Đối với các doanh nghiệp SME và nhà điều hành doanh nghiệp nhỏ

# Tự đánh giá về an toàn thông tin của công ty trong 5 phút

## Bạn có cập nhật các xu hướng mới nhất không?

### Những thay đổi trong các mối đe dọa và tấn công mạng

- Mã độc mã hóa dữ liệu
- Tấn công dò tìm mật khẩu
- Tấn công lừa đảo qua email

### Những thay đổi trong môi trường công nghệ thông tin

- Dịch vụ đám mây
- Máy tính bảng
- Điện thoại thông minh

Sử dụng **"Phiếu tự đánh giá trong 5 phút"** để kiểm tra tình trạng an toàn thông tin của công ty bạn trước khi bạn để tránh đánh mất bất kỳ dữ liệu nào!

ASEAN · JAPAN
Cybersecurity Cooperation

# Tự đánh giá

## 1 Vui lòng đọc thông tin này trước khi làm đánh giá.

### Cách sử dụng

Chúng tôi đã tập trung vào 25 biện pháp an toàn thông tin có hiệu quả và có thể thực hiện với chi phí thấp cho tổ chức.
Vui lòng kiểm tra tình trạng thực hiện của các mục này và thực hiện bất kỳ biện pháp nào chưa được tiến hành, đồng thời tham khảo các giải thích trong cuốn sổ tay này.

### Mục đích và ưu điểm

- Cho phép bạn hiểu rõ về bất kỳ vấn đề nào đang tồn tại.
- Khi hiểu vấn đề, bạn có thể tìm ra tiến trình hành động cụ thể để thực hiện như bước tiếp theo.

### Cách đọc các mô tả

Vui lòng thực hiện đánh giá không dựa vào những ví dụ cụ thể trong các mô tả. Ví dụ, ý chính của câu hỏi 16 là về "biện pháp phòng ngừa trộm." Câu hỏi này hỏi rằng bạn có thực hiện các bước để phòng ngừa trộm bằng cách đặt máy tính xách tay vào ngăn kéo nếu tổ chức của bạn sử dụng máy tính xách tay hay không.
Câu hỏi cũng hỏi rằng bạn có thực hiện các bước để phòng ngừa trộm bằng cách không để những phụ kiện như thanh USB hoặc ổ cứng gắn ngoài trên bàn làm việc nếu tổ chức của bạn không dùng máy tính xách tay hay không. Tham khảo cuốn sổ tay này nếu bạn không hiểu mục đích của câu hỏi hoặc cảm thấy khó hiểu.

### Nếu công ty của bạn không sử dụng  mục nào đó

Một vài mục dưới đây có thể không áp dụng cho công ty của bạn tùy vào loại hình doanh nghiệp. Trong những trường hợp này, khoanh tròn "Đã thực hiện."

- Số 4 Máy photocopy và ổ cứng đã kết nối mạng
- Số 5 Dịch vụ Web
- Số 9 Mạng LAN không dây
- Số 23 Dịch vụ đám mây

**Nếu bạn nghĩ, "Chúng tôi không có bất kỳ 'thông tin mật' nào, các mục dưới đây chính là những tài liệu mật!**

- Địa chỉ nhân viên, và phiếu trả lương
- Danh sách thanh toán đối với từng đối tác kinh doanh và thông tin giao dịch
- Thông tin kế toán trong tổ chức của bạn
- Danh sách liên lạc của khách hàng và đối tác kinh doanh
- Thông tin phát triển như bản vẽ thiết kế về sản phẩm mới
- Bất kỳ thông tin nào từ đối tác kinh doanh cần được xử lý cẩn thận

Có những thông tin phải được quản lý như thông tin mật trong các thông tin cơ bản của tổ chức. Bạn phải xác nhận và sắp xếp xem loại thông tin nào đang có trong công ty của bạn là thông tin mật. Việc phân loại dữ liệu này là bước đầu tiên trong bảo mật thông tin.

## 2 Đọc thông tin này sau khi thực hiện đánh giá.

| | |
|---|---|
| Nếu bạn đạt được 100 điểm tròn | Các biện pháp bảo đảm an toàn thông tin cơ bản của bạn đã hoàn hảo. Hãy nghĩ về việc đưa các biện pháp của bạn lên mức độ tiếp theo. |
| Nếu bạn đạt được từ 70-99 điểm | Gần như hoàn hảo nhưng có một số mảng có các biện pháp chưa hoàn thiện. |
| Nếu bạn đạt được từ 50-69 điểm | Nhiều mảng dễ thấy có các biện pháp không phù hợp. |
| Nếu bạn đạt được từ 49 điểm trở xuống | Bạn không nên ngạc nhiên nếu xảy ra sự cố như lộ lọt dữ liệu. |

Các biện pháp được mô tả trong phiếu Tự đánh giá công ty dựa trên những điều kiện sau.

