PHỤ LỤC A

Các mục tiêu kiểm soát và biện pháp kiểm soát tham chiếu

Các mục tiêu kiểm soát và biện pháp kiểm soát được liệt kê trong Bảng A.1 dưới đây được dẫn xuất trực tiếp và liên kết với các điều từ Điều 5 đến Điều 18 trong tiêu chuẩn ISO/IEC 27002:2013 và sẽ được sử dụng trong bối cảnh của 6.1.3.

Mục Lục

A.5. Các chính sách an toàn thông tin

A.5.1. Định hướng quản lý an toàn thông tin

Mục tiêu: Nhằm cung cấp định hướng quản lý và hỗ trợ đảm bảo an toàn thông tin phù hợp với các yêu cầu trong hoạt động nghiệp vụ, môi trường pháp lý và các quy định phải tuân thủ.

A.5.1.1. Các chính sách an toàn thông tin

Một tập hợp các chính sách an toàn thông tin cần được xác định, do ban quản lý phê duyệt, được công bố và thông báo cho nhân viên và các đối tác bên ngoai có liên quan.

A.5.1.2. Soát xét các chính sách an toàn thông tin

Cần soát xét các chính sách an toàn thông tin định kỳ theo kế hoạch hoặc khi có sự thay đổi đáng kể xảy ra để luôn đảm bảo sự phù hợp, đầy đủ và hiệu quả.

A.6. Tổ chức đảm bảo an toàn thông tin

A.6.1. Tổ chức nội bộ

Mục tiêu: Thiết lập một khuôn khổ quản lý nhằm khởi tạo và kiểm soát việc thực hiện và hoạt động của an toàn thông tin trong tổ chức.

A.6.1.1. Các vai trò và trách nhiệm đảm bảo an toàn thông tin

Tất cả các trách nhiệm an toàn thông tin phải được định nghĩa và phân phối.

A.6.1.2. Sự phân tách

Các nhiệm vụ và phạm vi trách nhiệm đối lập nhau phải được phân tách nhằm giảm thiểu khả năng sửa đổi trái phép hoặc vô tình, hoặc lạm dụng tài sản của tổ chức.

A.6.1.3. Liên lạc với những cơ quan/tổ chức có thẩm quyền

Cần duy trì kênh liên lạc thích hợp với các cơ quan có thẩm quyền liên quan.

A.6.1.4. Liên lạc với các nhóm chuyên gia

Cần duy trì liên lạc đầy đủ với các nhóm chuyên gia chuyên sâu hoặc các diễn đàn và các hiệp hội về an toàn thông tin.

A.6.1.5. An toàn thông tin trong quản lý dự án

An toàn thông tin cần được gắn với quản lý dự án, và bất kì loại dự án nào.

A.6.2. Các thiết bị di động và làm việc từ xa

Mục tiêu: Nhằm đảm bảo an toàn khi làm việc từ xa và sử dụng các thiết bị di động.

A.6.2.1. Chính sách đối với thiết bị di động

Một chính sách và các biện pháp hỗ trợ an toàn cần được áp dụng để quản lý các rủi ro được đã được nêu ra khi sử dụng các thiết bị di động.

A.6.2.2. Làm việc từ xa

Một chính sách và các biện pháp hỗ trợ an toàn cần được thực hiện để bảo vệ thông tin được truy nhập, xử lý hoặc được lưu trữ tại các nơi làm việc từ xa.

A.7. An toàn nguồn nhân lực

A.7.1. Trước khi tuyển dụng

Mục tiêu: Để đảm bảo rằng các nhân viên và các nhà tuyễn dụng nhận thức được và thực hiện trách nhiệm bảo mật thông tin của họ.

A.7.1.1. Thẩm tra

Việc xác minh lý lịch của tất cả các ứng viên tuyển dụng phải được thực hiện phù hợp theo quy định của pháp luật, các quy định và đạo đức có liên quan và phải tỷ lệ thuận với các yêu cầu của công việc, phân loại thông tin được truy nhập và các rủi ro có thể nhận thấy được.

A.7.1.2. Các điều khoản và điều kiện tuyển dụng

Các thỏa thuận hợp đồng giữa nhân viên và người ký kết hợp đồng phải được ghi rõ trách nhiệm của người được tuyển dụng và tổ chức tuyển dụng trong việc đảm bảo an toàn thông tin.

A.7.2. Trong thời gian làm việc

Mục tiêu: Đảm bảo rằng mọi nhân viên và nhà tuyển dụng nhận thức được và thực hiện trách nhiệm bảo mật an toàn thông tin của họ.

A.7.2.1. Trách nghiệm của ban quản lý

Ban quản lý phải yêu cầu tất cả nhân viên và nhà thầu áp dụng an toàn thông tin phù hợp với các chính sách và thủ tục an toàn thông tin đã được thiết lập của tổ chức.

