậu quả tiêu cực.

Tránh gây hậu quả tiêu cực: Chú trọng vào việc ngăn chặn các hậu quả không mong muốn của công nghệ máy tính, bao gồm cả sự thất bại về an toàn và bảo mật.

Trung thực và đáng tin cậy: Cung cấp thông tin đầy đủ và minh bạch về các khía cạnh kỹ thuật và đạo đức của công việc.

Hãy công bằng và hành động không phân biệt đối xử: Thúc đẩy sự công bằng và bình đẳng trong tất cả các khía cạnh của công việc máy tính

Tôn trọng quyền riêng tư: Bảo vệ quyền riêng tư của cá nhân và đảm bảo rằng thông tin cá nhân được sử dụng một cách hợp pháp và minh bạch.

Bảo mật danh dự: Bảo vệ thông tin nhạy cảm và tuân thủ các quy định về bảo mật thông tin.

Phấn đấu đạt chất lượng cao: Hướng đến việc tạo ra các sản phẩm và dịch vụ chất lượng cao cả về quy trình và sản phẩm.

Duy trì tiêu chuẩn cao về năng lực chuyên môn: Liên tục cập nhật và phát triển kỹ năng và kiến thức để duy trì tiêu chuẩn cao về năng lực chuyên môn.

Tôn trọng quyền lực: Thực hiện các biện pháp cần thiết để bảo vệ quyền lực và nguồn lực trong các lĩnh vực có thẩm quyền.

Nhận thức về công nghệ và hậu quả của chúng: Hiểu biết và chia sẻ kiến thức về công nghệ máy tính và nhận thức về các hậu quả của chúng đối với xã hội và cá nhân.

Truy cập tài nguyên máy tính và truyền thông một cách có trách nhiệm: Sử dụng các tài nguyên máy tính và truyền thông một cách có trách nhiệm và chỉ khi được ủy quyền.

Thiết kế và triển khai các hệ thống mạnh mẽ và an toàn: Đảm bảo rằng các hệ thống máy tính được thiết kế và triển khai một cách an toàn và bảo mật.

Bộ quy tắc này là một hướng dẫn quan trọng cho các chuyên gia máy tính về cách thực hiện công việc của họ một cách đạo đức và trách nhiệm, đồng thời đảm bảo rằng công nghệ máy tính mang lại lợi ích cho toàn xã hội.

Đến đây

1. **Khái niệm ACM**

## Association for Computing Machineryst (Thành lập năm 1947)

## Là một hiệp hội quốc tế về nghiên cứu, giáo dục ngành Khoa học máy tính và Tin học uy tín nhất thế giới với hơn 100.000 hội viên, tính đến năm 2011.**2. Bộ quy tắc đạo đức của ACM**

Được thiết kế để hướng dẫn hành vi đạo đức của tất cả các chuyên gia máy tính, bao gồm các giảng viên, sinh viên, người sử dụng công nghệ máy tính .Bộ luật bao gồm các nguyên tắc được xây dựng dưới dạng các tuyên bố về trách nhiệm, dựa trên sự hiểu biết rằng lợi ích công cộng luôn là yếu tố chính. Bộ luật đạo đức và hành vi chuyên nghiệp ACM thể hiện lương tâm của nghề.**\* NGUYÊN TẮC ĐẶC BIỆT CHUNG.**Một chuyên gia điện toán nên ...**1.1 Đóng góp cho xã hội và làm cho con người hạnh phúc**Liên quan đến chất lượng cuộc sống của tất cả mọi người,Giảm thiểu các hậu quả tiêu cực của máy tính, bao gồm các mối đe dọa đến sức khỏe, an toàn, bảo mật cá nhân và quyền riêng tư.**1.2 Tránh gây hậu quả tiêu cực**Chấn thương về thể chất hoặc tinh thần không hợp lýPhá hủy hoặc tiết lộ thông tin không hợp lý và thiệt hại không hợp lý đối với tài sản, danh tiếng và môi trường**1.3 Hãy trung thực và đáng tin cậy.**Minh bạch và cung cấp đầy đủ thông tin về tất cả các khả năng, hạn chế và các vấn đề tiềm ẩn của hệ thống cho các bên thích hợp**1.4 Hãy công bằng và hành động không phân biệt đối xử**Thúc đẩy sự tham gia công bằng của tất cả mọi ngườiBình đẳng, khoan dung, tôn trọng người khácTạo ra các sản phẩm hay các ứng dụng không phân biệt người dùng.**1.5 Tôn trọng công việc cần thiết để tạo ra các ý tưởng mới, sáng chế, tác phẩm sáng tạo và các tạo tác điện toán.**Ghi nhận những người tạo ra ý tưởng, sáng chế, tôn trọng quyền tác giả, bằng sáng chế, bí mật thương mại và các phương thức bảo vệ tác phẩm của tác giả.**1.6 Tôn trọng quyền riêng tư.**- Hiểu các quyền và trách nhiệm liên quan đến việc thu thập và sử dụng thông tin cá nhân.- Nên sử dụng thông tin cá nhân cho các mục đích hợp pháp và không vi phạm quyền của cá nhân và nhóm- Thiết lập các chính sách và quy trình minh bạch cho phép các cá nhân hiểu dữ liệu nào đang được thu thập và cách sử dụng dữ liệu, đồng ý cho thu thập dữ liệu tự động và xem xét, lấy, sửa lỗi không chính xác và xóa dữ liệu cá nhân của họ.**1.7 Bảo mật danh dự**- Các chuyên gia máy tính thường được giao phó thông tin bí mật như bí mật thương mại, dữ liệu khách hàng, chiến lược kinh doanh phi công cộng, thông tin tài chính, dữ liệu nghiên cứu, các bài báo nghiên cứu trước xuất bản và các ứng dụng bằng sáng chế. Các chuyên gia máy tính nên bảo vệ tính bảo mật ngoại trừ trong trường hợp đó là bằng chứng về vi phạm pháp luật, các quy định của tổ chức hoặc của Bộ luật.**\* TRÁCH NHIỆM NGHỀ NGHIỆP2.1 Phấn đấu đạt chất lượng cao cả về quy trình và sản phẩm của công việc chuyên môn.**- Nhấn mạnh và hỗ trợ công việc chất lượng cao từ bản thân và từ các đồng nghiệp**2.2 Duy trì các tiêu chuẩn cao về năng lực chuyên môn, hành vi và thực hành đạo đức.**- Cần duy trì năng lực chuyên môn, phát triển kỹ năng giao tiếp. Nâng cao kỹ năng nên là một quá trình liên tục và có thể bao gồm nghiên cứu độc lập, tham dự các hội nghị hoặc hội thảo, và giáo dục không chính thức hoặc chính thức khác. **2.3 Biết và tôn trọng các quy tắc hiện hành liên quan đến công việc chuyên môn.**- Tuân thủ các quy tắc bao gồm luật và quy định của địa phương, khu vực, quốc gia và quốc tế, cũng như mọi chính sách và thủ tục của tổ chức mà chuyên gia thuộc về- Chất lượng cao làm việc chuyên nghiệp trong máy tính phụ thuộc vào đánh giá chuyên nghiệp ở tất cả các giai đoạn. - Tìm kiếm và sử dụng đánh giá ngang hàng và các bên liên quan. **2.4 Chấp nhận và cung cấp đánh giá chuyên nghiệp phù hợp**Cung cấp các đánh giá mang tính xây dựng, quan trọng cho công việc của người khác.**2.5 Đưa ra các đánh giá toàn diện và toàn diện về hệ thống máy tính và tác động của chúng, bao gồm phân tích các rủi ro có thể xảy ra.**Các chuyên gia máy tính có trách nhiệm đặc biệt để cung cấp các đánh giá khách quan, đáng tin cậy cho người sử dụng lao động, nhân viên, khách hàng, người dùng và công chúng. Nhận thức, thấu đáo và khách quan khi đánh giá, giới thiệu và trình bày các mô tả hệ thống và các lựa chọn thay thế. Cần chú ý đặc biệt để xác định và giảm thiểu rủi ro tiềm ẩn trong các hệ thống học máy.**2.6 Chỉ thực hiện công việc trong các lĩnh vực có thẩm quyền.**Đánh giá tính khả thi của các công việc tiềm năng và đưa ra phán quyết về việc phân công công việc có nằm trong phạm vi thẩm quyền của chuyên gia hay không. Đánh giá đạo đức của một chuyên gia máy tính dựa trên quyết định của họ trong việc nhận nhiệm vụ.**2.7 Nhận thức, các công nghệ liên quan và hậu quả của chúng.**Chuyên gia máy tính nên chia sẻ về công nghệ máy tính kiến ​​thức kỹ thuật với công chúng, nhận thức về công nghệ máy tínhCác vấn đề quan trọng bao gồm các tác động của hệ thống máy tính, những hạn chế của chúng, các lỗ hổng của chúng và các rủi ro. Ngoài ra, một chuyên gia tính toán cần phải đánh giá được những thông tin không chính xác hoặc gây hiểu nhầm liên quan đến máy tính.**2.8 Truy cập tài nguyên máy tính và truyền thông chỉ khi được ủy quyền hoặc khi bị ép buộc bởi lợi ích công cộng.**Không nên truy cập vào hệ thống máy tính, phần mềm hoặc dữ liệu của người khác mà không được ủy quyền hoặc phù hợp với lợi ích chung.Trong trường hợp đặc biệt, một chuyên gia tính toán có thể sử dụng truy cập trái phép để làm gián đoạn hoặc ức chế hoạt động của các hệ thống độc hại; các biện pháp phòng ngừa bất thường phải được thực hiện trong những trường hợp này để tránh gây tổn hại cho người khác.**2.9 Thiết kế và triển khai các hệ thống mạnh mẽ và an toàn.**Các chuyên gia máy tính phải xem xét thiết kế và triển khai hệ thống bảo mật mạnh mẽ .Thực hiện thẩm định để đảm bảo các chức năng của hệ thống được bảo mật mạnh,có hành động thích hợp để bảo đảm các nguồn lực chống lại việc sử dụng sai mục đíchTính toán tích hợp các kỹ thuật và chính sách theo dõi, vá lỗi và báo cáo lỗ hổng. Thực hiện các bước để đảm bảo các bên bị ảnh hưởng bởi các vi phạm dữ liệu được thông báo một cách kịp thời và rõ ràng, cung cấp hướng dẫn và khắc phục thích hợp.Để đảm bảo hệ thống đạt được mục đích đã định, các tính năng bảo mật cần được thiết kế trực quan và dễ sử dụng nhất có thể. Ngăn cản các biện pháp phòng ngừa an ninh quá khó hiểu, có tình huống không phù hợp hoặc ngăn cản việc sử dụng hợp pháp.**\* NGUYÊN TẮC LÃNH ĐẠO CHUYÊN NGHIỆP.-** Đảm bảo rằng lợi ích công cộng là mối quan tâm chính trong tất cả các công việc điện toán chuyên nghiệp.- Kết nối, khuyến khích chấp nhận và đánh giá việc thực hiện trách nhiệm xã hội của các thành viên trong tổ chức hoặc nhóm.- Quản lý nhân sự và nguồn lực để nâng cao chất lượng cuộc sống làm việc.- Nói rõ, áp dụng và hỗ trợ các chính sách và quy trình phản ánh các nguyên tắc của Bộ luật.- Tạo cơ hội cho các thành viên của tổ chức hoặc nhóm phát triển thành các chuyên gia.- Sử dụng dịch vụ chăm sóc khi sửa đổi hoặc gỡ bỏ hệ thống.- Nhận biết và chăm sóc đặc biệt các hệ thống được tích hợp vào cơ sở hạ tầng của xã hội.**\* TUÂN THỦ BỘ QUY TẮC ĐẠO ĐỨC** Mở rộng, quảng bá và tôn trọng các nguyên tắc của Bộ luật.Mỗi thành viên ACM nên khuyến khích và hỗ trợ sự tuân thủ của tất cả các chuyên gia điện toán. Khi các thành viên ACM nhận ra vi phạm Bộ luật nên xem xét để báo cáo vi phạm đối với ACM để từ đó bộ quy tắc này được hoàn thiện.Điều chỉnh các quy tắc nếu phát hiện các sai phạm xảy ra.

