

TCVN

TIÊU CHUẨN QUỐC GIA

TCVN ISO/IEC 27002:2020

ISO/IEC 27002:2013

Xuất bản lần 2

**CÔNG NGHỆ THÔNG TIN –
CÁC KỸ THUẬT AN TOÀN – QUY TẮC THỰC HÀNH
QUẢN LÝ AN TOÀN THÔNG TIN**

*Information technology - Security techniques –
Code of practice for information security management*

HÀ NỘI - 2020

Mục lục

1	Phạm vi áp dụng	11
2	Tài liệu viện dẫn.....	11
3	Thuật ngữ và định nghĩa	11
4	Cấu trúc của tiêu chuẩn	11
4.1	Các lĩnh vực	12
4.2	Các phân loại kiểm soát.....	12
5	Chính sách an toàn thông tin.....	12
5.1	Định hướng quản lý an toàn thông tin.....	12
5.1.1	Chính sách cho an toàn thông tin	12
5.1.2	Soát xét chính sách an toàn thông tin.....	14
6	Tổ chức đảm bảo an toàn thông tin	15
6.1	Tổ chức nội bộ.....	15
6.1.1	Vai trò và trách nhiệm đảm bảo an toàn thông tin.....	15
6.1.2	Phân tách nhiệm vụ.....	16
6.1.3	Liên lạc với những cơ quan/ tổ chức có thẩm quyền	16
6.1.4	Liên lạc với các nhóm chuyên gia	17
6.1.5	An toàn thông tin trong quản lý dự án.....	17
6.2	Thiết bị di động và làm việc từ xa	18
6.2.1	Chính sách sử dụng thiết bị di động	18
6.2.2	Làm việc từ xa.....	20
7	An toàn nguồn nhân lực	21
7.1	Trước khi tuyển dụng	21
7.1.1	Thăm tra.....	21
7.1.2	Điều khoản và điều kiện tuyển dụng.....	22
7.2	Trong thời gian làm việc	23
7.2.1	Trách nhiệm của ban lãnh đạo	23

7.2.2	Nhận thức, giáo dục và đào tạo về an toàn thông tin.....	24
7.2.3	Xử lý kỷ luật.....	26
7.3	Chấm dứt hoặc thay đổi công việc	26
7.3.1	Trách nhiệm kết thúc hoặc thay đổi hợp đồng	27
8	Quản lý tài sản	27
8.1	Trách nhiệm đối với tài sản	27
8.1.1	Kiểm kê tài sản.....	27
8.1.2	Quyền sở hữu tài sản thông tin	28
8.1.3	Sử dụng hợp lý tài sản	29
8.1.4	Trả lại tài sản.....	29
8.2	Phân loại thông tin	30
8.2.1	Phân loại thông tin.....	30
8.2.2	Gắn nhãn thông tin	31
8.2.3	Xử lý tài sản	31
8.3	Xử lý thiết bị lưu trữ	32
8.3.1	Quản lý các phương tiện lưu trữ thông tin có thể di dời.....	32
8.3.2	Loại bỏ các phương tiện lưu trữ thông tin.....	33
8.3.3	Vận chuyển phương tiện vật lý	34
9	Kiểm soát truy cập.....	35
9.1	Yêu cầu nghiệp vụ đối với kiểm soát truy cập	35
9.1.1	Chính sách kiểm soát truy cập.....	35
9.1.2	Truy cập mạng và các dịch vụ mạng	36
9.2	Kiểm soát truy cập người dùng	37
9.2.1	Đăng ký và hủy thành viên đăng ký	37
9.2.2	Cấp phát quyền truy cập người dùng	38
9.2.3	Kiểm soát đặc quyền truy cập.....	39
9.2.4	Kiểm soát các thông tin xác thực bí mật của người dùng	39
9.2.5	Soát xét các quyền truy cập người dùng	40

9.2.6	Hủy bỏ hoặc chỉnh sửa quyền truy cập	41
9.3	Các trách nhiệm người dùng	42
9.3.1	Sử dụng thông tin xác thực bí mật	42
9.4	Kiểm soát truy cập vào hệ thống và ứng dụng.....	43
9.4.1	Hạn chế truy cập thông tin.....	43
9.4.2	Các thủ tục đăng nhập an toàn.....	43
9.4.3	Hệ thống quản lý mật khẩu.....	45
9.4.4	Sử dụng các chương trình tiện ích đặc quyền.....	45
9.4.5	Kiểm soát truy cập vào mã nguồn chương trình	46
10	Mật mã.....	47
10.1	Kiểm soát mật mã.....	47
10.1.1	Chính sách sử dụng các kiểm soát mật mã.....	47
10.1.2	Quản lý khóa	48
11	An toàn vật lý và môi trường	50
11.1	Các khu vực an toàn.....	50
11.1.1	Vành đai an toàn vật lý	50
11.1.2	Kiểm soát lối vào vật lý.....	51
11.1.3	Bảo vệ các văn phòng, phòng làm việc và vật dụng	52
11.1.4	Bảo vệ chống lại các mối đe dọa từ bên ngoài và từ môi trường.....	53
11.1.5	Làm việc trong các khu vực an toàn.....	53
11.1.6	Các khu vực phân phối và tập kết hàng	53
11.2	Đảm bảo an toàn trang thiết bị.....	54
11.2.1	Bố trí và bảo vệ thiết bị.....	54
11.2.2	Các tiện ích hỗ trợ	55
11.2.3	An toàn cho dây cáp.....	55
11.2.4	Bảo dưỡng thiết bị.....	56
11.2.5	An toàn khi di chuyển thiết bị.....	57

11.2.6	An toàn cho thiết bị và tài sản hoạt động bên ngoài các trụ sở tổ chức	57
11.2.7	Xử lý khi loại bỏ hoặc tái sử dụng thiết bị	58
11.2.8	Thiết bị người dùng không giám sát	59
11.2.9	Chính sách màn hình sạch và bàn làm việc sạch	59
12	An toàn vận hành.....	60
12.1	Thủ tục và trách nhiệm vận hành	60
12.1.1	Các thủ tục vận hành được lập tài liệu.....	60
12.1.2	Quản lý thay đổi.....	61
12.1.3	Quản lý năng lực	62
12.1.4	Phân tách các chức năng phát triển, kiểm thử và môi trường vận hành	63
12.2	Bảo vệ khỏi phần mềm độc hại	64
12.2.1	Kiểm soát chống lại phần mềm độc hại	64
12.3	Sao lưu	66
12.3.1	Thông tin sao lưu.....	66
12.4	Ghi nhật ký và giám sát.....	67
12.4.1	Ghi nhật ký các sự kiện	67
12.4.2	Bảo vệ các thông tin nhật ký.....	68
12.4.3	Nhật ký của người điều hành và người quản trị.....	69
12.4.4	Đồng bộ thời gian	69
12.5	Kiểm soát phần mềm điều hành.....	70
12.5.1	Cài đặt phần mềm trên các hệ thống vận hành.....	70
12.6	Quản lý lỗ hổng kỹ thuật	71
12.6.1	Quản lý các lỗ hổng kỹ thuật.....	71
12.6.2	Hạn chế cài đặt phần mềm	73
12.7	Soát xét việc đánh giá các hệ thống thông tin	74
12.7.1	Các kiểm soát đánh giá hệ thống thông tin	74
13	An toàn truyền thông.....	74
13.1	Quản lý an toàn mạng.....	74