A.7.2.2. Nhận thức, giáo dục và đào tạo về an toàn thông tin

Tất cả nhân viên trong tổ chức và, nếu có thể, các nhà thầu có liên quan cần phải được giáo dục và đào tạo nâng cao nhận thức thích hợp và cập nhật thường xuyên các chính sách và thủ tục của tổ chức, nếu phù hợp với chức năng công việc của họ.

A.7.2.3. Xử lý kỷ luật

Phải có hình thức xử lý kỷ luật chính thức và công khai nhằm ngăn chặn kịp thời các nhân viên vi phạm an toàn thông tin.

A.7.3. Chấm dứt hoặc thay đổi công việc

Mục tiêu: Bảo vệ lợi ích của tổ chức trong quá trình thay đổi hoặc chấm dứt công việc.

A.7.3.1. Trách nhiệm chấm dứt hoặc thay đổi việc làm

Trách nhiệm và nghĩa vụ bảo vệ an toàn thông tin vẫn có hiệu lực sau khi chấm dứt hoặc thay đổi việc làm phải được xác định, được thông báo tới nhân viên hoặc nhà thầu và phải được thi hành.

A.8. Quản lý tài sản

A.8.1. Trách nhiệm đối với tài sản

Mục tiêu: Nhằm xác định tài sản của tổ chức và xác định các trách nhiệm bảo vệ thích hợp.

A.8.1.1. Kiểm kê tài sản

Thông tin, tất cả tài sản khác liên quan đến thông tin và phương tiện xử lý thông tin phải được xác định và việc kiểm kê các tài sản này phải được thiết lập và duy trì.

A.8.1.2. Quyền sở hữu tài sản

Các tài sản được duy trì trong bảng kiểm kê phải có chủ sở hữu.

A.8.1.3. Sử dụng hợp lý tài sản

Các quy định về việc sử dụng hợp lý thông tin và sử dụng các tài sản gắn liền với thiết bị xử lý thông tin và thông tin phải được xác định, được ghi thành văn bản và được triển khai.

A.8.1.4. Bàn giao tài sản

Tất cả nhân viên và người sử dụng bên ngoài phải hoàn trả tất cả tài sản của tỗ chức sở hữu tài sản đó khi chấm dứt việc làm, hợp đồng hay thỏa thuận của họ.

A.8.2. Phân loại thông tin

Mục tiêu: Nhằm đảm bảo rằng thông tin sẽ có mức độ bảo vệ phù hợp theo tầm quan trọng của thông tin với tổ chức.

A.8.2.1. Phân loại thông tin

Thông tin cần được phân loại dựa trên các yêu cầu pháp lý, giá trị, mức độ quan trọng và độ nhạy cảm với việc tiết lộ hoặc sửa đổi trái phép.

A.8.2.2. Dán nhãn thông tin

Một tập hợp các thủ tục về việc dán nhãn thông tin một cách hợp lý cần được phát triển và triển khai phù hợp với kế hoạch phân loại thông tin đã được tổ chức thông qua.

A.8.2.3. Xử lý tài sản

Cần phải xây dựng và triển khai các thủ tục xử lý tài sản phù hợp với kế hoạch phân loại thông tin đã được tỗ chức thông qua.

A.8.3. Thông tin và các phương tiện xử lý thông tin

Mục tiêu: Nhằm ngăn ngừa việc tiết lộ, sửa đổi, xóa bỏ hoặc phá hoại trái phép thông tin được lưu trữ trên phương tiện truyền thông.

A.8.3.1. Quản lý phương tiện truyền thông có thể di dời

Cần triển khai các thủ tục quản lý các phương tiện có thể di dời phù hợp với cơ cấu phân loại đã được tỗ chức thông qua.

A.8.3.2. Loại bỏ các phương tiện truyền thông

Các phương tiện cần được loại bỏ một cách an toàn khi không còn cần thiết theo các thủ tục xử lý chính thức.

A.8.3.3. Vận chuyển phương tiện vật lý

Phương tiện truyền thông có chứa thông tin phải được bảo vệ chống lại sự truy cập trái phép, sử dụng sai mục đích hoặc làm hư hỏng trong quá trình vận chuyển.

A.9. Quản lý truy cập

A.9.1. Các yêu cầu nghiệp vụ cho việc kiểm soát truy cập

Mục tiêu: Nhằm giới hạn quyền truy cập vào các phương tiện xử lý thông tin và thông tin.

A.9.1.1. Chính sách quản lý truy cập

Một chính sách quản lý truy cập phải được thiết lập, được ghi thành văn bản và soát xét dựa trên các yêu cầu nghiệp vụ và an toàn thông tin.

A.9.1.2. Truy cập vào hệ thống mạng và các dịch vụ mạng

Người dùng chỉ được cấp quyền truy cập vào mạng và các dịch vụ mạng mà họ đã được cấp quyền sử dụng cụ thể.