1. **Những điều cần biết về Tội phạm công nghệ cao: Khái niệm, phân loại, cho ví dụ**
2. **Khái niệm tội phạm công nghệ cao**

**Theo Bộ Tư pháp Mỹ:** Tội phạm trong lĩnh vực công nghệ thông tin là “bất cứ hành vi vi phạm pháp luật hình sự nào có liên quan đến việc sử dụng các hiểu biết về công nghệ máy tính trong việc phạm tội”.

**Theo từ điển Bách khoa Công an nhân dân Việt Nam** “Loại tội phạm sử dụng những thành tựu mới của khoa học – kỹ thuật và công nghệ hiện đại làm công cụ, phương tiện để thực hiện hành vi phạm tội một cách cố ý hoặc vô ý, gây nguy hiểm cho xã hội. Chủ thể của loại tội phạm này thường là những người có trình độ học vấn, chuyên môn cao, có thủ đoạn rất tinh vi, khó phát hiện. Hậu quả do loại tội phạm này gây ra không chỉ là những thiệt hại về mặt kinh tế, xã hội mà nó còn xâm phạm tới an ninh quốc gia.”**Theo tổ chức Cảnh sát hình sự quốc tế INTERPOL:**

## Tội phạm công nghệ cao “là loại tội phạm sử dụng, lạm dụng những thiết bị kỹ thuật, dây chuyền công nghệ có trình độ cao như một công cụ phương tiện để thực hiện hành vi phạm tội”.**2. Phân loại:** Tội phạm sử dụng công nghệ cao, chia 2 loại- Tội phạm với mục đích tấn công Website, một hệ thống thông tin, CSDL chứa dữ liệu hoặc hệ thống mạng máy tính- Tội phạm “truyền thống” sử dụng công nghệ cao**3. Ví dụ**

Tội phạm công nghệ cao: Một nhóm hacker xâm nhập vào hệ thống máy tính của một ngân hàng và đánh cắp thông tin tài khoản của hàng nghìn khách hàng, sau đó sử dụng thông tin này để trộm tiền từ tài khoản của họ hoặc tiến hành giao dịch trái phép.

Tội phạm truyền thống: Một nhóm cướp ngân hàng tiến hành vũ trang đột nhập vào một ngân hàng, đe dọa nhân viên và khách hàng, rồi cướp đi một số lượng lớn tiền mặt từ quầy giao dịch trước khi bỏ trốn.

Trong ví dụ này, tội phạm công nghệ cao sử dụng kỹ thuật hacker và internet để thực hiện tội phạm, trong khi tội phạm truyền thống sử dụng vũ khí và bạo lực trực tiếp để đạt được mục tiêu của mình. Đây là một minh họa cho sự khác biệt trong phương pháp thực hiện và công cụ được sử dụng giữa hai loại tội phạm này.

## **4. So sánh giữa tội phạm trong lĩnh vực CNTT với tội phạm thông thường?**

Phạm vi và Phương thức thực hiện:

Tội phạm trong lĩnh vực CNTT thường có thể hoạt động từ xa qua internet và có khả năng tác động đến một lượng lớn người dùng một cách ẩn danh. Trong khi đó, tội phạm thông thường thường thực hiện tại các địa điểm cụ thể và có thể đòi hỏi tiếp xúc trực tiếp với nạn nhân hoặc nơi vi phạm.

Phạm vi của Tác động:

Tội phạm CNTT thường nhắm đến các hệ thống máy tính, dữ liệu trực tuyến và thông tin cá nhân. Hậu quả của các tội phạm này có thể là mất mát dữ liệu, lừa đảo tài chính hoặc xâm nhập vào quyền riêng tư. Trong khi đó, tội phạm thông thường thường liên quan đến hành vi như cướp, trộm, hành hung hoặc gây rối.

Phương tiện và Công cụ:

Tội phạm CNTT thường sử dụng công nghệ và phần mềm để thực hiện các hành vi phạm tội, bao gồm virus máy tính, malware, công cụ tấn công mạng và kỹ thuật xâm nhập xã hội. Trong khi đó, tội phạm thông thường có thể sử dụng vũ khí, công cụ hóa học hoặc vật lý để thực hiện hành vi phạm tội.

Tầm ảnh hưởng và Mức độ nguy hiểm:

Mặc dù cả hai loại tội phạm đều có thể gây hậu quả nghiêm trọng, tội phạm CNTT thường có khả năng lan rộng nhanh chóng và tác động lớn đến nhiều người dùng và tổ chức. Nó có thể gây ra hậu quả kinh tế lớn và ảnh hưởng đến quốc gia hoặc cộng đồng toàn cầu. Trong khi đó, tội phạm thông thường thường có tác động cục bộ và có thể gây hậu quả lớn cho các cá nhân hoặc cộng đồng nhỏ hơn.

Cách thức Xử lý và Điều tra:

Đối với tội phạm CNTT, việc xác định và truy tìm thủ phạm thường phức tạp hơn do tính chất ẩn danh và kỹ thuật của các hành vi phạm tội. Trong khi đó, tội phạm thông thường thường có dấu vết vật chứng rõ ràng hơn và quy trình điều tra thường dựa trên các phương tiện truyền thông, các nhân chứng và bằng chứng vật chứng vật lý.

# XII. Tình hình tội phạm Công nghệ cao hiện nay tại Việt Nam

Tình hình tội phạm công nghệ cao tại Việt Nam đang diễn ra phức tạp và đa dạng, phản ánh xu hướng tiến triển của Công nghệ thông tin và mức độ sẵn sàng của xã hội trong việc đối mặt và ngăn chặn các mối đe dọa an ninh mạng. Dưới đây là một số tình hình và xu hướng chính:

-Tăng cường về số lượng và đa dạng của các cuộc tấn công mạng: Việt Nam đang chứng kiến một tăng cường về cả số lượng và đa dạng của các cuộc tấn công mạng. Các cuộc tấn công này có thể bao gồm các loại virus, malware, phishing, xâm nhập vào dữ liệu cá nhân và tổ chức, cũng như các cuộc tấn công mục tiêu như các cơ quan chính phủ, tổ chức tài chính và doanh nghiệp.

-Tăng cường về sự phát triển của các nhóm tội phạm mạng: Việt Nam đã chứng kiến sự xuất hiện của nhiều nhóm tội phạm mạng chuyên nghiệp, hoạt động hợp pháp hoặc phi pháp. Những nhóm này thường tổ chức và có kỹ thuật cao, thường xuyên thực hiện các cuộc tấn công mạng có sự phối hợp rộng rãi và sử dụng công nghệ tiên tiến.

-Sự gia tăng của tội phạm mạng liên quan đến tài chính: Có một số loại tội phạm mạng tại Việt Nam tập trung vào việc phạm tội về tài chính, bao gồm lừa đảo, gian lận thẻ tín dụng, phá hoại hệ thống thanh toán điện tử và tội phạm liên quan đến tiền điện tử và tiền ảo.

-Căng thẳng trong an ninh mạng quốc gia: Với tình hình chính trị và kinh tế biến động, cũng như với vị trí địa lý chiến lược của Việt Nam, an ninh mạng quốc gia đang gặp phải các thách thức từ các cuộc tấn công mạng, đặc biệt là từ các nhóm tấn công mạng có liên quan đến các quốc gia khác.

-Nỗ lực từ phía chính phủ và tổ chức để ngăn chặn và chống lại tội phạm mạng: Chính phủ Việt Nam đã thực hiện nhiều biện pháp nhằm tăng cường an ninh mạng, bao gồm việc ban hành các quy định và luật pháp liên quan đến an ninh mạng, tăng cường hợp tác quốc tế, và đào tạo và phát triển lực lượng chuyên gia an ninh mạng.

Tóm lại, tình hình tội phạm công nghệ cao tại Việt Nam đang diễn biến phức tạp và đòi hỏi sự chú ý và nỗ lực từ phía cả chính phủ và các tổ chức để ngăn chặn và chống lại các mối đe dọa này.

# Tình huống luật CNTT

# Tình huống 2:

**2.Nếu bạn là bạn của sinh viên này, bạn sẽ khuyên nhủ như thế nào hay làm gì để bạn ấy nhận ra hành vi vi phạm của mình**

Nếu tôi là bạn của sinh viên này, tôi sẽ khuyên nhủ và hướng dẫn anh ta nhận ra hậu quả và tác động tiêu cực của hành vi của mình:

Nói rõ về những hậu quả pháp lý của việc tấn công vào hệ thống thông tin mà không có sự cho phép.