13.1.1	Các biện pháp kiểm soát mạng	74
13.1.2	An toàn các dịch vụ mạng	75
13.1.3	Phân tách mạng	76
13.2	An toàn truyền tải thông tin	77
13.2.1	Các chính sách và thủ tục truyền tải thông tin	77
13.2.2	Các thỏa thuận truyền tải thông tin	78
13.2.3	Thông điệp điện tử	79
13.2.4	Các thỏa thuận an toàn hay không tiết lộ	80
14	Tiếp nhận, phát triển và bảo trì hệ thống	81
14.1	Yêu cầu đảm bảo an toàn cho các hệ thống thông tin	81
14.1.1	Phân tích và đặc tả các yêu cầu về an toàn thông tin	81
14.1.2	An toàn các dịch vụ ứng dụng trên mạng công cộng	82
14.1.3	Bảo vệ các giao dịch dịch vụ ứng dụng	84
14.2	Bảo đảm an toàn trong các quá trình hỗ trợ và phát triển	85
14.2.1	Chính sách phát triển an toàn	85
14.2.2	Các thủ tục kiểm soát thay đổi hệ thống	86
14.2.3	Soát xét kỹ thuật của các ứng dụng sau khi thay đổi nền tảng hệ điều hành	87
14.2.4	Hạn chế thay đổi các gói phần mềm	88
14.2.5	Các nguyên tắc kỹ thuật an toàn hệ thống	88
14.2.6	Môi trường phát triển an toàn	89
14.2.7	Phát triển phần mềm thuê ngoài	90
14.2.8	Kiểm thử an toàn của hệ thống	91
14.2.9	Kiểm thử chấp nhận hệ thống	91
14.3	Dữ liệu kiểm thử	91
14.3.1	Bảo vệ dữ liệu kiểm thử	91
15	Các mối quan hệ với nhà cung cấp	92
15.1	An toàn thông tin trong các mối quan hệ với nhà cung cấp	92

15.1.1	Chính sách an toàn thông tin trong các mối quan hệ với nhà cung cấp	92
15.1.2	Đảm bảo an toàn trong các thỏa thuận với nhà cung cấp.....	94
15.1.3	Chuỗi cung ứng công nghệ thông tin và truyền thông.....	95
15.2	Quản lý chuyển giao dịch vụ của nhà cung cấp	97
15.2.1	Giám sát và soát xét dịch vụ của nhà cung cấp.....	97
15.2.2	Quản lý thay đổi của dịch vụ cung cấp	98
16	Quản lý sự cố an toàn thông tin	99
16.1	Quản lý các sự cố an toàn thông tin và các cải tiến	99
16.1.1	Trách nhiệm và thủ tục	99
16.1.2	Báo cáo các sự kiện an toàn thông tin.....	100
16.1.3	Báo cáo các lỗ hổng an toàn thông tin.....	101
16.1.4	Đánh giá và quyết định về sự kiện an toàn thông tin.....	101
16.1.5	Ứng phó sự cố an toàn thông tin	102
16.1.6	Rút bài học kinh nghiệm từ các sự cố an toàn thông tin	102
16.1.7	Thu thập bằng chứng	103
17	Các khía cạnh an toàn thông tin trong quản lý hoạt động nghiệp vụ liên tục.....	104
17.1	An toàn thông tin liên tục.....	104
17.1.1	Lập kế hoạch an toàn thông tin liên tục	104
17.1.2	Triển khai đảm bảo an toàn thông tin liên tục	105
17.1.3	Xác minh, soát xét và đánh giá an toàn thông tin liên tục	106
17.2	Dự phòng.....	107
17.2.1	Tính sẵn sàng của phương tiện xử lý thông tin.....	107
18	Sự tuân thủ.....	107
18.1	Sự tuân thủ các yêu cầu pháp lý và hợp đồng	107
18.1.1	Xác định các điều luật áp dụng và yêu cầu hợp đồng.....	107
18.1.2	Quyền sở hữu trí tuệ	108
18.1.3	Bảo vệ các hồ sơ.....	109
18.1.4	An toàn riêng tư và bảo vệ thông tin cá nhân	110

18.1.5	Quy định về quản lý mật mã.....	111
18.2	Soát xét về an toàn thông tin	111
18.2.1	Soát xét độc lập về an toàn thông tin.....	111
18.2.2	Sự tuân thủ các chính sách và tiêu chuẩn an toàn	112
18.2.3	Soát xét tuân thủ kỹ thuật.....	113
	Thư mục tài liệu tham khảo	115

Lời nói đầu

TCVN ISO/IEC 27002:2020 hoàn toàn tương đương với ISO/IEC 27002:2013 cùng các bản sửa chữa ISO/IEC 27002:2013/Cor.1:2014 và ISO/IEC 27002:2013/Cor.2:2015.

TCVN ISO/IEC 27002:2020 do Viện Công nghệ thông tin, Đại học Quốc gia Hà Nội biên soạn, Bộ Thông tin và Truyền thông đề nghị, Tổng cục Tiêu chuẩn Đo lường Chất lượng thẩm định, Bộ Khoa học và Công nghệ công bố.

Công nghệ thông tin – Các kỹ thuật an toàn - Quy tắc thực hành quản lý an toàn thông tin

Information technology – Security techniques – Code of practice for information security management

1 Phạm vi áp dụng

Tiêu chuẩn này đưa ra hướng dẫn cho các tiêu chuẩn an toàn thông tin và thực hành quản lý an toàn thông tin bao gồm việc lựa chọn, thực hiện và quản lý các kiểm soát có tính đến môi trường rủi ro an toàn thông tin của các tổ chức.

Tiêu chuẩn này được thiết kế để được sử dụng bởi các tổ chức có ý định:

- a) chọn lựa các kiểm soát trong quá trình thực hiện một hệ thống quản lý an toàn thông tin dựa trên TCVN ISO/IEC 27001^[10];
- b) thực hiện các kiểm soát an toàn thông tin được chấp nhận chung;
- c) phát triển các hướng dẫn quản lý an toàn thông tin của riêng mình.

2 Tài liệu viện dẫn

Tài liệu viện dẫn sau đây là cần thiết để áp dụng tiêu chuẩn này. Đối với các tài liệu viện dẫn ghi năm công bố thì áp dụng phiên bản được nêu. Đối với các tài liệu viện dẫn không ghi năm công bố thì áp dụng phiên bản mới nhất (bao gồm cả các sửa đổi, bổ sung).

TCVN 11238 (ISO/IEC 27000), Công nghệ thông tin - Các kỹ thuật an toàn - Hệ thống quản lý an toàn thông tin - Tổng quan và từ vựng.

3 Thuật ngữ và định nghĩa

Tiêu chuẩn này sử dụng các thuật ngữ và định nghĩa được đưa ra trong TCVN 11238.

4 Cấu trúc của tiêu chuẩn

Tiêu chuẩn này bao gồm 14 điều về kiểm soát an toàn, chứa đựng tổng số 35 phân loại an toàn và 114 biện pháp kiểm soát.

4.1 Các điều

Mỗi điều xác định các kiểm soát an toàn nằm trong một hoặc nhiều phân loại kiểm soát an toàn chính.