A.9.2. Quản lý truy cập người dùng

Mục tiêu: Nhằm đảm bảo người dùng hợp lệ được truy cập và ngăn chặn những người dùng không hợp lệ truy cập trái phép tới các hệ thống và dịch vụ thông tin.

A.9.2.1. Đăng ký và xóa đăng ký thành viên

Quy trình đăng ký và xóa đăng ký thành viên chính thức phải được thực hiện để cho phép gán các quyền truy cập hợp lệ.

A.9.2.2. Cấp phát quyền truy cập người dùng

Quy trình cấp phát quyền truy cập người dùng chính thức phải được triển khai để gan hoặc thu hồi quyền truy cập cho tất cả loại người sử dụng tới tất cả các hệ thống và dịch vụ.

A.9.2.3. Quản lý đặc quyền truy cập

Việc cấp phát và sử dụng các đặc quyền truy cập phải được giới hạn và kiểm soát.

A.9.2.4. Quản lý thông tin xác thực bí mật người dùng

Việc cấp phát thông tin xác thực bí mật phải được kiểm soát thông qua quá trình quản lý chính thức.

A.9.2.5. Soát xét quyền truy cập người dùng

Chủ sở hữu tài sản cần định kỳ soát xét các quyền truy cập của người dùng.

A.9.2.6. Hủy bỏ hoặc điều chỉnh quyền truy cập

Quyền truy cập của tất cả người lao động và người sử dụng bên ngoài vào các phương tiện xử lý thông tin và thông tin phải được dỡ bỏ sau khi chấm dứt công việc, hợp đồng hoặc thoả thuận của họ, hoặc phải điều chỉnh khi thay đổi.

A.9.3. Trách nhiệm của người sử dụng

Mục tiêu: Nhằm làm cho người dùng có trách nhiệm đảm bảo an toàn thông tin xác thực của họ.

A.9.3.1. Sử dụng thông tin xác thực bí mật

Người dùng phải được yêu cầu tuân thủ quy tắc thực hành của tổ chức trong quá trình sử dụng thông tin xác thực bí mật.

A.9.4. Quản lý truy cập vào hệ thống và ứng dụng

Mục tiêu: Nhằm ngăn chặn truy cập trái phép vào các hệ thống và ứng dụng.

A.9.4.1. Hạn chế truy cập thông tin

Truy cập tới thông tin và các chức năng của hệ thống ứng dụng cần được hạn chế phù hợp với chính sách quản lý truy cập đã xác định.

A.9.4.2. Các thủ tục đăng nhập an toàn

Khi có yêu cầu của chính sách quản lý truy cập, việc truy cập đến các hệ thống và ứng dụng cần được kiểm soát bởi thủ tục đăng nhập an toàn.

A.9.4.3. Hệ thống quản lý mật khẩu

Các hệ thống quản lý mật khẩu phải có khả năng tương tác và đảm bảo độ khó của mật khẩu.

A.9.4.4. Sử dụng các chương trình tiện ích ưu tiên

Việc sử dụng các chương trình tiện ích có khả năng ảnh hưởng đến các biện pháp kiểm soát ứng dụng và hệ thống phải được giới hạn và kiểm soát chặt chẽ.

A.9.4.5. Kiểm soát truy cập vào mã nguồn của chương trình

Việc truy cập đến mã nguồn của chương trình cần được giới hạn chặt chẽ.

A.10. Mật mã

A.10.1. Biện pháp kiểm soát mật mã

Mục tiêu: Đảm bảo sử dụng phù hợp và hiệu quả mật mã để bảo vệ tính bí mật, tính xác thực và/hoặc tính toàn vẹn của thông tin.

A.10.1.1. Chính sách sử dụng các biện pháp kiểm soát mật mã

Một chính sách về việc sử dụng các biện pháp kiểm soát mật mã để bảo vệ thông tin cần được xây dựng và triển khai.

A.10.1.2. Quản lý khóa

Cần xây dựng và triển khai chính sách sử dụng, bảo vệ và thời gian tồn tại của khóa mật mã trong suốt toàn bộ vòng đời của chúng.

A.11. Đảm bảo an toàn vật lý và môi trường

A.11.1. Khu vực an toàn

Mục tiêu: Nhằm ngăn chặn truy cập vật lý trái phép, gây thiệt hại và can thiệp tới các phương tiện xử lý thông tin và thông tin của tổ chức.

A.11.1.1. Vành đai an toàn vật lý

Vành đai an toàn phải được xác định và sử dụng để bảo vệ khu vực chứa các phương tiện xử lý thông tin và thông tin quan trọng hoặc nhạy cảm.

A.11.1.2. Kiểm soát lối vào vật lý

Các khu vực cần được bảo vệ bằng các biện pháp kiểm soát lối vào thích hợp nhằm đảm bảo chỉ những người có quyền mới được phép truy cập.