Giải thích về việc vi phạm quyền sở hữu trí tuệ và những rủi ro pháp lý có thể phải đối mặt khi sao chép và đăng tải thông tin bảo mật của người khác.

Khuyến khích anh ta tập trung vào việc học hỏi và nghiên cứu các kỹ thuật bảo mật một cách đạo đức và trách nhiệm, và thúc đẩy sự phát triển cá nhân và chuyên môn một cách tích cực và tích cực hơn.

# Tình huống 3:

**2.Nếu bạn là bạn A thì bạn nên như thế nào để tránh hành vi vi phạm tương tự như bạn B, nêu lý do tại sao?**

Nếu tôi là bạn A, để tránh hành vi vi phạm tương tự như bạn B, tôi sẽ thực hiện các biện pháp sau và có lý do như sau:

Tạo ra các tài khoản quản trị phù hợp: Thay vì sử dụng tài khoản Admin cho mọi hoạt động, tôi sẽ tạo ra các tài khoản quản trị có phạm vi hoạt động hạn chế, phù hợp với từng nhiệm vụ cụ thể. Điều này giúp giảm thiểu rủi ro truy cập trái phép vào thông tin cá nhân của người dùng.

Tuân thủ nguyên tắc cần thiết và trách nhiệm: Tôi sẽ tuân thủ nguyên tắc cần thiết và chỉ sử dụng tài khoản và tài nguyên của doanh nghiệp cho mục đích công việc, tránh sử dụng chúng cho mục đích cá nhân hoặc giải trí.

Tạo ra chính sách và quy trình rõ ràng: Tôi sẽ đề xuất và thực hiện các chính sách và quy trình rõ ràng về việc sử dụng tài nguyên của doanh nghiệp, đồng thời đảm bảo rằng nhân viên được đào tạo về các quy định và hạn chế liên quan đến việc truy cập thông tin của người dùng

# Tình huống 5:

**2. Nếu bạn là anh C, bạn có thực hiện tương tự như anh C không, nêu lý do tại sao?**

Nếu tôi là C, tôi sẽ không thực hiện tương tự như vậy vì:

Tuân thủ luật pháp: Sử dụng phần mềm crack là hành vi vi phạm luật pháp và có thể gây ra hậu quả pháp lý nghiêm trọng cho bản thân và doanh nghiệp. Tôi sẽ tuân thủ luật pháp và chỉ sử dụng phần mềm có bản quyền.

Bảo vệ tài sản trí tuệ: Sử dụng phần mềm crack không chỉ là hành vi không đạo đức mà còn đe dọa đến tài sản trí tuệ của các nhà sản xuất phần mềm. Tôi sẽ tôn trọng và bảo vệ tài sản trí tuệ của họ bằng cách mua các phần mềm có bản quyền.

Tránh rủi ro về an ninh mạng: Sử dụng phần mềm crack có thể mang lại rủi ro về an ninh mạng do các key crack có thể chứa mã độc hoặc phần mềm độc hại. Tôi sẽ tránh rủi ro này bằng cách chỉ sử dụng các phần mềm có bản quyền từ các nguồn tin cậy.

**3. Phân tích mối nguy hại của hành vi của C ảnh hưởng đến doanh nghiệp.**

- Mối nguy hại của hành vi của C ảnh hưởng đến doanh nghiệp:

o Tác động đến tính toàn vẹn và an ninh của hệ thống thông tin: Các phần mềm crack không đảm bảo tính toàn vẹn của hệ thống, có thể chứa mã độc và virus gây ra những thiệt hại không mong muốn cho doanh nghiệp.

o Tác động đến hiệu suất và ổn định của hệ thống: Các phần mềm crack thường không được kiểm tra kỹ lưỡng và có thể gây ra lỗi hoặc gây ảnh hưởng đến hiệu suất và ổn định của hệ thống máy tính.

o Vi phạm pháp luật bản quyền: Các phần mềm crack là hành vi vi phạm quyền sở hữu trí tuệ, có thể dẫn đến các vấn đề pháp lý và xử lý hình sự. Việc sử dụng phần mềm crack có thể ảnh hưởng đến uy tín của doanh nghiệp.

o Tác động đến tài chính của doanh nghiệp: Sử dụng phần mềm crack thay vì mua bản quyền sẽ dẫn đến chi phí thấp hơn trong thời điểm ngắn hạn, nhưng trong thời gian dài, chi phí có thể tăng lên do các vấn đề liên quan đến bảo trì, sửa chữa và nâng cấp phần mềm. Ngoài ra, việc sử dụng phần mềm crack có thể gây ra các khoản phạt và chi phí pháp lý nếu doanh nghiệp bị phát hiện vi phạm quyền sở hữu trí tuệ.

o Mất uy tín của doanh nghiệp: Việc sử dụng phần mềm crack sẽ làm giảm uy tín của doanh nghiệp trước các đối tác, khách hàng và cơ quan quản lý. Các đối tác và khách hàng có thể mất niềm tin vào doanh nghiệp vì hành vi vi phạm pháp luật bản quyền và không đảm bảo tính toàn vẹn và an ninh của hệ thống thông tin.

# Tình huống 6:2.Bạn hãy cho nhận xét về tình hình chung về việc vi phạm tương tự D ở Việt Nam, đề xuất một số giải pháp để giảm các hành vi vi phạm này.

Tình hình vi phạm tương tự như của D ở Việt Nam đang diễn ra phổ biến do sự phát triển mạnh mẽ của thương mại điện tử và việc kiểm soát trên internet không được chặt chẽ. Để giảm các hành vi vi phạm này, một số giải pháp có thể được đề xuất:

Tăng cường giáo dục và nâng cao nhận thức: Cần có sự tăng cường giáo dục về luật pháp liên quan đến thương mại điện tử, bản quyền và bảo vệ dữ liệu cá nhân. Nâng cao nhận thức cho người dùng internet về việc tuân thủ luật pháp khi hoạt động trực tuyến.

Tăng cường kiểm tra và xử lý vi phạm: Cần có sự tăng cường kiểm tra và xử lý các trang web thương mại điện tử không tuân thủ luật pháp, đặc biệt là việc không đăng ký kinh doanh và vi phạm bản quyền.

Quản lý chặt chẽ và tăng cường yêu cầu về đăng ký kinh doanh: Cơ quan quản lý phải tăng cường giám sát và yêu cầu các doanh nghiệp thương mại điện tử đăng ký kinh doanh đầy đủ để đảm bảo tuân thủ luật pháp.

Hỗ trợ và khuyến khích sử dụng phần mềm có bản quyền: Cần tăng cường hỗ trợ và khuyến khích doanh nghiệp sử dụng phần mềm có bản quyền thông qua chính sách khuyến mãi, giảm giá và chương trình đào tạo.

# Tình huống 7:2.Bạn hãy tìm hiểu xem hiện nay có những phần mềm/trang mạng xã hội nào mà thông tin cá nhân người dùng có thể bị sử dụng bất hợp pháp?

Hiện nay, có nhiều phần mềm và trang mạng xã hội có thể sử dụng thông tin cá nhân người dùng một cách bất hợp pháp, bao gồm:

Phần mềm giám sát di động: Ngoài Ptracker, còn có nhiều phần mềm giám sát khác có thể bị sử dụng bất hợp pháp để theo dõi và thu thập thông tin cá nhân người dùng điện thoại di động.

Trang mạng xã hội: Các trang mạng xã hội cũng có thể sử dụng thông tin cá nhân người dùng một cách không đúng đắn hoặc không đáng tin cậy, như việc thu thập và chia sẻ thông tin cá nhân mà không có sự cho phép của người dùng, hoặc việc sử dụng thông tin cá nhân với mục đích thương mại mà không có sự đồng ý của người dùng.

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\

# Tình huống vi phạm ACM

**Tình huống 1:**

**Trung tâm tin học của khoa công nghệ thông tin có nhiệm vụ đào tạo các khóa học ngắn hạn về CNTT cho các sinh viên của trường. Hiện nay trung tâm có một website** [**http://www.it.htt.edu.vn**](http://www.it.htt.edu.vn/) **để sinh viên xem, đăng ký và thanh toán học phí các khóa học qua website. Sau khi thi xong sinh viên cũng có thể xem kết quả của các khóa học qua website này. Người quản trị hệ thống website này phát hiện ra cơ chế thực hiện backup và Restore của hệ thống có vấn đề và nó đã không hoạt động hơn 6 tháng nay. Tuy nhiên anh ta không không biết cách khắt phục và anh ta cũng không báo cho ban giám đốc trung tâm. Tháng vừa rồi hệ thống Website bị sự cố và cần các bản backup để restore hệ thống thì không có để thực hiện.**

* **Dựa vào quy tắc ứng xử ACM, hãy phân tích các hành vi vi phạm quy tắc ứng xử vi phạm của người quản trị quản trị hệ thống, ban giám đốc.**

Dựa vào quy tắc ứng xử ACM, hành vi vi phạm quy tắc ứng xử vi phạm của người quản trị hệ thống và ban giám đốc có thể được phân tích như sau:

***o Người quản trị hệ thống:***

Vi phạm quy tắc 1.3 (Hãy trung thực và đáng tin cậy): Người quản trị không thông báo vấn đề về cơ chế backup và Restore của hệ thống cho ban giám đốc, dẫn đến việc không có bản backup khi cần thiết, gây ra hậu quả nghiêm trọng khi hệ thống gặp sự cố.

Vi phạm quy tắc 2.1 (Phấn đấu đạt chất lượng cao cả về quy trình và sản phẩm của công việc chuyên môn): Không chỉ vi phạm về khía cạnh kỹ thuật khi không sửa chữa cơ chế backup và Restore, mà còn thiếu sự chuyên nghiệp trong việc không báo cáo vấn đề này cho các cấp trên.

Vi phạm quy tắc 2.9 (Thiết kế và triển khai các hệ thống mạnh mẽ và an toàn): Không duy trì cơ chế backup và Restore hoạt động tốt, điều này vi phạm quy tắc về việc đảm bảo tính an toàn và ổn định của hệ thống.