Thứ tự của các điều trong tiêu chuẩn này không có ý nghĩa phản ánh tầm quan trọng của chúng. Tùy thuộc vào bối cảnh, các kiểm soát an toàn từ bất kỳ hoặc tất cả các điều có thể là quan trọng, do đó mỗi tổ chức áp dụng tiêu chuẩn này cần xác định các kiểm soát cần được áp dụng, và mức độ quan trọng của những kiểm soát này và ứng dụng của chúng trong các quy trình nghiệp vụ cá nhân. Hơn nữa, các danh sách trong tiêu chuẩn này không theo thứ tự ưu tiên.

4.2 Các phân loại kiểm soát

Mỗi phân loại kiểm soát an toàn chính bao gồm:

- a) một mục tiêu kiểm soát trong đó ghi những gì phải đạt được;
- b) một hoặc nhiều kiểm soát có thể được áp dụng để đạt được mục tiêu kiểm soát .

Các mô tả kiểm soát được cấu trúc như sau:

Kiểm soát

Xác định các báo cáo kiểm soát cụ thể, để đáp ứng mục tiêu kiểm soát.

Hướng dẫn thi hành

Cung cấp thông tin chi tiết hơn để hỗ trợ thực hiện việc kiểm soát và đáp ứng mục tiêu kiểm soát. Các hướng dẫn có thể không hoàn toàn phù hợp hoặc đầy đủ trong mọi tình huống và có thể không đáp ứng đầy đủ các yêu cầu kiểm soát cụ thể của tổ chức.

Thông tin khác

Cung cấp thêm thông tin có thể cần được cân nhắc, ví dụ về khía cạnh pháp lý và việc tham chiếu đến các tiêu chuẩn khác. Nếu không có thông tin khác được cung cấp thì phần này không được hiển thị.

5 Chính sách an toàn thông tin

5.1 Định hướng quản lý an toàn thông tin

Mục tiêu: cung cấp định hướng quản lý và hỗ trợ an toàn thông tin tuân thủ theo yêu cầu nghiệp vụ và các quy định, pháp luật có liên quan.

5.1.1 Chính sách cho an toàn thông tin

Kiểm soát

Một tập hợp các chính sách an toàn thông tin cần được định nghĩa, được phê duyệt bởi bộ phận quản lý và được xuất bản, thông báo tới mọi nhân viên cũng như các bên liên quan.

Hướng dẫn thi hành

Ở cấp độ cao nhất, các tổ chức cần xác định một "chính sách an toàn thông tin" được phê duyệt bởi bộ phận quản lý và đưa ra các phương pháp tiếp cận của tổ chức để quản lý các mục tiêu an toàn thông tin của tổ chức.

Chính sách an toàn thông tin cần hướng đến các yêu cầu tạo ra bởi:

- a) chiến lược kinh doanh;
- b) các quy định, pháp luật và hợp đồng;
- c) môi trường đe dọa an toàn thông tin ở hiện tại và trong dự báo.

Chính sách an toàn thông tin cần bao gồm các quy định liên quan đến:

- a) định nghĩa về an toàn thông tin, các mục tiêu và các nguyên tắc để hướng dẫn tất cả các hoạt động liên quan đến an toàn thông tin;
- b) phân công trách nhiệm chung và trách nhiệm cụ thể về quản lý an toàn thông tin trên cơ sở xác định đúng vai trò;
- c) các quy trình để xử lý những độ sai lệch, trường hợp ngoại lệ.

Ở một mức độ thấp hơn, các chính sách an toàn thông tin cần được hỗ trợ bởi chính sách chuyên sâu theo từng chủ đề, trong đó có uỷ quyền tiếp tục thực hiện các kiểm soát an toàn thông tin và thường được cấu trúc để đáp ứng nhu cầu của các nhóm mục tiêu nhất định trong một tổ chức hoặc các chủ đề nhất định.

Ví dụ về các chủ đề chính sách này bao gồm:

- a) kiểm soát truy cập (xem điều 9);
- b) phân loại thông tin (và xử lý) (xem 8.2);
- c) an toàn vật lý và môi trường (xem điều 11);
- d) các chủ đề định hướng người dùng cuối như:
 - 1) sử dụng hợp lý tài sản (xem 8.1.3);
 - 2) bàn và màn hình sạch (xem 11.2.9);
 - 3) truyền tải thông tin (xem 13.2.1);
 - 4) các thiết bị di động và làm việc từ xa (xem 6.2);
 - 5) hạn chế về các bộ cài đặt phần mềm và sử dụng (xem 12.6.2);

- e) sao lưu (xem 12.3);
- f) truyền tải thông tin (xem 13.2);
- g) bảo vệ khỏi phần mềm độc hại (xem 12.2);
- h) quản lý các lỗ hổng kỹ thuật (xem 12.6.1);
- i) kiểm soát mật mã (xem điều 10);
- j) an toàn truyền thông (xem điều 13);
- k) bảo mật riêng tư và bảo vệ thông tin cá nhân (xem 18.1.4);
- l) các quan hệ với nhà cung cấp (xem điều 15).

Các chính sách nêu trên phải được phổ biến cho nhân viên và các bên liên quan ngoài tổ chức theo một hình thức có liên quan, dễ tiếp cận và dễ hiểu đối với người đọc mong muốn, ví dụ như trong ngữ cảnh của một "chương trình giáo dục, đào tạo và nâng cao nhận thức an toàn thông tin" (xem 7.2.2).

Thông tin khác

Cần thiết có các chính sách nội bộ về an toàn thông tin khác nhau giữa các tổ chức. Chính sách nội bộ đặc biệt hữu ích trong các tổ chức lớn và phức tạp, nơi những người xác định và phê duyệt mức độ kiểm soát tách biệt với những người thực hiện các kiểm soát hoặc trong các tình huống nơi mà một chính sách áp dụng cho nhiều người khác nhau hoặc các bộ phận chức năng khác nhau trong tổ chức. Chính sách an toàn thông tin có thể được ban hành dưới dạng tài liệu đơn "chính sách an toàn thông tin" hoặc tập hợp các tài liệu riêng rẽ nhưng có liên quan với nhau.

Nếu chính sách an toàn thông tin được phổ biến ra ngoài phạm vi của tổ chức thì cần lưu ý không tiết lộ những thông tin có tính chất nhạy cảm.

Một số tổ chức sử dụng các thuật ngữ khác cho các văn bản chính sách này, chẳng hạn như "Tiêu chuẩn", "Chỉ thị" hoặc "Nội quy".

5.1.2 Soát xét chính sách an toàn thông tin

Kiểm soát

Chính sách an toàn thông tin cần thường xuyên được soát xét theo kế hoạch hoặc khi có những thay đổi lớn xuất hiện để luôn đảm bảo sự phù hợp, đầy đủ và thực sự có hiệu lực.

Hướng dẫn thi hành

Cần có một người chịu trách nhiệm trong việc phát triển, soát xét, và đánh giá chính sách an toàn thông tin. Quá trình soát xét cần đánh giá các cơ hội cải tiến chính sách an toàn thông tin của tổ chức và phương thức quản lý chính sách an toàn nhằm đáp ứng với những thay đổi của môi trường tổ chức, các tình huống nghiệp vụ, các điều kiện pháp lý, hoặc môi trường kỹ thuật.

Việc soát xét chính sách an toàn thông tin cần quan tâm đến các kết quả của việc soát xét về quản lý.