A.11.1.3. An toàn văn phòng, phòng làm việc và các thiết bị

Biện pháp bảo vệ an toàn vật lý cho các văn phòng, phòng làm việc và vật dụng cần được thiết kế và áp dụng.

A.11.1.4. Bảo vệ chống lại các mối đe dọa từ môi trường va bên ngoài

Bảo vệ vật lý chống lại các thảm họa thiên nhiên, các tai nạn hoặc tấn công độc hại phải được thiết kế và áp dụng.

A.11.1.5. Làm việc trong các khu vực an toàn

Cần thiết kế và áp dụng các thủ tục để làm việc trong các khu vực an toàn.

A.11.1.6 Các khu vực phân phối và tập kết hàng

Các điểm truy cập mà người truy cập không cần cấp phép như khu vực phân phối và tập kết hàng ... phải được quản lý và, nếu có thể, được cách ly khỏi các phương tiện xử lý thông tin để tránh tình trạng truy cập trái phép.

A.11.2. Thiết bị

Mục tiêu: Nhằm ngăn ngừa sự mất mát, hư hại, đánh cắp hoặc lợi dụng tài sản và làm gián đoạn hoạt động của tổ chức.

A.11.2.1. Bố trí và bảo vệ thiết bị

Thiết bị phải được bố trí và được bảo vệ nhằm giảm thiểu các rủi ro từ các mối đe dọa, các hiểm họa từ môi trường hay các truy cập trái phép.

A.11.2.2. Các tiện ích hỗ trợ

Thiết bị phải được bảo vệ khỏi sự cố về nguồn điện cũng như các sự gián đoạn khác có nguyên nhân từ các tiện ích hỗ trợ

A.11.2.3. An toàn cho dây cáp

Dây cáp điện và cáp truyền thông mang dữ liệu hoặc các dịch vụ thông tin hỗ trợ phải được bảo vệ khỏi việc bị chặn, bị xâm phạm hoặc làm hư hại.

A.11.2.4. Bảo dưỡng thiết bị

Thiết bị cần được bảo dưỡng đúng quy cách nhằm đảm bảo luôn sẵn sàng và toàn vẹn.

A.11.2.5. Di dời tài sản

Không được mang thiết bị, thông tin hoac phan mềm ra khỏi trụ sở nếu chưa được phép.

A.11.2.6. An toàn cho thiết bị và tài sản hoạt động bên ngoài trụ sở của tổ chức

Phải đảm bảo an toàn cho các tài sản sử dụng bên ngoài, chú ý đến các rủi ro khác nhau khi làm việc bên ngoài phạm vi của tổ chức.

A.11.2.7. An toàn khi loại bỏ và tái sử dụng thiết bị

Tất cả các bộ phận của thiết bị có chứa các phương tiện lưu trữ thông tin phải được kiểm tra nhằm đảm bảo rằng tất cả dữ liệu nhạy cảm và phần mềm có bản quyền phải được xóa bỏ hoặc ghi đè trước khi loại bỏ hoặc tái sử dụng thiết bị cho mục đích khác.

A.11.2.8. Thiết bị người dùng khi không sử dụng

Người dùng cần đảm bảo rằng thiết bị phải được bảo vệ thích hợp khi không sử dụng.

A.11.2.9. Chính sách bàn sạch và màn hình sạch

Một chính sách bàn sạch cho các loại giấy tờ và phương tiện truyền thông lưu trữ di động và một chính sách màn hình sạch cho các phương tiện xử lý thông tin phải được thông qua.

A.12. An toàn vận hành

A.12.1. Các thủ tục và trách nhiệm vận hành

Mục tiêu: Nhằm đảm bảo vận hành các phương tiện xử lý thông tin được an toàn và chính xác.

A.12.1.1. Các thủ tục vận hành được lập thành văn bản

Các thủ tục vận hành cần được lập thành văn bản và luôn sẵn sàng đối với mọi người dùng cần dùng đến.

A.12.1.2. Quản lý thay đổi

Cần phải kiểm soát các thay đổi trong tổ chức, các quy trình nghiệp vụ, các phương tiện xử lý thông tin và hệ thống xử lý thông tin có ảnh hưởng tới an toàn thông tin.

A.12.1.3. Quản lý năng lực hệ thống

Việc sử dụng tài nguyên phải được theo dõi, điều chỉnh và dự báo các yêu cầu năng lực hệ thống trong tương lai để đảm bảo yêu cầu hiệu năng.

A.12.1.4. Phân tách các chức năng phát triển, kiểm thử và vận hành

Các chức năng phát triển, kiểm thử và môi trường hoạt động cần được phân tách nhằm giảm thiểu các rủi ro của việc truy cập hoặc thay đổi môi trường vận hành trái phép.