■ Người điều hành (người đại diện) có thể trực tiếp hướng dẫn và xác nhận xem các biện pháp về chính sách có được thực hiện hay không.
■ Tất cả nhân viên đều nhận diện được nhau.
■ Công ty không sở hữu máy chủ hoặc thiết bị mạng yêu cầu cài đặt phức tạp trong công ty.
- Trang thông tin điện tử của công ty không sử dụng máy chủ kết nối trực tiếp với mạng Internet, như sử dụng dịch vụ đám m.
- Công ty không phát triển phần mềm ứng dụng nào, và chỉ sử dụng phần mềm ứng dụng có sẵn trên thị trường.
- Cho phép sử dụng máy tính cá nhân cho công việc chỉ khi áp dụng các biện pháp giống với biện pháp dành cho máy tính của công ty.

# Phiếu Tự đánh giá công ty trong 5 phút

Phiếu tự đánh giá công ty nhằm xác định các biện pháp bảo mật thông tin bạn nên ưu tiên với vai trò tổ chức

- Vui lòng đọc mục 1 ở trang trước trước khi thực hiện đánh giá này.
- Đọc các mục đánh giá bên dưới và khoanh tròn vào cột có thể áp dụng.
- Người điều hành hoặc quản lý nên điền vào phiếu này.
- Vui lòng trả lời các mục được biểu thị bằng có được tất cả nhân viên thực hiện hay không. Nếu có mục chỉ được một số nhân viên thực hiện, hãy chọn "Đã thực hiện một phần." Vui lòng trả lời các mục được biểu thị bằng có được công ty của bạn thực hiện hay không.
- Cộng số điểm của bạn ở cuối trang, và tiếp tục đọc mục 2 ở trang trước.

Tổ chức:

Người trả lời:

Ngày:

| Mục đánh giá | Số | Mô tả | Trả lời | | | |
|---|---|---|---|---|---|---|
| | | | Đã thực hiện | Đã thực hiện một phần | Chưa được thực hiện | Không biết |
| Phần 1 Các biện pháp cơ bản | 1 | Bạn có luôn bảo vệ hệ điều hành và phần mềm của bạn bằng cách cập nhật Windows (Windows Update)*1 hoặc sử dụng các biện pháp khác không? | 4 | 2 | 0 | 0 |
| | 2 | Bạn có thực hiện các biện pháp để bảo vệ PC của bạn khỏi virus, như cài đặt phần mềm chống virus và tự động cập nhật không?*2 | 4 | 2 | 0 | 0 |
| | 3 | Bạn có cài đặt mật khẩu mạnh không dễ đoán ra và không sử dụng những mật khẩu như tên, số điện thoại, hay ngày sinh của bạn không, và bạn có hạn chế sử dụng cùng một mật khẩu cho nhiều dịch vụ web không? | 4 | 2 | 0 | 0 |
| | 4 | Bạn có hạn chế thích hợp việc truy cập vào những thông tin quan trọng, như hạn chế chia sẻ máy photocopy hoặc ổ cứng đã kết nối mạng chỉ cho những người cần sử dụng không? | 4 | 2 | 0 | 0 |
| | 5 | Bạn có hệ thống sẵn có để xác định các mối đe dọa cũng như phương pháp tấn công mới và chia sẻ hệ thống này trong nội bộ bằng cách kiểm tra cũng như chia sẻ những cảnh báo bảo mật từ nhà sản xuất sản phẩm hoặc các dịch vụ web*3 mà bạn sử dụng không? | 4 | 2 | 0 | 0 |
| Phần 2 Các biện pháp với vai trò nhân viên | 6 | Bạn có cẩn trọng với các e-mail tấn công giả mạo, và cố gắng không mở tập tin đính kèm trong những e-mail khả nghi hoặc nhấp vào các đường dẫn trong tin nhắn không? | 4 | 2 | 0 | 0 |
| | 7 | Bạn có hệ thống sẵn có để kiểm tra và ngăn chặn việc gửi nhầm e-mail, như kiểm tra trực quan địa chỉ trước khi gửi e-mail không? | 4 | 2 | 0 | 0 |
| | 8 | Bạn có bảo vệ các thông tin quan trọng như bảo vệ tập tin đính kèm bằng mật khẩu hoặc biện pháp tương tự khác trước khi gửi qua email không? | 4 | 2 | 0 | 0 |
| | 9 | Bạn có thực hiện các bước để đảm bảo an toàn cho các mạng LAN không dây của bạn, như luôn thực hiện mã hóa ở mức độ cao khi sử dụng chúng không? | 4 | 2 | 0 | 0 |
| | 10 | Bạn có thực hiện các bước để kiểm soát việc sử dụng Internet, như đặt ra các quy định về duyệt web và đăng tải lên phương tiện truyền thông xã hội bằng máy tính văn phòng không? | 4 | 2 | 0 | 0 |
| | 11 | Bạn có thực hiện các bước để tiến hành sao lưu thường xuyên, để ngăn chặn việc đánh mất thông tin quan trọng do sự cố hoặc lỗi vận hành không? | 4 | 2 | 0 | 0 |
| | 12 | Bạn có thực hiện các bước để ngăn chặn việc mất hoặc rò rỉ thông tin quan trọng, như lưu trữ thông tin quan trọng trong tủ có khóa thay vì để trên bàn làm việc không? | 4 | 2 | 0 | 0 |
| | 13 | Khi mang thông tin quan trọng ra khỏi văn phòng, bạn có thực hiện các bước chống trộm hoặc làm mất, như bảo vệ thông tin bằng mật khẩu hoặc mã hóa thông tin và luôn giữ chúng bên cạnh bạn ở mọi thời điểm không? | 4 | 2 | 0 | 0 |
| | 14 | Bạn có thực hiện các bước để đảm bảo người khác không sử dụng máy tính của bạn, như cài đặt màn hình khóa của máy tính khi bạn rời khỏi bàn làm việc của mình không? | 4 | 2 | 0 | 0 |
| | 15 | Bạn có cố gắng ngăn không cho những người không được phép đi vào văn phòng bằng cách tiếp cận những người lạ khi bạn nhận ra có ai đó lạ mặt ở văn phòng, hoặc thực hiện bất kỳ biện pháp nào khác không? | 4 | 2 | 0 | 0 |
| | 16 | Bạn có thực hiện các bước để chống trộm khi rời khỏi văn phòng trong ngày, như khóa máy tính xách tay và phụ kiện trong ngăn kéo thay vì để chúng trên bàn làm việc không? | 4 | 2 | 0 | 0 |
| | 17 | Chìa khóa của văn phòng có được quản lý theo cách thích hợp, như người cuối cùng rời khỏi văn phòng trong ngày phải khóa cửa và ghi biên bản (về tên của họ, ngày và giờ) không? | 4 | 2 | 0 | 0 |
| | 18 | Khi tiêu hủy các thông tin quan trọng, bạn có thực hiện các bước khiến các thông tin quan trọng không thể đọc được nữa, như nghiền nhỏ tài liệu hoặc sử dụng công cụ xóa dữ liệu không? | 4 | 2 | 0 | 0 |
| Phần 3 Các biện pháp với vai trò tổ chức | 19 | Bạn có Bộ quy tắc ứng xử dành cho nhân viên để duy trì tính bí mật, như thông báo cho nhân viên khi họ được thuê rằng họ có nghĩa vụ duy trì tính bí mật và có các điều khoản xử phạt nếu vi phạm không? | 4 | 2 | 0 | 0 |
| | 20 | Bạn có tiến hành đào tạo nhận thức về bảo mật để các nhân viên có ý thức về tầm quan trọng của việc quản lý thông tin, như thường xuyên giải thích về tầm quan trọng của việc này không? | 4 | 2 | 0 | 0 |
| | 21 | Bạn có làm rõ việc nhân viên có thể sử dụng thiết bị cá nhân trong công việc của họ hay không, như thiết lập các chính sách về việc sử dụng máy tính cá nhân và điện thoại thông minh trong và ngoài công ty không? | 4 | 2 | 0 | 0 |
| | 22 | Bạn có yêu cầu đối tác kinh doanh duy trì tính bí mật, như bao gồm các điều khoản về tính bí mật (nghĩa vụ duy trì tính bí mật) trong hợp đồng không? | 4 | 2 | 0 | 0 |
| | 23 | Bạn có xác nhận tính an toàn và độ tin cậy của dịch vụ bằng cách kiểm tra các điều khoản sử dụng và biện pháp bảo mật trước khi lựa chọn các dịch vụ bên ngoài, như dịch vụ đám mây không? | 4 | 2 | 0 | 0 |
| | 24 | Bạn đã có chuẩn bị nếu xảy ra sự cố về bảo mật thông tin, như chuẩn bị quy trình xử lý đối với việc rò rỉ, mất, hoặc bị trộm các thông tin mật chưa? | 4 | 2 | 0 | 0 |
| | 25 | Bạn có xác định nội dung của các biện pháp bảo mật thông tin, như biến các biện pháp bảo mật thông tin (như mục từ 1 đến 24 ở trên) thành chính sách công ty không? | 4 | 2 | 0 | 0 |