Cần có được sự thông qua của cấp quản lý cho một chính sách sửa đổi.

6 Tổ chức đảm bảo an toàn thông tin

6.1 Tổ chức nội bộ

Mục tiêu: Nhằm thiết lập một khung quản lý để khởi động và kiểm soát việc thực hiện và vận hành an toàn thông tin trong tổ chức.

6.1.1 Vai trò và trách nhiệm đảm bảo an toàn thông tin

Kiểm soát

Tất cả các trách nhiệm đảm bảo an toàn thông tin cần được xác định một cách rõ ràng.

Hướng dẫn thi hành

Việc phân bổ các trách nhiệm về an toàn thông tin cần phù hợp với chính sách an toàn thông tin (xem 5.1.1). Các trách nhiệm về bảo vệ tài sản cá nhân và thực hiện các quy trình an toàn cụ thể cần được xác định rõ ràng. Nếu cần thiết thì trách nhiệm này cần được bổ sung bằng hướng dẫn chi tiết hơn về các vị trí công việc cụ thể và các phương tiện xử lý thông tin. Các trách nhiệm trong nội bộ về bảo vệ tài sản và thực hiện các quy trình an toàn đặc biệt, ví dụ lập kế hoạch đảm bảo tính liên tục về nghiệp vụ, cũng cần được xác định rõ.

Những cá nhân đã được phân bổ trách nhiệm về an toàn thông tin có thể ủy quyền các nhiệm vụ an toàn cho những người khác thực hiện. Tuy nhiên, họ vẫn phải duy trì trách nhiệm và đảm bảo rằng các nhiệm vụ đã được ủy quyền đều được thực hiện đúng cách thức.

Phạm vi trách nhiệm của các cá nhân có trách nhiệm cần được quy định rõ ràng. Cần quan tâm đến các vấn đề sau:

- a) các tài sản và các quy trình an toàn đối với từng hệ thống cụ thể cần được xác định và định danh rõ ràng;
- b) các thực thể chịu trách nhiệm cho mỗi quy trình an toàn tài sản và thông tin cần được phân công và cần ghi chép lại trách nhiệm một cách chi tiết;
- c) các mức cấp phép cần được xác định rõ và lập tài liệu;
- d) để có thể thực hiện đầy đủ trách nhiệm trong lĩnh vực an toàn thông tin, các cá nhân cần có năng lực trong lĩnh vực này và được cập nhật sự phát triển.
- e) cần xác định và ghi chép lại việc điều phối và giám sát các khía cạnh an toàn các mối quan hệ với nhà cung cấp.

Thông tin khác

Trong nhiều tổ chức, một người quản lý an toàn thông tin sẽ được bổ nhiệm nhằm thực hiện trách nhiệm chung trong việc phát triển, triển khai công tác an toàn và hỗ trợ việc tìm ra các biện pháp kiểm soát phù hợp.

Tuy nhiên, trách nhiệm trong việc tìm ra và triển khai các biện pháp kiểm soát sẽ thường thuộc về những người quản lý cụ thể. Một thực tế thường thấy là phải chỉ định ra người sở hữu đối với từng tài sản, người này có trách nhiệm đối với việc bảo vệ tài sản hàng ngày.

6.1.2 Phân tách nhiệm vụ

Kiểm soát

Các nhiệm vụ và phạm vi trách nhiệm có xung đột cần được tách biệt để giảm thiểu khả năng sửa đổi trái phép hoặc vô tình hoặc lạm dụng tài sản của tổ chức.

Hướng dẫn thi hành

Cần theo dõi chặt chẽ nhằm đảm bảo không một cá nhân nào có thể truy cập, chỉnh sửa hoặc sử dụng tài sản khi chưa được phép hoặc không bị phát hiện. Việc khởi tạo một sự kiện cần được tách ra khỏi quá trình cấp phép cho sự kiện đó. Khả năng câu kết giữa các cá nhân cũng cần được quan tâm trong khi thiết kế các biện pháp kiểm soát.

Các tổ chức có quy mô nhỏ có thể sẽ gặp khó khăn trong việc phân tách nhiệm vụ, nhưng cần áp dụng nguyên tắc này đến mức có thể và khả thi. Bất cứ khi nào gặp khó khăn trong việc phân tách nhiệm vụ thì cần quan tâm đến các biện pháp khác như giám sát các hoạt động, truy vết kiểm toán và giám sát quản lý.

Thông tin khác

Phân tách nhiệm vụ là một phương thức làm giảm nguy cơ lạm dụng vô tình hay cố tình tài sản của một tổ chức.

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

Kiểm soát

Phải duy trì liên lạc thỏa đáng với những cơ quan có thẩm quyền liên quan.

Hướng dẫn thi hành

Các tổ chức cần có các thủ tục xác định khi nào và ai có thẩm quyền (ví dụ, cơ quan thi hành luật, cơ quan quản lý, những người có thẩm quyền giám sát), và phương thức thông báo các sự cố an toàn thông tin xác định một cách kịp thời nếu có nghi ngờ đã có sự vi phạm luật.

Thông tin khác

Các tổ chức bị tấn công từ Internet có thể cần tiến hành các hoạt động chống lại nguồn gốc tấn công.

Sự duy trì những mối liên hệ như vậy có thể là một yêu cầu giúp hỗ trợ quản lý các sự cố an toàn thông tin ([xem điều 16](#)) hoặc quá trình lập kế hoạch nghiệp vụ đột xuất và liên tục ([xem điều 17](#)). Các mối liên hệ với các cơ quan quản lý cũng sẽ có lợi cho công tác dự báo và chuẩn bị cho những thay đổi sắp xảy ra trên phương diện luật pháp hoặc các quy định bắt buộc tổ chức phải tuân theo. Những liên hệ với những người có thẩm quyền bao gồm các dịch vụ khẩn cấp, tiện ích, điện, phòng cháy chữa cháy (có liên quan đến tính liên tục về nghiệp vụ), các nhà cung cấp dịch vụ viễn thông (có liên quan đến độ sẵn sàng), công ty cung cấp nước (có liên hệ với các công cụ làm mát cho thiết bị).

6.1.4 Liên lạc với các nhóm chuyên gia

Kiểm soát

Phải giữ liên lạc với các nhóm chuyên gia hoặc các diễn đàn và hiệp hội an toàn thông tin.

Hướng dẫn thi hành

Cần coi các thành viên trong các diễn đàn hoặc các nhóm có quan tâm đặc biệt như phương tiện nhằm:

- a) nâng cao kiến thức về thực tế tốt nhất và cập nhật những thông tin có liên quan về an toàn;
- b) đảm bảo rằng kiến thức về môi trường an toàn thông tin là đầy đủ và được phổ biến;
- c) nhận được các cảnh báo sớm từ các cảnh báo, những lời tư vấn, và các bản vá liên quan đến những tấn công và những lỗ hổng;
- d) tiếp cận đến những lời khuyên có tính chất chuyên gia về an toàn thông tin;
- e) chia sẻ và trao đổi thông tin về các công nghệ, sản phẩm, những mối đe dọa hoặc những lỗ hổng mới;
- f) cung cấp những mối liên hệ phù hợp khi giải quyết các sự cố về an toàn thông tin ([xem 16](#)).