A.12.2. Bảo vệ chống lại phần mềm độc hại

Mục tiêu: Nhằm đảm bảo rằng các phương tiện xử lý thông tin và thông tin được bảo vệ chống lại phần mềm độc hại.

A.12.2.1. Quản lý chống lại phần mềm độc hại

Các biện pháp kiểm soát trong việc phát hiện, ngăn chặn và phục hồi nhằm bảo vệ chống lại các phần mềm độc hại phải được thực hiện, kết hợp với nâng cao nhận thức của người sử dụng.

A.12.3. Sao lưu

Mục tiêu: Nhằm bảo vệ chống lại việc mất mát dữ liệu.

A.12.3.1. Sao lưu thông tin

Bản sao lưu các thông tin, phần mềm và các hình ảnh hệ thống phải được thực hiện và kiểm tra thường xuyên theo một chính sách sao lưu đã được thông qua.

A.12.4. Ghi nhật ký và giám sát

Mục tiêu: Nhằm ghi lại các sự kiện và tạo chứng cứ.

A.12.4.1. Ghi nhật ký sự kiện

Việc ghi nhật ký tất cả các hoạt động của người dùng, các ngoại lệ, các lỗi và các sự kiện an toàn thông tin cần phải được thực hiện và duy trì và soát xét thường xuyên.

A.12.4.2. Bảo vệ thông tin nhật ký.

Các chức năng ghi nhật ký cũng như thông tin nhật ký cần được bảo vệ khỏi sự giả mạo và truy cập trái phép.

A.12.4.3. Nhật ký điều hành và quản trị

Tất cả hoạt động của người quản trị cũng như người điều hành hệ thống cần phải được ghi nhật ký và các bản ghi đó cần được bảo vệ và soát xét thường xuyên.

A.12.4.4. Đồng bộ thời gian

Đồng hồ của các hệ thống xử lý thông tin có liên quan trong phạm vi tổ chức hoặc trong một phạm vi an toàn cần được đồng bộ với một nguồn thời gian tham chiếu duy nhất.

A.12.5 Quản lý các phần mềm vận hành

Mục tiêu: Nhằm đảm bảo tính toàn vẹn của các hệ thống vận hành.

A.12.5.1. Cài đặt phần mềm trên các hệ thống vận hành

Cần triển khai các thủ tục để kiểm soát quá trình cài đặt các phần mềm trên hệ thống vận hành.

A.12.6 Quản lý lỗ hổng kỹ thuật

Mục tiêu: Nhằm ngăn chặn việc khai thác các lỗ hỗng kỹ thuật.

A.12.6.1. Quản lý các lỗ hổng kỹ thuật

Thông tin về các lỗ hổng kỹ thuật của các hệ thống thông tin đang được sử dụng cần phải được thu thập kịp thời. Tổ chức cần công bố đánh giá về các lỗ hỗng này và thực hiện các biện pháp thích hợp để giải quyết các rủi ro liên quan.

A.12.6.2. Hạn chế việc cài đặt phần mềm

Cần thiết lập và triển khai các quy tắc cài đặt phần mềm đối với người dùng.

A.12.7. Soát xét việc đánh giá các hệ thống thông tin

Mục tiêu: Nhằm giảm thiều tác động của các hoạt động đánh giá đến các hệ thống vận hành.

A.12.7.1. Các biện pháp kiểm soát đánh giá hệ thống thông tin

Các yêu cầu và hoạt động đánh giá các hệ thống vận hành cần được hoạch định kỹ lưỡng và thống nhất để giảm thiều sự gián đoạn của các quy trình nghiệp vụ.

A.13. An toàn truyền thông

A.13.1. Quản lý an toàn mạng

Mục tiêu: Đảm bảo an toàn thông tin trong các mạng và hỗ trợ các phương tiện xử lý thông tin.

A.13.1.1. Các biện pháp kiểm soát mạng

Các mạng phải được kiểm soát và quản lý nhằm bảo vệ thông tin trong các hệ thống và các ứng dụng.

A.13.1.2. An toàn các dịch vụ mạng

Các cơ chế bảo mật, các mức dịch vụ và các yêu cầu quản lý của tất cả dịch vụ mạng phải được xác định và bao gồm trong thỏa thuận dịch vụ mạng, bất kể dịch vụ là do nội bộ cung cấp hay thuê khoán bên ngoài.

A.13.1.3. Sự phân tách trên mạng

Các nhóm dịch vụ thông tin, người dùng và hệ thống thông tin cần được phân tách trên các mạng.

A.13.2. Truyền thông tin

Mục tiêu: Nhằm duy trì an toàn cho các thông tin truyền trong nội bộ tổ chức hoặc với các thực thể bên ngoài.

A.13.2.1. Các thủ tục và chính sách truyền thông tin

Các chính sách, thủ tục và biện pháp kiểm soát chính thức phải được thực hiện nhằm bảo vệ việc truyền thông tin thông qua việc sử dụng tất cả các loại phương tiện truyền thông.