*1 Chương trình do Microsoft Corporation cung cấp để sửa chữa các sự cố trên Windows PC

*2 Tập tin cơ sở dữ liệu được gọi là "tập tin mẫu" dùng để phát hiện virus máy tính

*3 Tên chung của các dịch vụ được sử dụng qua Internet như Internet banking, phương tiện truyền thông xã hội, webmail, và lịch

★ Chúng tôi không bảo đảm các biện pháp được mô tả trong phiếu Tự đánh giá công ty có thể mang đến sự bảo vệ toàn diện.

| A Tổng số điểm đã thực hiện | B Tổng số điểm đã thực hiện một phần | A+B Điểm số |
|---|---|---|
| Điểm | Điểm | Điểm |

# Giải thích

## Phần 1 Các biện pháp cơ bản

**Các mục Số 1 đến 5 là các biện pháp nên được thực hiện bất kể quy mô và hình thức của công ty. Quan trọng là các biện pháp này nên được liên tục xem xét lại và không chỉ thực hiện một lần. Cần thực hiện các biện pháp này như quy định công ty để tất cả nhân viên có thể tuân theo.**


### Mục số 1 Các biện pháp bảo vệ điểm dễ bị tấn công

**Luôn cập nhật hệ điều hành và phần mềm của bạn**

Phớt lờ các vấn đề bảo mật với hệ điều hành và phần mềm của bạn sẽ khiến thiết bị của bạn dễ bị nhiễm virus nguy hiểm. Đảm bảo đã áp dụng cập nhật bản vá lỗi cho hệ điều hành và phần mềm của bạn hoặc sử dụng phiên bản mới nhất.

**Hành động** Thực hiện các biện pháp, như sử dụng Windows Update (Hệ điều hành Windows) hoặc sử dụng phiên bản mới nhất của Adobe Flash Player, Adobe Reader, Java runtime environment, và phần mềm khác.

### Mục số 2 Các biện pháp chống virus

**Cài đặt phần mềm chống virus và sử dụng phần mềm đó một cách thích hợp**

Số lượng virus trộm ID và mật khẩu, vận hành máy tính từ xa, và tùy ý mã hóa các tập tin đang ngày càng tăng lên. Đảm bảo đã cài đặt phần mềm chống virus và đảm bảo tập tin định nghĩa virus (tập tin mẫu) luôn được cập nhật.

**Hành động** Thực hiện các bước, như cài đặt thiết bị của bạn tự động cập nhật tập tin định nghĩa virus và xem xét việc cài đặt phần mềm bảo mật tích hợp.

### Mục số 3 Quản lý mật khẩu

**Sử dụng mật khẩu mạnh**

Tổng số thiệt hại từ việc đăng nhập trái phép do đoán được mật khẩu và việc sử dụng các ID và mật khẩu bị rò rỉ từ dịch vụ web với mục đích xấu đang ngày càng tăng lên. Giúp mật khẩu của bạn mạnh hơn bằng cách tăng độ dài và độ phức tạp, không sử dụng lại mật khẩu.

*Mật khẩu đơn giản: Mật khẩu mà bên thứ ba có thể dễ dàng đoán ra, như tên của bạn, tên công ty hoặc những từ tiếng Anh đơn giản trong từ điển.

**Hành động** Thực hiện các bước, như đặt mật khẩu kết hợp từ 10 ký tự, số, và biểu tượng trở lên. Không sử dụng tên, số điện thoại, ngày sinh, v.v... và không sử dụng cùng một mật khẩu cho nhiều dịch vụ web và các trang web khác.

### Mục số 4 Cài đặt thiết bị

**Xem lại cài đặt chia sẻ**

Ngày càng có nhiều lo ngại về những người không được phép có thể xem các thông tin do dữ liệu được lưu trữ trên máy chủ tập tin hoặc lưu trữ trực tuyến, hoặc máy photocopy nối mạng được cấu hình không đúng cách. Đảm bảo rằng các máy chủ và thiết bị đã nối mạng chỉ được chia sẻ với những người được phép truy cập chúng.