Thông tin khác

Có thể thiết lập những thỏa thuận về chia sẻ thông tin nhằm nâng cao sự phối hợp và cộng tác về các vấn đề an toàn. Những thỏa thuận như vậy cần xác định các yêu cầu về việc bảo vệ thông tin bí mật.

6.1.5 An toàn thông tin trong quản lý dự án

Kiểm soát

Trong quản lý dự án cần đề cập đến an toàn thông tin, với bất cứ loại dự án nào.

Hướng dẫn thi hành

An toàn thông tin cần được tích hợp vào phương thức quản lý dự án của tổ chức để đảm bảo rằng độ rủi ro an toàn thông tin được xác định và giải quyết như là một phần của dự án. Từng dự án có những

đặc điểm riêng nhưng nhìn chung điều này áp dụng cho hầu hết các dự án, ví dụ cốt lõi của một dự án là quá trình kinh doanh, công nghệ thông tin, quản lý cơ sở và các quy trình hỗ trợ khác. Phương thức quản lý dự án sử dụng cần quan tâm đến các yêu cầu sau:

- a) các đối tượng cần đảm bảo an toàn thông tin bao gồm các đối tượng trong dự án;
- b) cần tiến hành đánh giá rủi ro an toàn thông tin ở giai đoạn đầu của dự án để xác định kiểm soát cần thiết;
- c) các phương thức áp dụng trong dự án cần được an toàn thông tin trong tất cả các giai đoạn.

Vấn đề an toàn thông tin cần được soát xét và giải quyết thường xuyên trong tất cả các dự án. Vai trò, trách nhiệm đối với an toàn thông tin cần phải được xác định và phân bổ trong các phương thức quản lý dự án.

6.2 Thiết bị di động và làm việc từ xa

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

6.2.1 Chính sách sử dụng thiết bị di động

Kiểm soát

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

Hướng dẫn thi hành

Khi sử dụng thiết bị di động, cần thực hiện sự quan tâm đặc biệt để đảm bảo thông tin kinh doanh không bị tổn hại. Chính sách về thiết bị di động cần quan tâm đến những rủi ro do làm việc với di động trong những môi trường không được bảo vệ.

Các chính sách thiết bị di động cần quan tâm:

- a) các thiết bị di động cần phải được đăng ký;
- b) yêu cầu bảo vệ mức vật lý;
- c) hạn chế các phần mềm cài đặt;
- d) yêu cầu bảo vệ với các phiên bản phần mềm của thiết bị di động và áp dụng cho các bản vá lỗi;
- e) hạn chế kết nối với các dịch vụ thông tin;
- f) kiểm soát truy cập;
- g) các kỹ thuật mật mã;
- h) bảo vệ trước mã độc;
- i) vô hiệu hóa từ xa, xóa hoặc khóa máy;

- j) sao lưu;
- k) sử dụng các dịch vụ web và ứng dụng web.

Cũng cần quan tâm khi sử dụng các thiết bị di động ở những nơi công cộng, phòng họp và các khu vực không được bảo vệ khác. Việc bảo vệ cần phù hợp để tránh truy nhập trái phép tới hoặc tiết lộ thông tin được lưu trữ và được xử lý bởi các thiết bị này, ví dụ sử dụng kỹ thuật mật mã (xem 10) và thực thi sử dụng các thông tin xác thực bí mật (xem 9.2.4).

Các thiết bị di động cũng phải được bảo vệ vật lý chống lại trộm cắp đặc biệt khi được để, ví dụ, trong ô tô hoặc các phương tiện vận tải khác, phòng khách sạn, trung tâm hội nghị, và các nơi hội họp. Một thủ tục cụ thể về các yêu cầu pháp lý, bảo hiểm và các yêu cầu an toàn khác của tổ chức cần được thiết lập đối với những trường hợp bị mất cắp hoặc làm mất thiết bị tính toán di động. Thiết bị mang thông tin nghiệp vụ quan trọng, nhạy cảm hoặc trọng yếu không được để tự do, và nếu có thể phải được để ở nơi có khóa, hoặc sử dụng các loại khóa đặc biệt để bảo vệ thiết bị.

Cần thu xếp đào tạo các nhân viên sử dụng tính toán di động để làm tăng nhận thức của họ về những rủi ro của cách làm việc này và triển khai các biện pháp kiểm soát.

Trong trường hợp các chính sách thiết bị cho phép việc sử dụng các thiết bị di động cá nhân, cần soát xét các chính sách có liên quan và biện pháp an toàn:

- a) thiết bị của cá nhân và doanh nghiệp cần tách bạch, bao gồm việc sử dụng phần mềm để hỗ trợ cách ly và bảo vệ dữ liệu doanh nghiệp trên thiết bị riêng;
- b) quyền truy cập vào thông tin doanh nghiệp được cung cấp chỉ sau khi người dùng đã ký một thỏa thuận cuối cùng thừa nhận trách nhiệm của mình (bảo vệ vật lý, cập nhật phần mềm,...) bao gồm quyền sở hữu dữ liệu kinh doanh, cho phép xóa dữ liệu từ xa của các tổ chức trong trường hợp bị mất cắp thiết bị hoặc khi không còn được phép sử dụng dịch vụ. Cần có luật riêng cho các chính sách này.

Thông tin khác

Các kết nối không dây của thiết bị di động cũng tương tự như các dạng kết nối mạng khác, nhưng có các điểm khác biệt quan trọng cần được lưu ý khi xác định các biện pháp kiểm soát. Các điểm khác biệt gồm:

- a) một số giao thức an toàn trong mạng không dây vẫn chưa chín muồi và được coi là các lỗ hổng;
- b) thông tin lưu trữ trên các thiết bị di động có thể không được sao lưu do băng tần mạng hạn chế và/hoặc do các thiết bị di động có thể không được kết nối tại các những thời điểm đã được lập lịch để thực hiện sao lưu.

Các thiết bị di động thường chia sẻ các chức năng phổ biến, ví dụ như mạng, truy cập mạng, thư điện tử và xử lý tập tin, với các thiết bị sử dụng cố định. Kiểm soát an toàn thông tin cho các thiết bị di động thông thường bao gồm những người đã được thông qua sử dụng các thiết bị cố định và giải quyết những mối đe dọa lớn như sử dụng chúng ngoài phạm vi của tổ chức.

6.2.2 Làm việc từ xa

Kiểm soát

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

Hướng dẫn thi hành

Các tổ chức khi hoạt động bên ngoài cần ban hành một chính sách xác định các điều kiện cũng như giới hạn sử dụng từ xa. Nơi được áp dụng và cho phép bởi luật pháp, cần quan tâm đến các vấn đề sau:

- a) sự an toàn mức vật lý hiện tại của vị trí làm việc từ xa, trong đó cần lưu ý đến sự an toàn vật lý của các tòa nhà và môi trường bên trong;
- b) yêu cầu về đảm bảo an toàn vật lý khi cho môi trường làm việc từ xa;
- c) các yêu cầu an toàn truyền thông, trong đó cần lưu ý nhu cầu truy cập từ xa tới các hệ thống bên trong tổ chức, thông tin nhạy cảm sẽ được truy cập và đi qua liên kết truyền thông và sự nhạy cảm của hệ thống bên trong;
- d) việc truy cập máy tính ảo có thể ngăn chặn xử lý thông tin và lưu trữ thông tin trên thiết bị cá nhân;
- e) mối đe dọa từ việc truy cập trái phép tới thông tin hoặc các nguồn tài nguyên từ những người sống cùng khác, ví dụ gia đình và bạn bè;
- f) việc sử dụng các mạng gia đình, các yêu cầu hoặc các hạn chế đối với việc cấu hình các dịch vụ mạng không dây;
- g) các chính sách và thủ tục phòng ngừa tranh chấp liên quan đến các quyền sở hữu trí tuệ được phát triển trên thiết bị thuộc sở hữu cá nhân;
- h) truy nhập tới thiết bị thuộc sở hữu cá nhân (để kiểm tra sự an toàn của thiết bị hoặc khi điều tra), loại truy cập này có thể được ngăn chặn bằng quy định pháp lý;
- i) những thỏa thuận đăng ký bản quyền phần mềm quy định trách nhiệm pháp lý của tổ chức trong việc đăng ký bản quyền phần mềm khách trên các máy trạm thuộc sở hữu của các nhân viên, người của các nhà thầu hoặc bên thứ ba;
- j) các yêu cầu bảo vệ chống mã độc và tường lửa.