A.13.2.2. Các thỏa thuận truyền thông tin

Các thỏa thuận phải đặt ra việc truyền thông an toàn các thông tin nghiệp vụ giữra tổ chức và các đối tác bên ngoài.

A.13.2.3. Thông điệp điện tử

Thông tin bao hàm trong các thông điệp điện tử cần được bảo vệ một cách thích hợp.

A.13.2.4. Thỏa thuận bảo mật hoặc không tiết lộ

Các yêu cầu cho thỏa thuận bảo mật hoặc không tiết lộ phản ánh nhu cầu của tổ chức đối với việc bảo vệ thông tin phải được xác định rõ, thường xuyên được soát xét và được ghi thành văn bản.

A.14. Tiếp nhận, phát triển và duy trì các hệ thống thông tin

A.14.1 Các yêu cầu an toàn của hệ thống thông tin

Mục tiêu: Nhằm đảm bảo rằng an toàn thông tin là một phần không thể tách rời của các hệ thống thông tin trong toàn bộ vòng đời. Điều này cũng bao gồm các yêu cầu đối với hệ thống thông tin cung cấp các dịch vụ trên mạng công cộng.

A.14.1.1. Phân tích và đặc tả các yêu cầu an toàn thông tin

Các yêu cầu liên quan tới an toàn thông tin phải được bao gồm trong các yêu cầu đối với các hệ thống thông tin mới hoặc các cải tiến từ các hệ thống thông tin hiện có.

A.14.1.2. An toàn các dịch vụ ứng dụng trên mạng công cộng

Thông tin liên quan trong các dịch vụ ứng dụng đi qua mạng công cộng phải được bảo vệ khỏi các hành vi gian lận, tranh chấp kết nối, tiết lộ và sửa đổi trái phép.

A.14.1.3. Bảo vệ các giao dịch dịch vụ ứng dụng

Thông tin liên quan đến các giao dịch dịch vụ ứng dụng phải được bảo vệ để ngăn ngừa sự truyền dẫn không đầy đủ, lỗi định tuyến, thay đổi thông điệp trái phép, tiết lộ trái phép, sao chép hoặc chuyển tiếp thông tin trái phép.

A.14.2. An toàn trong quá trình phát triển và hỗ trợ

Mục tiêu: Nhằm đảm bảo rằng an toàn thông tin được thiết kế và triển khai trong vòng đời phát triển của các hệ thống thông tin.

A.14.2.1. Chính sách phát triển an toàn

Quy tắc cho phát triển phần mềm và hệ thống cần được thiết lập và áp dụng để phát triển trong tổ chức.

A.14.2.2. Các thủ tục kiểm soát thay đổi hệ thống

Các thay đổi hệ thống trong vòng đời phát triển phải được kiểm soát bằng cách sử dụng các thủ tục kiểm soát thay đổi chính thức.

A.14.2.3. Soát xét kỹ thuật của các ứng dụng sau khi thay đổi nền tảng hệ điều hành

Khi nền tảng hệ điều hành thay đổi, các ứng dụng nghiệp vụ quan trọng phải được soát xét và kiểm tra nhằm đảm bảo không có tác động xấu đến hoạt động hoặc sự an toàn của tổ chức.

A.14.2.4. Hạn chế thay đổi các gói phần mềm

Việc sửa đổi các gói phần mềm không được khuyến khích, chỉ giới hạn trong những thay đổi cần thiết và tất cả những thay đổi phải được kiểm soát chặt chẽ.

A.14.2.5. Các nguyên tắc kỹ thuật an toàn hệ thống

Các nguyên tắc kỹ thuật an toàn hệ thống phải được thiết lập, ghi thành văn bản, duy trì và áp dụng cho bất kỳ hệ thống thông tin nào được triển khai.

A.14.2.6. An toàn môi trường phát triển

Các tổ chức cần thiết lập và bảo vệ thích hợp môi trường phát triển an toàn cho hệ thống và các nỗ lực tích hợp bao gồm toàn bộ vòng đời phát triển hệ thống.

A.14.2.7. Phát triển phần mềm thuê ngoài

Tổ chức phải thực hiện giám sát và theo dõi các hoạt động phát triển hệ thống phần mềm thuê ngoài.

A.14.2.8. Kiểm thử an toàn hệ thống

Kiểm thử các chức năng an toàn phải được thực hiện trong quá trình phát triển.

A.14.2.9. Kiểm thử chấp nhận hệ thống

Các chương trình kiểm thử chấp nhận và các tiêu chí liên quan phải được thiết lập cho các hệ thống thông tin mới, các nâng cấp và phiên bản mới.

A.14.3. Dữ liệu kiểm thử

Mục tiêu: Nhằm đảm bảo bảo vệ dữ liệu được sử dụng cho việc kiểm thử.