**Hành động** Thực hiện các bước, như giới hạn phạm vi chia sẻ dịch vụ đám mây, giới hạn phạm vi chia sẻ các thiết bị đã kết nối mạng, và thay đổi cài đặt khi nhân viên chuyển đến phòng ban khác hoặc thôi việc.

### Mục số 5 Thu thập thông tin

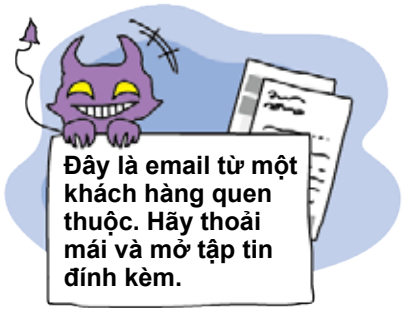
**Tìm hiểu về mối đe dọa cũng như các phương pháp tấn công và thực hiện các bước đối phó với chúng.**

Số lượng các vụ tấn công giả mạo để trộm ID và mật khẩu thông qua email bằng virus mạo danh đối tác kinh doanh hoặc các bên liên quan khác, hoặc dẫn mọi người đến các trang web lừa đảo giả mạo những trang web hợp pháp đang ngày càng tăng lên. Thực hiện các bước để đối phó với mối đe dọa và các phương pháp tấn công bằng cách tìm hiểu về chúng.

**Hành động** Thực hiện các bước, như kiểm tra trang web IPA và đặt mua tạp chí qua e-mail để tìm hiểu về các mối đe dọa cũng như phương pháp tấn công mới nhất, và xác nhận các cảnh báo được cung cấp bởi Internet banking và các dịch vụ khác đang sử dụng.

# Phần 2 Các biện pháp với vai trò nhân viên

Các mục Số 6 đến 18 là những mục nhân viên nên biết. Lỗi do con người có thể dễ dàng xảy ra do sự quen thuộc khi xử lý các thông tin quan trọng mỗi ngày và do sai sót gây ra. Hơn nữa, tính chất của các mối đe dọa thay đổi từng ngày, nên bạn cần phải cảnh giác ở mọi thời điểm.




**Mục số 6** Quy định về e-mail

## Luôn đặt nghi vấn với bất kỳ e-mail nào nhận được từ người bạn không biết

Điều này có thể dẫn đến việc nhiễm virus khi mở tập tin đính kèm trong e-mail hoặc nhấp vào đường dẫn URL trong nội dung chính của e-mail. Thận trọng với tập tin đính kèm và việc nhấp vào đường dẫn từ người gửi mà bạn không biết.

**Hành động** Thực hiện các bước, như không mở tập tin đính kèm hoặc nhấp vào đường dẫn trong những e-mail khả nghi, báo cáo các e-mail khả nghi cho bộ phận bảo mật của bạn để chia sẻ thông tin về các e-mail khả nghi trong công ty.

**Mục số 7** Quy định về e-mail

## Ngăn chặn việc gửi e-mail đến sai người nhận

Sẽ có sự cố rò rỉ thông tin cho người lạ do gửi nhầm e-mail hoặc fax đến sai người. Đảm bảo đã kiểm tra cẩn thận người bạn sẽ gửi e-mail và fax đến. Hơn nữa, rò rỉ thông tin xảy ra khi bạn cung cấp cho người khác sai địa chỉ e-mail. Khi gửi e-mail cho nhiều người, đảm bảo đã xác nhận các địa chỉ của người nhận.

**Hành động** Thực hiện các bước, như kiểm tra hai lần các địa chỉ trước khi gửi e-mail hoặc fax, và chọn riêng các địa chỉ cho To, CC và BCC trong các e-mail.

**Mục số 8** Quy định về e-mail

## Bảo vệ thông tin quan trọng khi gửi e-mail

Khi gửi thông tin quan trọng bằng e-mail, không viết các thông tin này vào nội dung chính của e-mail. Thay vào đó, hãy viết thông tin này vào một tập tin, bảo vệ bằng mật khẩu, và đính kèm tập tin vào e-mail. Thông báo cho người nhận e-mail về mật khẩu của tập tin bằng cách gọi điện thoại cho họ hoặc thông qua các phương tiện khác, thay vì viết mật khẩu vào e-mail.

**Hành động** Thực hiện các bước, như viết thông tin quan trọng vào tập tin và bảo vệ thông tin đó bằng mật khẩu. Thông báo cho người nhận e-mail về mật khẩu qua điện thoại hoặc thông qua các phương tiện khác.