***o Ban giám đốc:***

**Vi phạm quy tắc 2.1 (Phấn đấu đạt chất lượng cao cả về quy trình và sản phẩm của công việc chuyên môn):** Ban giám đốc không tạo điều kiện cho nhân viên, đặc biệt là người quản trị hệ thống, để báo cáo vấn đề kỹ thuật quan trọng và không kiểm soát việc duy trì cơ chế backup và Restore đúng cách.

**Vi phạm quy tắc 2.9 (Thiết kế và triển khai các hệ thống mạnh mẽ và an toàn):** Ban giám đốc chịu trách nhiệm cuối cùng trong việc đảm bảo hệ thống hoạt động một cách an toàn và hiệu quả. Việc không quản lý việc duy trì cơ chế backup và Restore có thể gây ra những hậu quả nghiêm trọng khi sự cố xảy ra.

* + **Nếu ở vị trí người quản trị hệ thống, bạn sẽ hành xử như thế nào?**

o Nếu tôi ở vị trí người quản trị hệ thống, tôi sẽ thực hiện các hành động sau:

- Khắc phục vấn đề backup và restore của hệ thống ngay lập tức.

- Báo cáo vấn đề này cho ban giám đốc và giải thích tình hình thực tế.

- Đề xuất các giải pháp khắc phục vấn đề backup và restore hệ thống, bao gồm việc tìm kiếm các giải pháp công nghệ mới để đảm bảo an toàn và đáng tin cậy cho dữ liệu của sinh viên.

- Đề xuất các biện pháp để đảm bảo việc backup và restore hệ thống được thực hiện định kỳ và được kiểm tra định kỳ để đảm bảo tính khả dụng của hệ thống.

- Tự đánh giá lại các quy trình và chính sách liên quan đến bảo mật và bảo vệ dữ liệu của trung tâm, đồng thời đề xuất các cải tiến nếu cần thiết.

o Nếu tôi là ban giám đốc của trung tâm, tôi sẽ thực hiện các hành động sau:

- Thông qua với người quản trị hệ thống để xác định tình hình thực tế và đề xuất các giải pháp khắc phục vấn đề backup và restore của hệ thống.

- Đảm bảo rằng các quy trình và chính sách liên quan đến bảo mật và bảo vệ dữ liệu được tuân thủ đầy đủ và đưa ra các biện pháp cải tiến nếu cần thiết.

- Đánh giá lại quy trình kiểm tra và bảo trì hệ thống để đảm bảo hệ thống được kiểm soát chặt chẽ, đầy đủ.

**Tham khảo:**

Xác định và khắc phục vấn đề: Tôi sẽ thực hiện một cuộc kiểm tra toàn diện về cơ chế backup và restore của hệ thống. Nếu phát hiện ra vấn đề, tôi sẽ xác định nguyên nhân và thực hiện các biện pháp cần thiết để khắc phục.

Báo cáo cho ban giám đốc: Tôi sẽ thông báo về vấn đề này cho ban giám đốc trung tâm tin học một cách trung thực và minh bạch. Tôi sẽ cung cấp thông tin chi tiết về tình trạng của cơ chế backup và restore, cùng với các biện pháp mà tôi đã thực hiện hoặc đề xuất để khắc phục vấn đề.

Thực hiện các biện pháp khẩn cấp: Nếu hệ thống đang gặp sự cố và cần các bản backup để restore, tôi sẽ thực hiện các biện pháp khẩn cấp để khôi phục dữ liệu và hoạt động của hệ thống một cách nhanh chóng và hiệu quả.

Tích hợp học bài học: Tôi sẽ rút ra bài học từ trường hợp này và đề xuất các biện pháp cần thiết để cải thiện quy trình quản lý và giám sát hệ thống, đặc biệt là về cơ chế backup và restore, để đảm bảo tính ổn định và an toàn của hệ thống trong tương lai.

**Tình huống 2:**

**Bạn A là một nhân viên IT của công ty đầu tư chứng khoán, vàng bạc, bất động sản hay nhà băng bạn A có thể theo dõi và đọc được emails, documentations, thậm chí ghi băng được những trao đổi CEO, CFO và điều này sẽ giúp bạn A mua bán stocks hữu hiệu, kiếm được nhiều tiền cho bản thân hoặc bán tin tức cho những đối thủ cạnh tranh .Trong một lần uống cafe bạn A đã tiếc lộ thông tin bảo mật cho một người bạn thân và sau đó nhận về một số tiền gọi là quà là 100 ngàn đô.**

**1.Dựa vào quy tắc ứng xử ACM, hãy phân tích các hành vi vi phạm quy tắc ứng xử vi phạm của bạn A.**

− Dựa vào quy tắc ứng xử ACM, hành vi vi phạm quy tắc ứng xử vi phạm của bạn A được phân tích như sau:

**Vi phạm quy tắc 1.2 (Tránh gây hậu quả tiêu cực):** Bạn A đã sử dụng thông tin bảo mật mà anh ta có quyền truy cập thông qua công việc của mình để mục đích cá nhân, cụ thể là để mua bán cổ phiếu và kiếm lợi ích cá nhân. Việc này không chỉ gây ra hậu quả tiêu cực cho công ty mà anh ta làm việc mà còn có thể gây ra tổn thất cho các nhà đầu tư và thị trường tài chính nói chung.

**Vi phạm quy tắc 1.3 (Hãy trung thực và đáng tin cậy):** Bạn A đã không tuân thủ quy tắc về việc cung cấp thông tin đầy đủ và chính xác về tất cả các khả năng và hạn chế của hệ thống thông tin cho các bên liên quan thích hợp. Thay vào đó, anh ta sử dụng thông tin mà không có sự cho phép hoặc hiểu biết của các bên liên quan.

**Vi phạm quy tắc 1.4 (Hãy công bằng và hành động không phân biệt đối xử):** Bạn A đã lợi dụng vị trí và quyền hạn của mình để thu thập và sử dụng thông tin bí mật cho lợi ích cá nhân, không công bằng và không đối xử công bằng với những người khác.

**Vi phạm quy tắc 1.7 (Bảo mật danh dự):** Bạn A đã vi phạm quy tắc về việc bảo vệ thông tin bí mật của công ty bằng cách tiết lộ thông tin cho người bạn thân mà không có sự cho phép của công ty.

**2.Nếu ở vị trí người người A, bạn sẽ hành xử như thế nào?**

- Nếu ở vị trí của bạn A, tôi sẽ hành xử theo quy tắc ứng xử ACM và bảo vệ thông tin bảo mật của công ty. Tôi sẽ không tiết lộ thông tin bảo mật của công ty cho bất kỳ ai, bao gồm người bạn thân nhất, và tôi sẽ không nhận bất kỳ tiền quà nào có liên quan đến việc tiết lộ thông tin bảo mật của công ty. Nếu tôi phát hiện bất kỳ hành vi vi phạm quy tắc ứng xử nào, tôi sẽ báo cáo cho các cơ quan chức năng hoặc quản lý của công ty để giải quyết vấn đề đó.

**Thêm:**

Nếu ở vị trí của bạn A, tôi sẽ:

Ngưng việc truy cập và đọc các thông tin bảo mật mà không có sự cho phép của các bên liên quan.

Thực hiện việc bảo vệ thông tin cá nhân và bảo mật thông tin một cách chặt chẽ theo quy định của công ty và luật pháp.

Thực hiện việc trung thực và minh bạch trong công việc, không tiết lộ thông tin bảo mật cho bất kỳ ai mà không có sự cho phép của các bên liên quan.

Báo cáo về việc tiếc lộ thông tin bảo mật và chấp nhận trách nhiệm pháp lý hoặc kỷ luật từ phía công ty nếu cần thiết.

Tìm cách cải thiện quy trình và biện pháp bảo mật để đảm bảo rằng việc tiếc lộ thông tin không xảy ra lại trong tương lai.

Việc tuân thủ các quy tắc ứng xử và tuân thủ pháp luật là rất quan trọng trong môi trường công việc, và nó đảm bảo rằng các hành động của bạn không gây ra hậu quả tiêu cực cho bạn và cho công ty.

Nếu có vấn đề về cơ chế backup và Restore của hệ thống, tôi sẽ tìm kiếm cách để khắc phục vấn đề này hoặc đề xuất các biện pháp cải thiện cho cấp trên.

# Tình huống 3:

**Bạn là kỹ sư phần mềm tại một công ty mới thành lập. Công ty đang phát triển một ứng dụng mới cho phép nhân viên bán hàng tạo ra và gửi email báo giá bán hàng và hóa đơn của khách hàng từ điện thoại thông minh của họ. Bộ phận maketing của công ty bạn đã giới thiệu ứng dụng này cho một tập đoàn lớn và nói rằng ứng dụng này hiện nay đã sẳn sàng. Nhưng thực tế, tại thời điểm này ứng dụng vẫn còn chứa khá nhiều lỗi, cần phải hơn 1 tháng thì ứng dụng mới được khắc phục các lổi nghiêm trọng. Tuy nhiên, trưởng nhóm testing đã báo cáo rằng tất cả các lỗi đã được tìm ra và có thể khắc phục dễ dàng. Do sự cạnh tranh khốc liệt trong ngành công nghiệp phần mềm trên điện thoại thông minh, ban giám đốc quyết định công ty phải là “người đầu tiên” đưa ứng dụng này ra thị trường cho dù vẫn biết ứng dụng chưa hoàn chỉnh. Nếu sản phẩm này không xuất hiện đầu tiên, công ty khởi nghiệp của bạn có thể sẽ bị pháp sản. Bạn là người có trách nhiệm đưa sản phẩm đó ra thị trường.**

**1.Dựa vào quy tắc ứng xử ACM, hãy phân tích các hành vi vi phạm quy tắc ứng xử vi phạm của ban giám đốc.**

- Vi phạm quy tắc ứng xử ACM của ban giám đốc:

**Vi phạm quy tắc 1.2 (Tránh gây hậu quả tiêu cực):** Ban giám đốc đã quyết định đưa ứng dụng ra thị trường mặc dù biết rằng nó vẫn chứa nhiều lỗi nghiêm trọng. Hành động này có thể gây ra hậu quả tiêu cực cho khách hàng khi họ sử dụng sản phẩm chưa hoàn chỉnh, có thể dẫn đến mất mát dữ liệu hoặc trải qua trải nghiệm người dùng không tốt.