A.14.3.1. Bảo vệ dữ liệu kiểm thử

Dữ liệu kiểm thử cần được lựa chọn, kiểm soát và bảo vệ một cách thận trọng.

A.15. Quan hệ với nhà cung cấp

A.15.1. An toàn thông tin trong các mối quan hệ với nhà cung cấp

Mục tiêu: Nhằm đảm bảo bảo vệ các tài sản có thể truy cập bởi các nhà cung cấp của tổ chức.

A.15.1.1. Chính sách an toàn thông tin trong mối quan hệ với nhà cung cấp

Các yêu cầu an toàn thông tin nhằm giảm thiểu rủi ro liên quan đến việc truy cập của các nhà cung cấp tới hệ thống thông tin hoặc các phương tiện xử lý thông tin của tổ chức phải lập thành văn bản.

A.15.1.2. Đảm bảo an toàn trong các thỏa thuận với nhà cung cấp

Tất cả các yêu cầu an toàn thông tin liên quan phải được thiết lập và thống nhất với từng nhà cung cấp để có thể truy cập, xử lý, lưu trữ, truyền thông hoặc cung cấp các thành phần cơ sở hạ tầng công nghệ thông tin cho tổ chức.

A.15.1.3. Chuỗi cung ứng công nghệ thông tin và truyền thông

Các thỏa thuận với các nhà cung cấp phải bao gồm các yêu cầu để giải quyết các rủi ro an toàn thông tin liên quan đến chuỗi cung cấp sản phẩm và các dịch vụ truyền thông và công nghệ thông tin.

A.15.2. Quản lý chuyển giao dịch vụ cho nhà cung cấp

Mục tiêu: Để duy trì một mức độ thống nhất về an toàn thông tin và chuyển giao dịch vụ phù hợp trong các thỏa thuận với nhà cung cấp.

A.15.2.1. Giám sát và soát Biện pháp kiểm soát xét các dịch vụ của nhà cung cấp

Các tổ chức phải thường xuyên giám sát, soát xét và đánh giá dịch vụ cung cấp.

A.15.2.2. Quản lý các thay đổi của các dịch vụ cung cấp

Các thay đỗi về cung cấp các dịch vụ của các nhà cung cấp, bao gồm việc duy trì và cải tiến các chính sách, thủ tục và biện pháp kiểm soát an toàn thông tin hiện hành, cần được quản lý, chú ý đến mức độ rủi ro của thông tin, hệ thống và quy trình nghiệp vụ cũng như việc đánh giá lại các rủi ro.

A.16. Quản lý các sự cố an toàn thông tin

A.16.1. Quản lý sự cố an toàn thông tin và các cải tiến

Mục tiêu: Nhằm đảm bảo một cách tiếp cận nhất quán và hiệu quả được áp dụng trong việc quản lý các sự cố an toàn thông tin, bao gồm cả truyền thông về các điểm yếu và các sự kiện an toàn thông tin.

A.16.1.1. Các trách nhiệm và thủ tục

Các trách nhiệm và thủ tục quản lý cần được thiết lập nhằm đảm bảo sự phản ứng nhanh chóng, hiệu quả, đúng trình tự khi xảy ra các sự cố an toàn thông tin.

A.16.1.2. Báo cáo các sự kiện an toàn thông tin

Các sự kiện an toàn thông tin cần được báo cáo thông qua các kênh quản lý thích hợp theo cách nhanh nhất có thể.

A.16.1.3. Báo cáo các điểm yếu về an toàn thông tin

Mọi nhân viên, người kí kết hợp đồng sử dụng dịch vụ và hệ thống thông tin của tổ chức cần được yêu cầu ghi chú và báo cáo lại bất kỳ điểm yếu nào về an toàn thông tin thấy được hoặc cảm thấy nghi ngờ trong các hoạt động hoặc dịch vụ của hệ thống.

A.16.1.4. Đánh giá và quyết định về các sự kiện an toàn thông tin

Các sự kiện an toàn thông tin phải được đánh giá và quyết định liệu chúng có được phân loại là các sự cố an toàn thông tin.

A.16.1.5. Ứng phó với các sự cố an toàn thông tin

Các sự cố an toàn thông tin phải được ứng phó phù hợp với các thủ tục đã được lập thành văn bản.

A.16.1.6. Rút bài học kinh nghiệm từ các sự cố an toàn thông tin

Kiến thức thu được từ việc phân tích và giải quyết các sự cố an toàn thông tin phải được sử dụng để giảm thiểu khả năng hoặc tác động của các sự cố trong tương lai.

A.16.1.7. Tập hợp bằng chứng

Các tổ chức phải xác định và áp dụng các quy trình xác định, tập hợp, thu nhận và bảo quản thông tin có thể được dùng làm bằng chứng.