Các hướng dẫn và bố trí sau cần được quan tâm:

- a) cung cấp trang bị lưu trữ và thiết bị phù hợp cho các hoạt động làm việc từ xa nếu việc sử dụng thiết bị thuộc sở hữu cá nhân không chịu sự quản lý của tổ chức là không được phép;
- b) xác định công việc được phép, giờ làm việc, phân loại thông tin có thể được lấy, và các hệ thống bên trong và dịch vụ mà người làm việc từ xa được phép truy cập;
- c) cung cấp thiết bị truyền thông phù hợp, gồm các phương pháp đảm bảo an toàn cho việc truy cập từ xa;
- d) đảm bảo an toàn mức vật lý;
- e) các quy tắc và hướng dẫn cho gia đình và khách truy cập tới thiết bị và thông tin;
- f) cung cấp hỗ trợ và bảo trì phần cứng và phần mềm;
- g) cung cấp các hợp đồng bảo hiểm;
- h) các thủ tục sao lưu và đảm bảo sự liên tục của hoạt động nghiệp vụ;
- i) kiểm toán và giám sát an toàn;
- j) thu hồi các cấp phép và quyền truy cập, và hoàn trả thiết bị khi chấm dứt các hoạt động làm việc từ xa.

Thông tin khác

Làm việc từ xa đề cập đến tất cả các hình thức làm việc bên ngoài văn phòng, bao gồm cả môi trường làm việc phi truyền thống, chẳng hạn những người "làm việc tại nhà", "địa điểm làm việc linh hoạt", môi trường "làm việc từ xa" và "làm việc ảo hóa".

7 An toàn nguồn nhân lực

7.1 Trước khi tuyển dụng

Mục tiêu: Đảm bảo rằng các nhân viên, người của nhà thầu hiểu rõ trách nhiệm của mình và phù hợp với vai trò người đó được giao.

7.1.1 Thăm tra

Kiểm soát

Việc xác minh lai lịch của mọi ứng viên tuyển dụng phải được thực hiện phù hợp với pháp luật, quy định, đạo đức và phù hợp với các yêu cầu của công việc, phân loại thông tin được truy nhập và các rủi ro có thể nhận thấy được.

Hướng dẫn thi hành

Việc xác minh cần quan tâm đến tính riêng tư, việc bảo vệ dữ liệu cá nhân và thông tin tuyển dụng dựa trên luật sử dụng lao động, và nếu được phép cần bao gồm những vấn đề sau:

- a) tính sẵn có của các giấy tờ chứng minh danh tính, ví dụ công việc và cá nhân;
- b) kiểm tra (tính đầy đủ và chính xác) hồ sơ của ứng viên;
- c) xác nhận về các văn bằng nghề nghiệp và học thuật đã khai;
- d) kiểm tra giấy tờ tùy thân (chứng minh thư, căn cước, công dân, hộ chiếu);
- e) các kiểm tra chi tiết hơn, ví dụ các kiểm tra về tài chính hoặc các kiểm tra về lý lịch tư pháp;

Khi một cá nhân được tuyển dụng một vị trí đặc thù cho an toàn thông tin, tổ chức cần đảm bảo chắc chắn về ứng viên:

- a) có năng lực cần thiết để thực hiện vị trí an toàn thông tin được giao;
- b) đảm bảo tính tin cậy để đảm nhiệm vị trí, đặc biệt là nếu vị trí đó rất quan trọng đối với tổ chức.

Với các công việc, cho dù là được chỉ định từ đầu hoặc do thăng tiến, có sự truy cập của cá nhân tới các phương tiện xử lý thông tin, đặc biệt là nếu các thiết bị này đang xử lý thông tin nhạy cảm, ví dụ thông tin tài chính hoặc thông tin có độ an toàn cao, thì tổ chức cũng cần soát xét thực hiện các cuộc kiểm tra chi tiết hơn.

Các thủ tục cần xác định chỉ tiêu và các giới hạn đối với các cuộc kiểm tra xác minh, ví dụ người có đủ tư cách kiểm tra, và cách thức, thời gian và lý do thực hiện các cuộc kiểm tra xác minh.

Quá trình kiểm tra cũng cần được thực hiện với các nhà thầu. Trong những trường hợp này, các thỏa thuận giữa tổ chức và các nhà thầu cần xác định rõ trách nhiệm trong việc kiểm tra và các thủ tục khai báo mà họ cần tuân thủ nếu việc kiểm tra không hoàn tất hoặc nếu các kết quả kiểm tra gây ra hổn loạn hoặc lo ngại.

Thông tin của tất cả các ứng viên đang được cân nhắc cho các vị trí tuyển dụng trong tổ chức cũng cần được thu thập và xử lý theo pháp luật hiện hành với phạm vi quyền hạn tương ứng. Tùy theo quy định của luật pháp phù hợp mà các ứng viên cần phải được thông báo trước về các hoạt động kiểm tra này.

7.1.2 Điều khoản và điều kiện tuyển dụng

Kiểm soát

Các thỏa thuận hợp đồng với nhân viên và nhà thầu cần nêu rõ trách nhiệm của họ và tổ chức đối với an toàn thông tin.

Hướng dẫn thi hành

Các nghĩa vụ hợp đồng cho nhân viên hay nhà thầu phải phản ánh chính sách của tổ chức đối với an toàn thông tin, thêm vào việc cần làm và nêu rõ:

- a) tất cả các nhân viên, người của nhà thầu - những người được phép truy cập đến thông tin nhạy cảm, cần ký vào một thỏa thuận an toàn hoặc không tiết lộ trước khi được cấp phép truy cập đến các phương tiện xử lý thông tin (xem 13.2.4);
- b) các quyền và trách nhiệm pháp lý của các nhân viên, người của các nhà thầu và những người dùng khác, ví dụ các quyền và trách nhiệm liên quan đến luật bản quyền hoặc pháp luật về bảo vệ dữ liệu (xem 18.1.2 và 18.1.4);
- c) các trách nhiệm đối với việc phân loại thông tin và quản lý thông tin thuộc tổ chức, các tài sản khác liên quan đến thông tin, các thiết bị xử lý thông tin và các dịch vụ thông tin được xử lý bởi nhân viên hoặc người của nhà thầu (xem điều 8);
- d) các trách nhiệm của nhân viên, người của nhà thầu trong việc xử lý thông tin nhận được từ các công ty khác hoặc các tổ chức bên ngoài;
- e) các hoạt động sẽ được thực thi nếu nhân viên, người của nhà thầu hoặc bên thứ ba thiếu quan tâm đến các yêu cầu về an toàn của tổ chức (xem 7.2.3).