**Mục số 9** Quy định về mạng LAN không dây

## Ngăn chặn việc nghe trộm và sử dụng trái phép các mạng LAN không dây

Mạng LAN không dây không có cài đặt bảo mật thích hợp có thể bị đọc dữ liệu hoặc sử dụng với mục đích xấu cho các hoạt động tội phạm bằng cách kết nối trái phép với chúng. Đảm bảo đã cài đặt bảo mật cho các mạng LAN không dây để ngăn chặn việc nghe lén hoặc sử dụng trái phép.

**Hành động** Thực hiện các bước, như sử dụng cài đặt mã hóa (ví dụ như WPA2-PSK) và sử dụng cụm mật khẩu dài và khó đoán.

**Mục số 10** Quy định khi sử dụng Inernet

## Ngăn chặn rắc rối khi sử dụng Internet

Việc xem các trang web độc hại hoặc các trang web có vấn đề về bảo mật có thể khiến thiết bị của bạn bị nhiễm virus. Hơn nữa, công ty có thể bị thiệt hại bởi các trò chơi khăm được đăng tải trên phương tiện truyền thông xã hội hoặc bảng thông báo hoặc do vô tình đăng tải các thông tin mật. Cần ngăn chặn thiệt hại bằng cách thiết lập sẵn hệ thống và các quy định giới hạn việc sử dụng Inernet tại nơi làm việc.

**Hành động** Thực hiện các bước, như tạo ra các quy định truy cập khi sử dụng Internet và phương tiện truyền thông xã hội, và sử dụng bộ lọc web để giới hạn có hệ thống việc sử dụng Internet.

**Mục số 11** Quy định khi sao lưu

## Khuyến khích sao lưu thường xuyên

Dữ liệu được lưu trên PC hoặc máy chủ có thể bị mất do sự cố, vận hành bị lỗi, hoặc nhiễm virus. Thực hiện sao lưu dữ liệu để chuẩn bị cho các tình huống bất ngờ đó.

**Hành động** Thực hiện các bước, như thường xuyên tiến hành sao lưu thông tin quan trọng và lưu dữ liệu sao lưu ở nơi riêng biệt.

# Giải thích

**Mục số 12** | **Quy định khi lưu trữ**

## Thông tin/tài liệu quan trọng phải được xử lý phù hợp

Việc để các thông tin/tài liệu không có người giám sát trên bàn làm việc là điều nguy hiểm vì chúng có thể bị người khác lấy đi hoặc đọc được. Các thông tin/tài liệu quan trọng phải được xử lý phù hợp để ngăn chặn người khác nhìn thấy hoặc chạm vào chúng và đảm bảo rằng chúng không được để mà không có người giám sát. Xác định nơi lưu trữ thông tin/tài liệu, chỉ lấy chúng ra khi cần thiết cho công việc, và đảm bảo trả trở lại khi đã hoàn tất.

**Hành động** Thực hiện các bước, như giữ bàn làm việc gọn gàng và ngăn nắp, và lưu trữ các thông tin/tài liệu quan trọng trong tủ có khóa.

**Mục số 13** | **Quy định khi vận chuyển thông tin**

## Vận chuyển các thông tin quan trọng theo cách an toàn

Khi lấy thông tin quan trọng ra ngoài công ty, thông tin đó thể bị trộm bất ngờ hoặc vô tình bị mất. Thực hiện trước các bước khi sử dụng máy tính xách tay hoặc điện thoại thông minh, như cài đặt mật khẩu hoặc mã hóa các tập tin dữ liệu để người khác không thể dễ dàng xem được thông tin trong trường hợp thông tin bị trộm hoặc bị mất.

**Hành động** Thực hiện các bước, như bắt buộc phải có sự cho phép khi vận chuyển thông tin quan trọng, đảm bảo an toàn cho dữ liệu bằng mật khẩu trên máy tính xách tay, điện thoại thông minh, và thanh USB, và tuyệt đối không để hành lý mà không có người giám sát.

**Mục số 14** | **Quản lý an toàn văn phòng**

## Không để bất kỳ ai sử dụng thiết bị mà không có sự cho phép

Không để máy tính không có người giám sát trong quá trình làm việc. PC không có người giám sát có thể bị bất kỳ ai vận hành, như người có thể đăng nhập mà không cần mật khẩu, và có thể bị sử dụng với mục đích không phù hợp. Thực hiện các bước bảo vệ PC khỏi việc sử dụng trái phép.

**Hành động** Thực hiện các bước, như khóa PC của bạn khi rời khỏi bàn làm việc, tắt PC khi rời khỏi văn phòng trong ngày, và ngăn không để người khác sử dụng PC của bạn.