A.17. Các khía cạnh an toàn thông tin trong quản lý hoạt động nghiệp vụ liên tục

A.17.1. Đảm bảo an toàn thông tin liên tục

Mục tiêu: Tính liên tục của an toàn thông tin cần phải nằm trong các hệ thống quản lý tính liên tục nghiệp vụ của tổ chức.

A.17.1.1. Kế hoạch đảm bảo an toàn thông tin liên tục

Tổ chức phải xác định các yêu cầu của mình cho an toàn thông tin và tính liên tục của việc quản lý an toàn thông tin trong các tình huống bất lợi, ví dụ: trong một cuộc khủng hoảng hay thiên tai.

A.17.1.2. Triển khai đảm bảo an toàn thông tin liên tục

Tổ chức phải thiết lập, lập văn bản, triển khai và duy trì các quy trình, thủ tục và các biện pháp kiểm soát nhằm đảm bảo mức độ liên tục cho an toàn thông tin được yêu cầu trong các tình huống bất lợi.

A.17.1.3. Xác minh, soát xét và đánh giá đảm bảo an toàn thông tin liên tục

Tổ chức cần xác minh việc thiết lập và triển khai các biện pháp kiểm soát an toàn thông tin liên tục thường xuyên trong nội bộ để đảm bảo rằng chúng có hiệu lực cũng như hiệu quả trong các tình huống bất lợi.

A.17.2. Dự phòng

Mục tiêu: Nhằm đảm bảo tính sẵn sàng của các phương tiện xử lý thông tin.

A.17.2.1. Tính sẵn sàng của các phương tiện xử lý thông tin

Các phương tiện xử lý thông tin phải được triển khai với dự phòng đủ để đáp ứng các yêu cầu về tính sẵn sàng.

A.18. Sự tuân thủ

A.18.1. Sự tuân thủ với các yêu cầu pháp lý và hợp đồng

Mục tiêu: Nhằm tránh sự vi phạm pháp luật, quy định, nghĩa vụ theo các hợp đồng đã ký kết có liên quan đến an toàn thông tin và tránh vi phạm các yêu cầu về đảm bảo an toàn thông tin.

A.18.1.1. Xác định các yêu cầu của hợp đồng và điều luật được áp dụng

Tất cả các yêu cầu về luật pháp, quy định, hợp đồng đã ký có liên quan và phương pháp tiếp cận của tổ chức để đáp ứng các yêu cầu này phải được xác định một cách rõ ràng, lập thành văn bản và cập nhật thường xuyên cho mỗi hệ thống và tổ chức.

A.18.1.2. Quyền sở hữu trí tuệ (IPR)

Các thủ tục phù hợp cần được triển khai nhằm đảm bảo sự tuân thủ với các yêu cầupháp lý, các quy định và cam kết theo hợp đồng liên quan đến quyền sở hữu trí tuệ và sử dụng các sản phẩm phần mềm bản quyền.

A.18.1.3. Bảo vệ các hồ sơ

Các hồ sơ cần được bảo vệ khỏi sự mất mát, phá hủy, giả mạo, truy cập trái phép và phát hành trái phép, phù hợp với pháp luật, quy định, các nghĩa vụ trong hợp đồng đã ký và các yêu cầu nghiệp vụ.

A.18.1.4. Sự riêng tư và bảo vệ thông tin có thể định danh cá nhân

Sự riêng tư và thông tin có thể định danh cá nhân phải được đảm bảo theo yêu cầu của pháp luật và các quy định liên quan nếu có.

A.18.1.5. Quy định về quản lý mật mã

Các kiểm soát mật mã phải được áp dụng phù hợp với tất cả các thỏa thuận, luật pháp và các quy định liên quan.

A.18.2 Soát xét an toàn thông tin

Mục tiêu: Nhằm đảm bảo rằng an toàn thông tin được triển khai và vận hành phù hợp với các chính sách và thủ tục của tổ chức.

A.18.2.1. Soát xét một cách độc lập về an toàn thông tin

Cách tiếp cận của tổ chức để quản lý an toàn thông tin và việc triển khai (tức là các mục tiêu, biện pháp kiểm soát, các chính sách, các quá trình và thủ tục đảm bảo an toàn thông tin) phải được soát xét độc lập theo định kỳ hoặc khi xuất hiện những thay đổi đáng kể về triển khai an toàn xảy ra.

A.18.2.2. Sự tuân thủ các chính sách và tiêu chuẩn an toàn

Người quản lý phải thường xuyên soát xét sự tuân thủ của việc xử lý thông tin và quy trình trong phạm vi trách nhiệm của mình với các chính sách, các tiêu chuẩn an toàn và các yêu cầu an toàn khác.

A.18.2.3. Soát xét tuân thủ kỹ thuật

Các hệ thống thông tin phải được soát xét thường xuyên sự tuân thủ các chính sách và các tiêu chuẩn an toàn thông tin của tổ chức.