**Vi phạm quy tắc 1.3 (Hãy trung thực và đáng tin cậy):** Ban giám đốc đã không cung cấp thông tin đầy đủ và chính xác về trạng thái thực sự của sản phẩm cho khách hàng và các bên liên quan. Thay vào đó, anh ta đã chấp nhận sự cố che giấu thông tin và lựa chọn đưa sản phẩm ra thị trường mặc dù biết rằng nó chưa hoàn chỉnh.

**Vi phạm quy tắc 2.1 (Phấn đấu đạt chất lượng cao cả về quy trình và sản phẩm của công việc chuyên môn):** Ban giám đốc đã không tuân thủ quy tắc về việc đảm bảo chất lượng sản phẩm trước khi đưa ra thị trường. Thay vào đó, anh ta đã chấp nhận việc tung ra sản phẩm chưa hoàn chỉnh với mục tiêu là "người đầu tiên" trên thị trường.

**Vi phạm quy tắc 2.6 (Chỉ thực hiện công việc trong các lĩnh vực có thẩm quyền):** Ban giám đốc đã không đánh giá tính khả thi của việc đưa sản phẩm chưa hoàn chỉnh ra thị trường và đã quyết định thực hiện hành động này mặc dù biết rằng nó không đảm bảo tính chuyên nghiệp và không phù hợp với các quy định và tiêu chuẩn trong ngành.

**2.Dựa vào quy tắc ứng xử ACM, hãy phân tích các hành vi vi phạm quy tắc ứng xử vi phạm của bạn nếu bạn đồng ý đưa sản phẩm ra trong tuần tới.**

Vi phạm quy tắc ứng xử ACM của tôi:

**Vi phạm quy tắc 1.1 (Đóng góp cho xã hội và làm cho con người hạnh phúc):**Việc đưa ra sản phẩm chưa hoàn chỉnh và chứa lỗi có thể gây ra những hậu quả tiêu cực cho người dùng, từ việc gặp khó khăn trong việc sử dụng đến mất thông tin quan trọng.

**Vi phạm quy tắc 1.2 (Tránh gây hậu quả tiêu cực):**Việc đưa ra sản phẩm chưa hoàn chỉnh và không kiểm tra kỹ lưỡng có thể dẫn đến những hậu quả tiêu cực, bao gồm sự không hài lòng của khách hàng, sự mất lòng tin từ phía khách hàng và ảnh hưởng đến uy tín của công ty.

**Vi phạm quy tắc 2.1 (Phấn đấu đạt chất lượng cao cả về quy trình và sản phẩm của công việc chuyên môn):**Bằng việc chấp nhận đưa ra sản phẩm chưa hoàn chỉnh, tôi vi phạm quy tắc về việc phấn đấu đạt chất lượng cao cho sản phẩm của công việc chuyên môn.

**Vi phạm quy tắc 2.9 (Thiết kế và triển khai các hệ thống mạnh mẽ và an toàn):**Đưa ra sản phẩm chưa hoàn chỉnh có thể đặt người dùng vào tình huống rủi ro và không an toàn, đặc biệt nếu sản phẩm liên quan đến giao dịch tài chính như trong trường hợp này.

**Vi phạm quy tắc 1.3 (Hãy trung thực và đáng tin cậy):**Việc đưa ra sản phẩm mà biết rằng nó chưa hoàn thiện và có lỗi mà không cung cấp thông tin đầy đủ và chính xác cho khách hàng là không trung thực và không đáng tin cậy.

**3.Nếu bạn muốn đưa sản phẩm ra tuần tới mà không vi phạm quy tắc xứng xử thì bạn sẽ làm gì và giải thích lý do tại sao**

- Để đưa sản phẩm ra thị trường mà không vi phạm quy tắc ứng xử ACM, tôi có thể:

o Thông báo cho khách hàng rằng sản phẩm vẫn chưa hoàn thiện và còn một số lỗi cần được khắc phục. Bạn có thể cung cấp danh sách các lỗi đang được sửa chữa và thời gian dự kiến để hoàn thành sửa chữa các lỗi này.

o Cung cấp cho khách hàng phiên bản thử nghiệm của sản phẩm để họ có thể kiểm tra trước khi mua sản phẩm.

# Tình huống 4:

**Bạn làm cho công ty chuyên thiết kế Website cho các khách hàng. Ban lãnh đạo của công ty luôn yêu cầu bạn dùng chính Website của khách hàng mà công ty thiết kế để đi backlinks cho Website công ty mình. Mục tiêu là SEO Website cho công ty. Các khách hàng không hề biết việc làm này của công ty. Và điều đáng nói hơn nữa là có những website công ty đặt backlink thông qua một dòng text có fontsize nhỏ (2px),màu chữ trắng vì sợ khách hàng biết và phàn nàn. Bạn đã làm đều này từ nhiều năm trước đến nay.**

**1.Dựa vào quy tắc ứng xử ACM, hãy phân tích các hành vi vi phạm quy tắc ứng xử vi phạm của ban giám đốc công ty.**

Theo quy tắc ứng xử ACM, hành vi vi phạm quy tắc ứng xử của ban giám đốc công ty bao gồm:

**Quy tắc 1.1 - Đóng góp cho xã hội và làm cho con người hạnh phúc:**Bạn giám đốc vi phạm nguyên tắc này bằng cách sử dụng website của khách hàng mà không có sự đồng ý của họ để tạo backlinks cho công ty của mình. Hành vi này không chỉ không đóng góp cho xã hội mà còn có thể gây phiền toái và mất lòng tin từ phía khách hàng.

**Quy tắc 1.2 - Tránh gây hậu quả tiêu cực:**Bằng việc đặt backlinks không được sự chấp thuận từ khách hàng, bạn giám đốc đã gây ra hậu quả tiêu cực có thể làm mất uy tín và danh tiếng của họ nếu hành động này được phát hiện.

**Quy tắc 1.3 - Trung thực và đáng tin cậy:**Bạn giám đốc không trung thực khi không cung cấp đầy đủ thông tin và không thông báo cho khách hàng về việc sử dụng website của họ để tạo backlinks cho công ty.

**Quy tắc 1.4 - Hãy công bằng và hành động không phân biệt đối xử:**Hành động này không công bằng với khách hàng vì không có sự cho phép từ họ. Việc sử dụng website của họ mà không được sự đồng ý là hành động không phân biệt đối xử.

**Quy tắc 1.6 - Tôn trọng quyền riêng tư:**Bằng cách sử dụng website của khách hàng để đặt backlinks mà không được sự chấp thuận, bạn giám đốc đã vi phạm quyền riêng tư và không tôn trọng quyền riêng tư của khách hàng.

**Quy tắc 2.1 (Phấn đấu đạt chất lượng cao cả về quy trình và sản phẩm của công việc chuyên môn):**Hành động này không đảm bảo chất lượng cao cả về quy trình và sản phẩm của công việc chuyên môn vì nó liên quan đến việc sử dụng phương pháp không đạo đức để tăng cường SEO.

**Quy tắc 3.1 - Đảm bảo rằng lợi ích công cộng là mối quan tâm chính:** Hành vi vi phạm này không đảm bảo rằng lợi ích công cộng là mối quan tâm chính. Thay vào đó, nó tập trung vào lợi ích cá nhân của công ty mà không xem xét đến hậu quả có thể gây ra cho khách hàng và cộng đồng internet.

**2.Dựa vào quy tắc ứng xử ACM, hãy phân tích các hành vi vi phạm quy tắc ứng xử vi phạm của chính bạn.**

Theo quy tắc ứng xử ACM, hành vi vi phạm quy tắc ứng xử của bạn bao gồm:

**Quy tắc 1.3 - Tránh gây hậu quả tiêu cực và 1.4 - Hãy công bằng và hành động không phân biệt đối xử:** Việc sử dụng các phương pháp không minh bạch và không công bằng để tạo backlink không chỉ có thể dẫn đến các hậu quả tiêu cực cho khách hàng và người dùng, mà còn là một hành động không công bằng và không trung thực với họ.

**Quy tắc 1.6 - Tôn trọng quyền riêng tư:**Việc đặt backlink mà không được sự cho phép của các chủ sở hữu trang web có thể vi phạm quyền riêng tư của họ và cách sử dụng thông tin trên trang web của họ.

**Quy tắc 2.2 - Duy trì các tiêu chuẩn cao về năng lực chuyên môn, hành vi và thực hành đạo đức:**Sử dụng các phương pháp không đạo đức để thúc đẩy SEO có thể vi phạm tiêu chuẩn đạo đức của một chuyên gia máy tính và không duy trì tiêu chuẩn cao về hành vi và thực hành đạo đức.

**Quy tắc 4 - Tuân thủ bộ quy tắc đạo đức:**Vi phạm các quy tắc đạo đức này không chỉ là vi phạm quy tắc ACM mà còn làm mất đi tính đáng tin cậy và uy tín của người làm trong lĩnh vực công nghệ thông tin.

Những hành vi này không chỉ vi phạm quy tắc ứng xử ACM mà còn có thể gây ra hậu quả nghiêm trọng đối với uy tín và lòng tin của công ty trong mắt khách hàng. Đồng thời, cũng có thể đặt công ty vào tình thế pháp lý không mong muốn nếu bị phát hiện.