Vai trò an toàn thông tin và trách nhiệm cần được thông báo tới các ứng viên trong quá trình trước khi làm việc.

Tổ chức cần đảm bảo rằng các nhân viên, người của nhà thầu đồng ý các điều khoản và điều kiện liên quan đến an toàn thông tin phù hợp với bản chất và phạm vi truy cập mà họ sẽ thực hiện tới các tài sản của tổ chức liên quan đến các dịch vụ và hệ thống thông tin.

Nếu thích hợp thì các trách nhiệm nằm trong các điều khoản và điều kiện sử dụng lao động cần được tiếp tục duy trì trong thời gian xác định sau khi đã chấm dứt sử dụng lao động (xem 7.3).

Thông tin khác

Một quy tắc ứng xử có thể được sử dụng để nêu trách nhiệm an toàn thông tin của nhân viên hoặc nhà thầu liên quan đến an toàn, bảo vệ dữ liệu, đạo đức, việc sử dụng thiết bị và cơ sở vật chất của tổ chức, cũng như hoạt động có trách nhiệm được chờ đợi bởi tổ chức. Một bên tham gia bên ngoài, với một nhà thầu có liên quan, có thể được yêu cầu nhập vào các thỏa thuận trong hợp đồng đại diện cho các cá nhân ký hợp đồng.

7.2 Trong thời gian làm việc

Mục tiêu: Đảm bảo nhân viên và nhà thầu nhận thức và thực hiện đầy đủ trách nhiệm an toàn thông tin của họ.

7.2.1 Trách nhiệm của ban lãnh đạo

Kiểm soát

Ban lãnh đạo cần yêu cầu các nhân viên, người của nhà thầu và bên thứ ba chấp hành an toàn thông tin phù hợp với các chính sách và các thủ tục an toàn thông tin đã được thiết lập của tổ chức.

Hướng dẫn thi hành

Ban lãnh đạo cần có trách nhiệm đảm bảo rằng các nhân viên, người của nhà thầu:

- a) được chỉ dẫn thích hợp về các trách nhiệm và vai trò của họ đối với an toàn thông tin trước khi được chấp nhận truy cập thông tin hoặc các hệ thống thông tin nhạy cảm;
- b) được cung cấp các hướng dẫn phù hợp vai trò về an toàn thông tin của họ trong tổ chức;
- c) được thúc đẩy thực hiện các chính sách an toàn của tổ chức;
- d) đạt được một mức độ hiểu biết về an toàn thông tin tương xứng với các vai trò và trách nhiệm của họ trong tổ chức (xem 7.2.2);
- e) tuân theo các điều khoản và điều kiện tuyển dụng, bao gồm chính sách an toàn thông tin của tổ chức và các phương pháp làm việc phù hợp;
- f) tiếp tục đạt được các kỹ năng và chứng chỉ phù hợp và được đào tạo thường xuyên;
- g) được cung cấp kênh báo cáo mà không cần cung cấp danh tính để báo cáo những vi phạm trong chính sách và thủ tục an toàn thông tin ("hệ thống cung cấp thông tin nội bộ").

Ban lãnh đạo cần hỗ trợ giải thích các chính sách, thủ tục và biện pháp kiểm soát an toàn thông tin, và thực hiện trước tiên để làm hình mẫu.

Thông tin khác

Nếu các nhân viên, người của nhà thầu và bên thứ ba không nhận thức được các trách nhiệm an toàn thông tin của họ thì họ có thể gây ra những thiệt hại đáng kể cho tổ chức. Các cá nhân được đào tạo sẽ có xu hướng đáng tin cậy hơn và ít gây ra những sự cố về an toàn thông tin hơn.

Quản lý kém cũng có thể làm cho nhân viên coi thường và dẫn đến kết quả là làm ảnh hưởng xấu đến công tác an toàn thông tin của tổ chức. Ví dụ, việc quản lý kém có thể dẫn đến công tác an toàn thông tin bị xao nhãng hoặc tiềm ẩn sự sử dụng sai các tài sản của tổ chức.

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

Kiểm soát

Tất cả các nhân viên trong tổ chức và, nếu liên quan, cả người của nhà thầu và bên thứ ba cần phải được giáo dục và đào tạo nhận thức thích hợp và cập nhật thường xuyên những chính sách, thủ tục an toàn thông tin của tổ chức như một phần công việc bắt buộc.

Hướng dẫn thi hành

Chương trình nhận thức an toàn thông tin cần hướng đến mục tiêu làm cho các nhân viên và lao động hợp đồng nhận thức được trách nhiệm của họ trong việc đảm bảo an toàn cho thông tin và những phương tiện để hoàn thành nhiệm vụ.

Chương trình nhận thức an toàn thông tin cần được thiết lập thống nhất với các chính sách và thủ tục an toàn thông tin của tổ chức, có xét đến những thông tin của tổ chức cần được bảo vệ và những biện pháp kiểm soát được tiến hành để bảo vệ thông tin. Chương trình nhận thức an toàn thông tin cần lồng ghép những hoạt động nâng cao nhận thức chẳng hạn như các đợt vận động (ví dụ như "ngày an toàn thông tin") và phát hành các sổ tay hoặc bản tin.

Chương trình nhận thức cần được lên kế hoạch có xét đến vai trò của nhân viên trong tổ chức và cả lao động hợp đồng. Các hoạt động trong chương trình nhận thức cần được lên kế hoạch theo thời gian, mang tính thường xuyên, để các hoạt động lặp lại và tiếp cận được với những nhân viên và lao động hợp đồng mới. Chương trình nhận thức cần được cập nhật thường xuyên để đồng bộ với các chính sách và thủ tục của tổ chức và cần được xây dựng dưới dạng những bài học rút ra từ các sự cố an toàn thông tin.

Đào tạo nhận thức cần được thực hiện theo yêu cầu trong chương trình nhận thức an toàn thông tin của tổ chức. Đào tạo nhận thức có thể tiến hành theo nhiều hình thức khác nhau chẳng hạn như thông qua lớp học, đào tạo từ xa, qua mạng, tự học và các hình thức khác.

Giáo dục và đào tạo an toàn thông tin cũng cần đề cập đến những khía cạnh tổng quát chẳng hạn như:

- a) nêu rõ cam kết của ban lãnh đạo về an toàn thông tin rộng rãi trong tổ chức;
- b) sự cần thiết phải nắm vững và tuân thủ các quy tắc và nghĩa vụ an toàn thông tin hiện đang được áp dụng, như xác định trong các chính sách, tiêu chuẩn, luật pháp, quy định, các hợp đồng và thỏa thuận;
- c) trách nhiệm cá nhân về những gì nên làm và không nên làm, trách nhiệm chung hướng đến an toàn hoặc bảo vệ thông tin của tổ chức và các đối tác bên ngoài;
- d) các thủ tục an toàn thông tin cơ bản (chẳng hạn như báo cáo sự cố an toàn thông tin) và các biện pháp kiểm soát cơ bản (chẳng hạn như cài đặt mật khẩu, kiểm soát phần mềm độc hại và bàn làm việc sạch);
- e) các đầu mối liên lạc và các nguồn tham khảo thông tin, tư vấn về các vấn đề an toàn thông tin bao gồm giáo dục an toàn thông tin và các tài liệu đào tạo.