**Mục số 15** | **Quản lý an toàn văn phòng**

## Tiếp cận những người bạn không nhận diện được

Thông tin có nguy cơ bị trộm nếu bạn không giới hạn truy cập đối với những người không được phép vào văn phòng. Đảm bảo không cho phép những người không được phép truy cập vào nơi lưu trữ các thông tin/tài liệu quan trọng, đặc biệt là máy chủ, phòng lưu trữ và két sắt.

**Hành động** Thực hiện các bước, như tiếp cận một người bạn không nhận diện được trong văn phòng hoặc thiết lập quầy tiếp tân.

**Mục số 16** | **Quản lý an toàn văn phòng**

## Thực hiện các biện pháp để ngăn chặn việc trộm thiết bị và phụ kiện

Mặc dù các thiết bị như máy tính xách tay, máy tính bảng, và thanh USB rất tiện lợi và dễ mang đi, nhưng điều này cũng khiến những thiết bị đó có nguy cơ bị mất trộm cao. Khi không sử dụng những thiết bị này, hãy thực hiện các bước để lưu trữ chúng ở nơi an toàn, như trong ngăn kéo có thể khóa được.

**Hành động** Thực hiện các bước, như khóa máy tính xách tay, máy tính bảng và phụ kiện (đĩa CD, thanh USB, ổ cứng gắn ngoài, v.v...) trong ngăn kéo của bàn làm việc khi rời khỏi văn phòng trong ngày

**Mục số 17** | **Quản lý an toàn văn phòng**

## Cảnh giác về việc khóa cửa văn phòng

Việc lưu giữ biên bản về thời gian người cuối cùng rời khỏi văn phòng cũng giúp nâng cao tinh thần trách nhiệm để người cuối cùng khóa cửa. Cố gắng quản lý chìa khóa và các biên bản.

**Hành động** Thực hiện các bước, như quản lý chìa khóa và lưu giữ biên bản về việc người cuối cùng rời khỏi văn phòng khóa cửa (ngày, giờ, và tên).

**Mục số 18** | **Tiêu hủy thông tin an toàn**

## Xóa các thông tin quan trọng để những thông tin này không thể phục hồi

Việc chỉ vứt các tài liệu chứa thông tin quan trọng vào thùng rác có thể dẫn đến rò rỉ thông tin nghiêm trọng vì những người khác có thể đọc được các tài liệu đó. Ngoài ra, thông tin được lưu trên các thiết bị điện tử và phương tiện truyền thông điện tử có thể được khôi phục ngay cả khi đã xóa các tập tin. Khi tiêu hủy thông tin quan trọng, hãy tiêu hủy từng loại thông tin theo cách thích hợp, như sử dụng máy hủy giấy hoặc phần mềm xóa dữ liệu.

**Hành động** Thực hiện các bước để tiêu hủy thông tin, như sử dụng phần mềm xóa dữ liệu, tiêu hủy bằng phương pháp vật lý, hoặc yêu cầu chuyên gia xóa thông tin.

**Lưu trữ tài liệu chứa các thông tin quan trọng trong ngăn kéo có khóa**

**Ngăn chặn việc trộm thiết bị**

**Khóa cửa văn phòng**

# Phần 3 Các biện pháp dành cho tổ chức

**Các mục Số 19 đến 25 là những biện pháp được thực hiện sau khi thiết lập chính sách cho tổ chức. Nâng cao ý thức của nhân viên bằng cách ghi chép rõ ràng về quy định bảo mật thông tin và chia sẻ chúng trong văn phòng.**


## Mục số 19 Thông báo về nghĩa vụ của nhân viên trong việc duy trì tính bí mật

**Giúp nhân viên hiểu rõ về nghĩa vụ của họ trong việc duy trì tính bí mật**

Dù có thể nói rằng các quy định của công ty đã yêu cầu nhân viên duy trì tính bí mật trong công việc của họ, tuy nhiên, cũng nên thông báo với nhân viên về quy định của công ty một cách rõ ràng để họ làm theo.

**Hành động** Thực hiện các bước, như thông báo với nhân viên về nghĩa vụ của họ trong việc duy trì tính bí mật khi họ được thuê.

## Mục số 20 Đào tạo nhân viên

**Tiến hành đào tạo nhân viên thường xuyên**

Nhân viên xử lý thông tin hàng ngày trong quá trình làm việc của mình, và sự quen thuộc này cũng đồng nghĩa với việc dễ bị sai sót và họ quên cách quản lý thông tin một cách an toàn. Đào tạo nhân viên thường xuyên là cách hiệu quả trong việc nâng cao ý thức của nhân viên.