# Tình huống 5:

**Một sinh viên ngành CNTT rất đam mê công việc của một bác sĩ máy tính chuyên cứu hộ các máy tính bị tấn công bởi các mã độc, phân tích các mối đe dọa của một hệ thống thông tin để từ đó cài đặt các cơ chế phù hợp để giảm thiểu các rũi ro cho hệ thống thông tin đó. Vì vậy, sinh viên này thường xuyên vào các diễn dàn để tìm hiểu, học hỏi các kỹ thuật tấn công, các mã độc, các kỹ thuật tìm kiếm các lỗ hỏng của các công nghệ,… Sau đó thực hiện thử nghiệm hết tất cả các kỹ thuật đã học hỏi vào bất cứ hệ thống thông tin bất kỳ mà mình thích. Kết quả đến nay đã thử nghiệm thành công rất nhiều công cụ và kỹ thuật đã học hỏi và làm nhiều máy tính, cũng như website của nạn nhận lao đao vì các thử nghiệm này. Ngoài ra trong một lần tấn công thử nghiệm, người này đã sao chép được rất nhiều thông tin bảo mật của hệ thống này. Sau đó người này đem các thông tin này đăng tải lên các diễn đàn công cộng như là chiến tích của cá nhân mình.**

**1.Dựa vào quy tắc ứng xử ACM, hãy phân tích các hành vi vi phạm quy tắc ứng xử vi phạm của sinh viên này.**

**Quy tắc 1.1 - Đóng góp cho xã hội và làm cho con người hạnh phúc:**Hành động tấn công vào các hệ thống thông tin và công khai thông tin bảo mật của hệ thống làm tăng nguy cơ gây hậu quả tiêu cực cho người sử dụng hệ thống và ảnh hưởng đến sự hạnh phúc và an ninh của họ.

**Quy tắc 1.2 - Tránh gây hậu quả tiêu cực:**Bằng cách thử nghiệm các kỹ thuật tấn công và công khai thông tin bảo mật của các hệ thống, sinh viên này gây ra các hậu quả tiêu cực không mong muốn cho các nạn nhân và hệ thống mà họ không biết hoặc chấp thuận.

**Quy tắc 1.3 - Hãy trung thực và đáng tin cậy:**Việc sao chép thông tin bảo mật của hệ thống và đăng tải lên các diễn đàn công cộng như là chiến tích cá nhân là không trung thực và không đáng tin cậy.

**Quy tắc 1.6 - Tôn trọng quyền riêng tư:**Việc công khai thông tin bảo mật của các hệ thống thông tin là vi phạm quyền riêng tư của chủ sở hữu hệ thống và người dùng của họ.

**Quy tắc 2.7 - Nhận thức, các công nghệ liên quan và hậu quả của chúng:**Sinh viên này không chỉ không nhận thức được hậu quả của hành động tấn công của mình mà còn tự hào và công khai về chúng, không quan tâm đến ảnh hưởng tiêu cực đối với người dùng và tổ chức.

**Quy tắc 4 - Tuân thủ bộ quy tắc đạo đức:**Hành động của sinh viên này không tuân thủ các nguyên tắc đạo đức của ACM, đặc biệt là việc tôn trọng quyền riêng tư, an ninh và sự an toàn của người dùng và hệ thống thông tin.

**Quy tắc 2.2 - Duy trì các tiêu chuẩn cao về năng lực chuyên môn, hành vi và thực hành đạo đức**: Sinh viên không tuân thủ quy tắc này bằng cách thực hiện các hành động không đạo đức và không chuyên nghiệp, đặc biệt là việc thử nghiệm các kỹ thuật tấn công trên các hệ thống thông tin mà không có sự chấp thuận hoặc hiểu biết sâu sắc về các hệ thống đó.

**Quy tắc 3.1 - Đảm bảo rằng lợi ích công cộng là mối quan tâm chính**: Sinh viên không tuân thủ quy tắc này bằng cách không đặt lợi ích công cộng lên hàng đầu mà thay vào đó tập trung vào việc thực hiện các hành động cá nhân mà không xem xét đến hậu quả tiêu cực đối với cộng đồng hoặc tổ chức.

**2.Nếu bạn là bạn của sinh viên này, bạn sẽ khuyên nhủ như thế nào hay làm gì để bạn ấy nhận ra hành vi vi phạm của mình**

Thảo luận về hậu quả của hành động:Tôi sẽ giải thích cho anh ấy hiểu rõ hậu quả của hành động của mình đối với người dùng và tổ chức. Tôi sẽ nhấn mạnh rằng việc tấn công hệ thống thông tin và công khai thông tin bảo mật không chỉ ảnh hưởng đến sự tin cậy của người dùng mà còn có thể gây ra những hậu quả tiêu cực nghiêm trọng cho họ.

Giải thích về đạo đức và trách nhiệm:Tôi sẽ nhắc anh ấy về quy tắc đạo đức trong lĩnh vực công nghệ thông tin và trách nhiệm của một chuyên gia trong việc bảo vệ thông tin cá nhân và an ninh mạng. Tôi sẽ giải thích rằng mỗi cá nhân hoặc chuyên gia máy tính đều có trách nhiệm đối với việc sử dụng công nghệ một cách đạo đức và trách nhiệm.

Khuyến khích hành động tích cực:Tôi sẽ khuyến khích anh ấy tham gia vào các hoạt động tích cực và hợp pháp trong lĩnh vực an ninh mạng, như tham gia các cuộc thi hợp pháp, nghiên cứu các phương pháp bảo mật và tham gia cộng đồng an ninh mạng.

Đề xuất học hỏi từ các nguồn chính thống:Tôi sẽ đề xuất anh ấy tìm kiếm thông tin và học hỏi từ các nguồn chính thống như sách vở, tài liệu học tập, khóa học trực tuyến hoặc tham gia các cộng đồng an ninh mạng chính thống để nâng cao kiến thức và kỹ năng mà không vi phạm đạo đức.

Nhấn mạnh về trách nhiệm và tự giác:Tôi sẽ nhấn mạnh rằng trách nhiệm và tự giác là hai yếu tố quan trọng mà mỗi chuyên gia máy tính cần phải có. Anh ấy cần nhận thức rõ trách nhiệm của mình và hành động một cách có ý thức để đảm bảo an toàn và bảo mật cho mọi người và tổ chức.**Top of Form**

**Tham khảo:**

Bạn của sinh viên này có thể khuyên nhủ anh ta về những hậu quả pháp lý và đạo đức của hành vi của mình. Nhấn mạnh rằng việc xâm phạm vào quyền riêng tư và bảo mật của người khác là không đạo đức và có thể gây ra những hậu quả nghiêm trọng.

Bạn có thể khuyên sinh viên này tìm kiếm các cách thức hợp pháp và đạo đức để phát triển kỹ năng của mình trong lĩnh vực an ninh mạng và bảo mật thông tin. Đề xuất cho anh ta tham gia vào các hoạt động hợp pháp như các chương trình bug bounty hoặc các khóa học về an ninh mạng để thực hiện các thử nghiệm mà không gây hại cho người khác.

Đồng thời, bạn có thể khuyến khích sinh viên này tìm hiểu về quy tắc ứng xử ACM và nhấn mạnh tầm quan trọng của việc tuân thủ các quy định đạo đức và pháp luật trong lĩnh vực CNTT.

# Tình huống 6:

**A là nhóm trưởng của một tổ quản trị hệ thống thông tin gồm có 4 thành viên. Nhiệm vụ của nhóm là bảo trì và nâng cấp hệ thống thông tin của doanh nghiệp. Trong một sự cố một số dữ liệu quan trọng của doanh nghiệp bị mất và không thể phục hồi được. Vì A là nhóm trưởng nên đã bị chủ doanh nghiệp cho nghỉ việc trong khi các thành viên khác vẫn làm việc bình thường. Sau khi bạn nghỉ việc thì bạn B là một trong 3 bạn còn lại được đưa lên làm nhóm trưởng. Sau này A đã phát hiện ra rằng sự cố lúc trước là một sự cố có sự sắp đặt cố ý của B nhằm loại trừ A ra khỏi doanh nghiệp để chiếm vị trí của A. A cảm thấy thù ghét B và muốn trả thù B. A tìm hiểu các kỹ thuật tấn công và sự hiểu biết ngọn ngành về hệ thống thông tin của doanh nghiệp cũ, A đã thực hiện các tấn công và làm điêu đứng hệ thống thông tin của doanh nghiệp nhiều lần.**

**1.Dựa vào quy tắc ứng xử ACM, hãy phân tích các hành vi vi phạm quy tắc ứng xử vi phạm của A.**

- Vi phạm quy tắc ứng xử ACM của A:

**Quy tắc 1.1 - Đóng góp cho xã hội và làm cho con người hạnh phúc:**A vi phạm quy tắc này bằng cách tấn công và làm hỏng hệ thống thông tin của doanh nghiệp, gây ảnh hưởng đến sự vận hành của doanh nghiệp và có thể gây tổn thất kinh doanh. Hành động này không đóng góp vào sự hạnh phúc và sự an toàn của cộng đồng.

**Quy tắc 1.2 - Tránh gây hậu quả tiêu cực:**Bằng cách tấn công hệ thống thông tin của doanh nghiệp, A gây ra hậu quả tiêu cực nghiêm trọng cho doanh nghiệp, bao gồm mất mát dữ liệu quan trọng không thể phục hồi và sự gián đoạn trong hoạt động kinh doanh.

**Quy tắc 1.3 - Hãy trung thực và đáng tin cậy:**A không tuân thủ quy tắc này bằng cách thực hiện các hành động tấn công mà không tiết lộ hoặc đưa ra cảnh báo trước cho doanh nghiệp, không cung cấp thông tin đầy đủ và trung thực về mục đích hoặc hậu quả của hành động của mình.

**Quy tắc 2.1 - Phấn đấu đạt chất lượng cao cả về quy trình và sản phẩm của công việc chuyên môn:**A không tuân thủ quy tắc này bằng cách thực hiện các hành động tấn công hệ thống thông tin của doanh nghiệp mà không có mục tiêu cụ thể hoặc kế hoạch đảm bảo chất lượng công việc.

**Quy tắc 2.2 - Duy trì các tiêu chuẩn cao về năng lực chuyên môn, hành vi và thực hành đạo đức:**Bằng cách thực hiện các hành động tấn công hệ thống thông tin của doanh nghiệp, A không chỉ vi phạm các tiêu chuẩn chuyên môn mà còn đặt ra các hành vi không đạo đức và không chuyên nghiệp trong lĩnh vực của mình.

**Quy tắc 3.1 - Đảm bảo rằng lợi ích công cộng là mối quan tâm chính:**A không tuân thủ quy tắc này bằng cách đặt lợi ích cá nhân và ý muốn trả thù lên hàng đầu, thay vì quan tâm đến lợi ích của doanh nghiệp và cộng đồng.