**Hành động** Thực hiện các bước, như thường xuyên giải thích về tầm quan trọng của việc quản lý thông tin và tiến hành đào tạo nội bộ.

## Mục số 21 Sử dụng thiết bị cá nhân

**Quyết định xem có cho phép sử dụng thiết bị cá nhân cho công việc hay không**

Việc đảm bảo bảo mật sẽ trở nên khó khăn nếu các thiết bị cá nhân như PC và điện thoại thông minh được sử dụng cho công việc, vì khó quản lý việc nhân viên đang sử dụng chúng như thế nào. Quyết định xem các thiết bị cá nhân có được sử dụng cho công việc hay không và cố gắng đặt ra các quy định về việc sử dụng chúng.

**Hành động** Thực hiện các bước, như thiết lập hệ thống cho phép đối với việc sử dụng các thiết bị cá nhân như PC và điện thoại thông minh cho công việc và xác định các quy định về việc sử dụng chúng nếu được phép sử dụng các thiết bị này cho công việc.

## Mục số 22 Quản lý đối tác kinh doanh

**Yêu cầu các đối tác kinh doanh duy trì tính bí mật**

Tránh việc nghĩ rằng các đối tác kinh doanh sẽ tự duy trì tính bí mật dựa trên tính chất của thông tin. Khi cung cấp thông tin mật cho các đối tác, cần nêu rõ rằng những thông tin này phải được xử lý như tài liệu mật.

**Hành động** Thực hiện các bước, như soạn thảo hợp đồng nêu rõ những nội dung phải được xử lý như tài liệu mật.

## Mục số 23 Sử dụng các dịch vụ bên ngoài

**Sử dụng các dịch vụ bên ngoài đáng tin cậy**

Nếu bạn chọn các dịch vụ bên ngoài, như dịch vụ đám mây, với chi phí tiết kiệm, bạn có thể thấy rằng dịch vụ này có thể không dùng được do hư hỏng hoặc các vấn đề khác. Nghiên cứu kỹ hiệu suất, độ tin cậy, chi tiết về bồi thường, và các xem xét liên quan khác khi sử dụng dịch vụ bên ngoài cho những ứng dụng có ảnh hưởng quan trọng đến tính liên tục của hoạt động kinh doanh.

**Hành động** Thực hiện các bước, như kiểm tra điều khoản dịch vụ, chi tiết về bồi thường, biện pháp bảo mật, và các vấn đề liên quan khác khi lựa chọn nhà cung cấp.

# Giải thích

| Mục số 24 | Chuẩn bị đối với các sự cố về bảo mật thông tin |
|---|---|

## Chuẩn bị trước đối với sự cố về bảo mật thông tin

Khi sự cố xảy ra, thông thường sẽ không có thời gian để bình tĩnh suy nghĩ, và bất kỳ sự trì hoãn nào khi giải quyết sự cố cũng có khuynh hướng làm tăng tác động của sự cố đó. Sử dụng những sự cố được thuật lại trên các phương tiện truyền thông làm tài liệu tham khảo để cân nhắc về việc người nào, sẽ làm gì và khi nào để giải quyết sự cố, giả định rằng chuyện tương tự sẽ xảy ra ở công ty của bạn.

| Hành động | Thực hiện các bước, như chuẩn bị tài liệu về cách xử lý khi thông tin quan trọng bị rò rỉ, bị mất hoặc bị trộm. |
|---|---|

| Mục số 25 | Quy định khi chuẩn bị |
|---|---|

## Đặt ra các quy định về biện pháp bảo mật thông tin

Ngay cả khi người điều hành đã thiết lập sẵn các chính sách về biện pháp bảo mật thông tin, nhưng nếu chúng không được ghi chép rõ ràng như quy định nội bộ, nhân viên sẽ phải luôn tìm kiếm lời khuyên từ những người quản lý của họ. Để cho phép nhân viên tự mình hành động theo các quy định, cần ghi chép rõ ràng về “các quy định của công ty” để nhân viên có thể tham khảo chúng bất kỳ lúc nào.

| Hành động | Thực hiện các bước, như sử dụng các mục Số 1-24 trong phiếu đánh giá làm quy định đối với biện pháp bảo mật thông tin, chia sẻ chúng trong công ty và thường xuyên xem lại những quy định này để cải thiện chúng khi phát hiện thiếu sót. |
|---|---|

NISC National center of Incident readiness and Strategy for Cybersecurity
AIS Viet Nam Ministry of Information and Communications Authority of Information Security
IPA Information-technology Promotion Agency, Japan

2019.04