**2.Dựa vào quy tắc ứng xử ACM, hãy phân tích các hành vi vi phạm quy tắc ứng xử vi phạm của B.**

- Vi phạm quy tắc ứng xử ACM của B:

**Quy tắc 1.1 - Đóng góp cho xã hội và làm cho con người hạnh phúc:**B vi phạm quy tắc này bằng cách sắp đặt cố ý sự cố để loại bỏ A ra khỏi doanh nghiệp, không chỉ gây ảnh hưởng đến A mà còn ảnh hưởng đến sự ổn định của hệ thống thông tin của doanh nghiệp và có thể gây thiệt hại cho doanh nghiệp và cộng đồng.

**Quy tắc 1.2 - Tránh gây hậu quả tiêu cực:**B vi phạm quy tắc này bằng cách gây ra sự cố tình cố ý trong hệ thống thông tin của doanh nghiệp, dẫn đến mất mát dữ liệu quan trọng không thể phục hồi và sự gián đoạn trong hoạt động kinh doanh.

**Quy tắc 1.3 - Hãy trung thực và đáng tin cậy:**B không tuân thủ quy tắc này bằng cách không tiết lộ hoặc đưa ra cảnh báo trước cho doanh nghiệp về ý định hoặc hậu quả của việc sắp đặt sự cố, và không cung cấp thông tin đầy đủ và trung thực về mục đích của hành động của mình.

**Quy tắc 2.1 - Phấn đấu đạt chất lượng cao:**B vi phạm quy tắc này bằng cách thực hiện hành động không đạo đức và không chuyên nghiệp để loại bỏ A ra khỏi doanh nghiệp và chiếm vị trí của A, thay vì tập trung vào việc cải thiện và bảo trì hệ thống thông tin của doanh nghiệp.

**Quy tắc 3.1 - Đảm bảo rằng lợi ích công cộng là mối quan tâm chính:**B không tuân thủ quy tắc này bằng cách đặt lợi ích cá nhân lên hàng đầu, thay vì quan tâm đến lợi ích của doanh nghiệp và cộng đồng.

# Tình huống 7:

**C là người quản trị khoảng 20 máy tính nối mạng của một công ty nhỏ. Mọi vấn đề liên quan đến việc cài đặt, cấu hình các phần cứng cũng như phần mềm trên hệ thống máy tính Ban giám đốc đều giao cho bạn C tự quyết và tự thực hiện, chủ công ty tin tưởng và giao khoán hết cho anh C. Khi cài mới hoặc cập nhật các phần mềm anh C đều có các đề xuất chi tiền mua các phần mềm có bản quyền. Tuy nhiên anh C không bao giờ mua các phần mềm có bản quyền đó về cài đặt mà chỉ cài đặt các bản crack. Số tiền mua bản quyền hằng năm anh C chiếm đoạt hết. Do dùng các phần mềm crack nên thỉnh thoảng anh C phải tìm các key crack trên các trang crack để cấu hình lại các phần mềm.**

**1.Dựa vào quy tắc ứng xử ACM, hãy phân tích các hành vi vi phạm quy tắc ứng xử vi phạm của C.**

- Dựa trên quy tắc ứng xử ACM, hành vi của C vi phạm quy tắc ứng xử ACM ở các điểm sau:

**Quy tắc 1.1 - Đóng góp cho xã hội và làm cho con người hạnh phúc:**C vi phạm quy tắc này bằng cách không đảm bảo chất lượng và tính bảo mật của hệ thống máy tính của công ty. Việc sử dụng phần mềm crack không chỉ là vi phạm bản quyền mà còn tiềm ẩn các rủi ro về an ninh thông tin và ổn định của hệ thống.

**Quy tắc 1.2 - Tránh gây hậu quả tiêu cực:**Việc sử dụng phần mềm crack có thể gây ra các hậu quả tiêu cực như mất dữ liệu, lỗ hổng bảo mật, và rủi ro pháp lý cho doanh nghiệp. Điều này không chỉ ảnh hưởng đến công ty mà còn có thể ảnh hưởng đến khách hàng và người dùng cuối.

**Quy tắc 1.3 - Hãy trung thực và đáng tin cậy:**C vi phạm quy tắc này bằng cách không cung cấp thông tin đầy đủ và trung thực về việc sử dụng phần mềm crack và ảnh hưởng của nó đối với công ty. Anh ta cũng không tuân thủ quy tắc về việc mua bản quyền phần mềm như yêu cầu từ ban lãnh đạo.

**Quy tắc 2.1 - Phấn đấu đạt chất lượng cao cả về quy trình và sản phẩm của công việc chuyên môn:**C không phấn đấu đạt chất lượng cao trong công việc của mình khi anh ta sử dụng phần mềm crack thay vì các phần mềm có bản quyền, điều này ảnh hưởng đến tính ổn định và an toàn của hệ thống máy tính.

**Quy tắc 2.3 - Biết và tôn trọng các quy tắc hiện hành liên quan đến công việc chuyên môn:**C không tuân thủ các quy tắc và luật pháp liên quan đến việc sử dụng phần mềm và bản quyền, đặc biệt là trong lĩnh vực công nghệ thông tin.

**Quy tắc 1.4 - Hãy công bằng và hành động không phân biệt đối xử:**C vi phạm quy tắc này bằng cách không đối xử công bằng với các nhà cung cấp phần mềm, không trả giá trị công bằng cho sản phẩm mà họ cung cấp. Thay vào đó, anh ta lợi dụng và chiếm đoạt các phần mềm thông qua việc sử dụng crack.

**Quy tắc 2.2 - Duy trì các tiêu chuẩn cao về năng lực chuyên môn,hành vi và thực hành đạo đức:**C không duy trì tiêu chuẩn cao về năng lực chuyên môn khi sử dụng phần mềm crack thay vì các phần mềm có bản quyền. Điều này không chỉ làm giảm giá trị của kiến thức và kỹ năng của anh ta mà còn đe dọa uy tín của công ty và sự tin cậy của khách hàng.

**Quy tắc 2.7 - Nhận thức, các công nghệ liên quan và hậu quả của chúng:**C vi phạm quy tắc này bằng cách không hiểu rõ về các rủi ro và hậu quả của việc sử dụng phần mềm crack, bao gồm cả vấn đề về bảo mật thông tin và tiềm ẩn các lỗ hổng trong hệ thống máy tính.

**Quy tắc 2.9 - Thiết kế và triển khai các hệ thống mạnh mẽ và an toàn:**Bằng cách sử dụng phần mềm crack, C không đảm bảo rằng hệ thống máy tính của công ty được triển khai với các biện pháp bảo mật mạnh mẽ và an toàn. Thay vào đó, anh ta tạo ra một môi trường không ổn định và dễ bị tấn công.

**Quy tắc 4 - Tuân thủ Bộ quy tắc đạo đức:**C vi phạm quy tắc này bằng cách không tuân thủ các quy tắc đạo đức được xác định trong lĩnh vực công nghệ thông tin. Thay vào đó, anh ta chọn lựa các hành động không đạo đức như sử dụng phần mềm crack và chiếm đoạt tiền của công ty cho mục đích cá nhân

**2.Phân tích mối nguy hại của hành vi của C ảnh hưởng đến doanh nghiệp.**

- Mối nguy hại của hành vi của C ảnh hưởng đến doanh nghiệp:

o Tác động đến tính toàn vẹn và an ninh của hệ thống thông tin: Các phần mềm crack không đảm bảo tính toàn vẹn của hệ thống, có thể chứa mã độc và virus gây ra những thiệt hại không mong muốn cho doanh nghiệp.

o Tác động đến hiệu suất và ổn định của hệ thống: Các phần mềm crack thường không được kiểm tra kỹ lưỡng và có thể gây ra lỗi hoặc gây ảnh hưởng đến hiệu suất và ổn định của hệ thống máy tính.

o Vi phạm pháp luật bản quyền: Các phần mềm crack là hành vi vi phạm quyền sở hữu trí tuệ, có thể dẫn đến các vấn đề pháp lý và xử lý hình sự. Việc sử dụng phần mềm crack có thể ảnh hưởng đến uy tín của doanh nghiệp.

o Tác động đến tài chính của doanh nghiệp: Sử dụng phần mềm crack thay vì mua bản quyền sẽ dẫn đến chi phí thấp hơn trong thời điểm ngắn hạn, nhưng trong thời gian dài, chi phí có thể tăng lên do các vấn đề liên quan đến bảo trì, sửa chữa và nâng cấp phần mềm. Ngoài ra, việc sử dụng phần mềm crack có thể gây ra các khoản phạt và chi phí pháp lý nếu doanh nghiệp bị phát hiện vi phạm quyền sở hữu trí tuệ.

o Mất uy tín của doanh nghiệp: Việc sử dụng phần mềm crack sẽ làm giảm uy tín của doanh nghiệp trước các đối tác, khách hàng và cơ quan quản lý. Các đối tác và khách hàng có thể mất niềm tin vào doanh nghiệp vì hành vi vi phạm pháp luật bản quyền và không đảm bảo tính toàn vẹn và an ninh của hệ thống thông tin.

**Tham khảo**

Nguy cơ bị tấn công từ mã độc và phần mềm độc hại: Việc sử dụng phần mềm crack tạo điều kiện cho các hacker tiềm ẩn các mã độc vào hệ thống của công ty, gây mất bảo mật thông tin, rủi ro mất dữ liệu quan trọng và ảnh hưởng đến hoạt động kinh doanh.

Rủi ro pháp lý và tài chính: Việc sử dụng phần mềm crack vi phạm bản quyền có thể gây ra hậu quả pháp lý nghiêm trọng đối với doanh nghiệp, bao gồm việc phải trả tiền phạt lớn và mất uy tín trên thị trường, có thể dẫn đến giảm doanh thu và tổn thất tài chính đáng kể.

**Tình huống 8:**

**Hơn 14.000 điện thoại ở Việt Nam đã bị một công ty tư nhân nghe lén. Các điện thoại này bị theo dõi tin nhắn, danh bạ, ghi âm cuộc gọi, định vị điện thoại, quay phim, chụp ảnh... Nghiêm trọng hơn, toàn bộ dữ liệu được gửi về máy chủ của công ty này. Kết quả thanh tra đã khiến người sử dụng điện thoại ở Việt Nam cảm thấy lo lắng. Đoàn thanh tra liên ngành gồm thanh tra Sở Thông tin và Truyền thông Hà Nội, phòng Cảnh sát phòng chống tội phạm sử dụng công nghệ cao - PC50 của Công an Hà Nội đã thanh tra tại công ty TNHH công nghệ Việt Hồng ở quận Thanh Xuân, Hà Nội và phát hiện công ty này kinh doanh phần mềm Ptraker. Đây là phần mềm giúp người dùng có thể xem tin nhắn, danh bạ, ghi âm cuộc gọi, định vị điện thoại, quay phim, chụp ảnh, bật - tắt 3G/GPRS của điện thoại bị giám sát. Thậm chí người sử dụng còn có thể ra lệnh điều khiển từ xa điện thoại bị cài Ptracker bằng cách nhắn tin tới điện thoại này**

**1.Dựa vào quy tắc ứng xử ACM, hãy phân tích các hành vi vi phạm quy tắc ứng xử vi phạm của người ra quyết định kinh doanh phần mềm này.**

Phân tích hành vi vi phạm quy tắc ứng xử của người ra quyết định kinh doanh phần mềm Ptracker:

**Quy tắc 1.1 - Đóng góp cho xã hội và làm cho con người hạnh phúc:**Việc phát triển và kinh doanh phần mềm Ptracker vi phạm quy tắc này bởi nó làm ảnh hưởng tiêu cực đến sự riêng tư và an ninh của người dùng điện thoại. Sự vi phạm này góp phần làm suy giảm niềm tin của người dùng vào công nghệ và gây ra lo ngại về an toàn thông tin cá nhân.

**Quy tắc 1.2 - Tránh gây hậu quả tiêu cực:**Việc sử dụng phần mềm Ptracker để nghe lén, theo dõi và thu thập thông tin cá nhân của người dùng điện thoại gây ra các hậu quả tiêu cực nghiêm trọng, bao gồm vi phạm quyền riêng tư, gây lo lắng và mất niềm tin từ phía người dùng.

**Quy tắc 1.3 - Trung thực và đáng tin cậy:**Người ra quyết định kinh doanh phần mềm Ptracker không tuân thủ quy tắc này bởi việc không cung cấp đầy đủ thông tin cho người dùng về mục đích và phạm vi của việc thu thập thông tin cá nhân của họ.

**Quy tắc 1.6 - Tôn trọng quyền riêng tư:**Vi phạm quy tắc này bởi việc sử dụng phần mềm Ptracker để thu thập thông tin cá nhân của người dùng mà không có sự đồng ý của họ, và không cung cấp các cơ chế cho người dùng kiểm soát và bảo vệ quyền riêng tư của mình.

**Quy tắc 4 - Tuân thủ Bộ quy tắc đạo đức:**Hành vi kinh doanh phần mềm Ptracker vi phạm quy tắc này bởi việc không tuân thủ các quy tắc đạo đức cơ bản trong việc sử dụng công nghệ và không tôn trọng quyền riêng tư và an ninh thông tin của người dùng.

**2.Dựa vào quy tắc ứng xử ACM, hãy phân tích các hành vi vi phạm quy tắc ứng xử vi phạm của người dùng phần mềm trên để theo dõi và điều khiển điện thoại của người khác**

Dựa vào quy tắc ứng xử ACM, hãy phân tích các hành vi vi phạm quy tắc ứng xử vi phạm của người dùng phần mềm trên để theo dõi và điều khiển điện thoại của người khác.

**Quy tắc 1.1 - Đóng góp cho xã hội và làm cho con người hạnh phúc:**Hành vi theo dõi và điều khiển điện thoại của người khác không đóng góp vào việc làm cho con người hạnh phúc. Thay vào đó, nó làm gia tăng sự lo ngại và mất an ninh thông tin cho người dùng bị theo dõi, tạo ra một môi trường không tin cậy trong xã hội.

**Quy tắc 1.3 - Tránh gây hậu quả tiêu cực:**Hành vi này gây ra hậu quả tiêu cực rất lớn cho người bị theo dõi. Bằng cách xâm nhập vào quyền riêng tư và an ninh cá nhân của họ, người dùng phần mềm này tạo ra sự không an toàn và lo lắng trong cộng đồng.

**Quy tắc 1.6 - Tôn trọng quyền riêng tư:**Việc theo dõi và điều khiển điện thoại của người khác là một vi phạm trực tiếp đến quyền riêng tư của họ. Bằng cách thu thập dữ liệu cá nhân và kiểm soát thiết bị mà không có sự đồng ý của chủ sở hữu, người dùng phần mềm vi phạm quyền riêng tư và không tôn trọng tính riêng tư của người khác.

**Quy tắc 2.3 - Biết và tôn trọng các quy tắc hiện hành:**Người dùng phần mềm không tuân thủ các quy tắc và luật lệ hiện hành về quyền riêng tư và an ninh thông tin. Thay vào đó, họ chọn lựa các hành động không đạo đức để xâm nhập vào quyền riêng tư của người khác mà không có sự đồng ý hoặc sự hiểu biết từ phía họ.

**Quy tắc 4 - Tuân thủ Bộ quy tắc đạo đức:**Hành vi của người dùng phần mềm không tuân thủ các quy tắc đạo đức được xác định trong lĩnh vực công nghệ thông tin. Thay vào đó, họ lựa chọn các hành động không đạo đức như việc xâm nhập vào quyền riêng tư của người khác và kiểm soát thiết bị của họ mà không có sự cho phép hoặc sự hiểu biết.

# Tình huống 09:

**Để giám sát tất cả hành động truy cập web của các nhân viên trong công ty. Ban giám đốc đã xây dựng một ứng dụng ghi nhận lại hết tất cả các lịch sử sử dụng máy tính của các nhân viên. Phần mềm ghi nhận lịch sử truy cập web, ghi nhận lại hết thao tác gõ bàn phím, các màn hình máy tính được theo dõi 24/24. Ban giám đốc thường xuyên vào ứng dụng này kiểm soát xem ai đã truy cập nội dung mang tính giải trí trong giờ làm việc hoặc đang làm gì trên màn hình,... nhằm mục tiêu nhắc nhỡ cũng như phạt cảnh cáo các nhân viên vi phạm.**

* + - 1. **Nếu bạn là ban giám đốc - người quyết định giám sát nhân viên bằng hình thức trên thì bạn có thông báo trước cho người dùng hay không?**

Nếu tôi là ban giám đốc, tôi sẽ thông báo trước cho nhân viên về việc triển khai hệ thống giám sát và ghi nhận các hoạt động truy cập web và sử dụng máy tính. Thông báo này không chỉ giúp tạo ra một môi trường làm việc minh bạch và công bằng mà còn giúp xây dựng niềm tin và tôn trọng giữa ban quản lý và nhân viên. Người lao động có quyền biết được cách mà dữ liệu cá nhân của họ được sử dụng và giám sát, và thông báo trước cũng giúp họ hiểu rõ hơn về mục đích và phạm vi của việc giám sát.

Theo quy định chung của pháp luật, khi giám sát nhân viên bằng các phương tiện như camera, máy tính, thì cần phải có sự đồng ý của nhân viên được giám sát, trừ những trường hợp đặc biệt (ví dụ như trong các khu vực quân sự, an ninh quốc gia ). Vì vậy, ban giám đốc cần phải thông báo trước cho nhân viên về việc sử dụng ứng dụng giám sát và thu thập thông tin hành vi của họ trên máy tính. Việc thông báo này cần được thực hiện một cách rõ ràng và cụ thể, giúp cho nhân viên hiểu được quyền lợi và nghĩa vụ của mình.

1. **Dựa vào quy tắc ứng xử ACM, hãy phân tích các hành vi vi phạm quy tắc ứng xử vi phạm của ban giám đốc này**

Dựa vào quy tắc ứng xử ACM, hành vi của ban giám đốc này có thể vi phạm một số quy tắc như sau:

**Quy tắc 1.2 - Tránh gây hậu quả tiêu cực:**Ban giám đốc vi phạm quy tắc này bằng cách thu thập và ghi lại tất cả các hoạt động máy tính của nhân viên mà không cân nhắc đến quyền riêng tư của họ. Việc này có thể gây ra sự mất lòng tin và lo ngại cho nhân viên, tạo ra một môi trường làm việc không lành mạnh.

**Quy tắc 1.6 - Tôn trọng quyền riêng tư:**Ban giám đốc không tôn trọng quyền riêng tư của nhân viên khi ghi nhận lại toàn bộ lịch sử truy cập web và hoạt động máy tính của họ mà không có sự đồng ý hoặc thông báo trước.

**Quy tắc 1.7 - Bảo mật danh dự:**Bằng cách ghi lại toàn bộ các hoạt động trực tuyến và offline của nhân viên, ban giám đốc không bảo vệ tính bảo mật và danh dự của họ. Hành vi này làm mất lòng tin và đề xuất rủi ro đối với dữ liệu cá nhân của nhân viên.

**Quy tắc 2.3 - Biết và tôn trọng các quy tắc hiện hành:**Ban giám đốc không tuân thủ các quy tắc và luật lệ về quyền riêng tư và bảo mật thông tin khi thực hiện việc giám sát hành động của nhân viên mà không có sự cho phép hay sự thông báo trước.

**Quy tắc 4 - Tuân thủ Bộ quy tắc đạo đức:**Hành vi của ban giám đốc không tuân thủ các nguyên tắc và quy tắc đạo đức của ACM, đặc biệt là quy tắc về tôn trọng quyền riêng tư và bảo mật thông tin cá nhân của nhân viên.

**Quy tắc 3 - Nguyên tắc lãnh đạo chuyên nghiệp:**Ban giám đốc không đảm bảo rằng lợi ích công cộng là ưu tiên hàng đầu trong việc thực hiện các biện pháp giám sát và kiểm soát hành động của nhân viên trên máy tính.

- Tóm lại, việc giám sát nhân viên bằng cách ghi nhận lịch sử truy cập web, thao tác gõ bàn phím và màn hình máy tính của họ mà không được sự đồng ý của họ có thể xâm phạm quyền riêng tư, tính đa dạng và nghĩa vụ đạo đức của nhân viên. Ban giám đốc cần phải đảm bảo rằng việc giám sát này được thực hiện đúng quy định của pháp luật và tôn trọng các quy định đạo đức trong nghề nghiệp của người giám sát.