Giáo dục và đào tạo an toàn thông tin cần thực hiện định kỳ. Giáo dục và đào tạo ban đầu cho những người chuyển sang vị trí hoặc vai trò mới với các yêu cầu an toàn thông tin thay đổi nhiều, không chỉ dành cho những người mới bắt đầu và cần tiến hành trước khi họ đảm nhận vai trò mới của mình.

Tổ chức cần xây dựng chương trình giáo dục và đào tạo để tiến hành hoạt động này có hiệu quả. Chương trình phải phù hợp với chính sách và thủ tục an toàn thông tin của tổ chức, có xét đến những thông tin cần được bảo vệ và những biện pháp cần tiến hành để bảo vệ thông tin. Chương trình cần đưa ra các phương thức giáo dục và đào tạo khác nhau, chẳng hạn như bằng bài giảng hoặc bằng tự học.

Thông tin khác

Khi soạn một chương trình nhận thức, chúng ta không chỉ tập trung vào "what" (những gì cần làm) và "how" (cách làm), mà cần phải tập trung vào "why" (lý do tại sao phải làm như vậy). Các nhân viên cần phải hiểu mục tiêu an toàn thông tin và những tác động tiềm ẩn, tích cực và tiêu cực từ những hành động cá nhân của họ đối với tổ chức.

Nhận thức, giáo dục và đào tạo có thể tiến hành riêng hoặc phối hợp với các hoạt động đào tạo khác chẳng hạn như đào tạo công nghệ thông tin tổng quát hoặc đào tạo an toàn thông tin tổng quát.

Các hoạt động đào tạo, giáo dục và nhận thức về an toàn cần phù hợp và liên quan đến vai trò, các trách nhiệm và kỹ năng của từng cá nhân. Có thể tiến hành kiểm tra kiến thức của nhân viên ở cuối khóa đào tạo để đánh giá khả năng tiếp nhận thông tin.

7.2.3 Xử lý kỷ luật

Kiểm soát

Cần có một quy trình xử lý kỷ luật chính thức đối với những người có hành vi vi phạm an toàn thông tin đã cam kết.

Hướng dẫn thi hành

Quy trình xử lý kỷ luật không nên thực hiện mà không xác minh trước về sự vi phạm an toàn thông tin đã xảy ra ([xem 16.1.7](#))

Quy trình kỷ luật chính thức cần đảm bảo xử lý công bằng và đúng đắn đối với các nhân viên bị nghi ngờ có hành vi vi phạm an toàn. Quy trình kỷ luật chính thức cần đưa ra đáp ứng từng bước trong đó quan tâm đến các yếu tố như bản chất và tính nghiêm trọng của vi phạm và ảnh hưởng nghiệp vụ của nó, xem xét xem đây là vi phạm lần đầu hay lặp lại, xem xét xem người vi phạm đã được đào tạo phù hợp chưa, các vấn đề pháp lý liên quan, các hợp đồng nghiệp vụ và các yếu tố khác nếu cần.

Thông tin khác

Quy trình xử lý kỷ luật cũng có thể trở thành một động lực hay một sự khích lệ nếu biện pháp xử phạt tích cực được xác định cho những hành vi đáng chú ý liên quan tới an toàn thông tin.

7.3 Chấm dứt hoặc thay đổi công việc

Mục tiêu: Sự thay đổi hoặc chấm dứt công việc như là một phần quá trình bảo vệ lợi ích của tổ chức.

7.3.1 Trách nhiệm kết thúc hoặc thay đổi hợp đồng

Kiểm soát

Trách nhiệm an toàn thông tin và những nghĩa vụ vẫn có hiệu lực sau khi đã thay đổi hoặc chấm dứt hợp đồng cần phải được xác định, thông báo cho các nhân viên hoặc nhà thầu và thi hành.

Thông tin khác

Các trách nhiệm về chấm dứt sử dụng lao động cần bao gồm các yêu cầu tiếp theo về an toàn, các trách nhiệm pháp lý và, nếu thích hợp, cả các trách nhiệm đã được ghi trong thỏa thuận an toàn bất kỳ (xem 13.2.4), và các điều khoản và điều kiện về tuyển dụng (xem 7.1.2) được duy trì trong một thời gian xác định sau khi chấm dứt sử dụng lao động của nhân viên.

Các trách nhiệm và nhiệm vụ vẫn còn hiệu lực sau khi chấm dứt sử dụng lao động cần được ghi vào các bản hợp đồng của các nhân viên, người của nhà thầu và điều kiện lao động (xem 7.1.2).

Những thay đổi về trách nhiệm hoặc việc sử dụng lao động cần được quản lý khi chấm dứt trách nhiệm hoặc việc sử dụng lao động tương ứng kết hợp với việc triển khai các trách nhiệm hoặc công việc mới.

Thông tin khác

Phòng tổ chức nhân sự phải chịu trách nhiệm chung đối với các công việc và toàn bộ quy trình chấm dứt cùng với người quản lý của người chấm dứt lao động nhằm quản lý được các vấn đề về an toàn của các thủ tục liên quan. Trong trường hợp với bản hợp đồng thì quy trình chấm dứt trách nhiệm có thể được thực thi khẩn cấp đối với nhà thầu, trong các trường hợp với người dùng khác thì có thể được xử lý bởi tổ chức của họ.

Cũng cần thông báo cho các nhân viên, người của nhà thầu và bên thứ ba về những thay đổi và việc sắp xếp công việc mới.

8 Quản lý tài sản

8.1 Trách nhiệm đối với tài sản

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

8.1.1 Kiểm kê tài sản

Kiểm soát

Thông tin, các loại tài sản khác gắn liền với thông tin và các thiết bị xử lý thông tin cần được xác định và một bản kiểm kê những tài sản này phải được xây dựng và duy trì.

Thông tin khác

Tổ chức cần xác định các tài sản có thông tin liên quan trong vòng đời và tầm quan trọng tài liệu của họ. Vòng đời của thông tin bao gồm việc tạo, xử lý, lưu trữ, truyền tải, xóa và phá hủy. Tài liệu cần được duy trì trong chỗ lưu trữ chuyên dụng hoặc chỗ hiện có cho phù hợp.

Việc kiểm kê tài sản phải chính xác, luôn cập nhật, nhất quán và phù hợp với các nơi lưu trữ khác.

Đối với mỗi tài sản được định danh, quyền sở hữu tài sản phải được chỉ định ([xem 8.1.2](#)) và việc phân loại cần phải được định danh ([xem 8.2](#)).

Thông tin khác

Các biện bản kiểm kê tài sản giúp đảm bảo rằng việc bảo vệ tài sản một cách hiệu quả đã được thực hiện, và có thể được yêu cầu cho các mục đích nghiệp vụ khác, như các lý do về sức khỏe và an toàn, bảo hiểm hoặc tài chính (quản lý tài sản).

ISO/IEC 27005^[11] cung cấp các ví dụ về tài sản mà cần được xem xét bởi các tổ chức khi định danh tài sản. Quá trình biên soạn kiểm kê tài sản là một điều kiện quan trọng tiên quyết của quản lý rủi ro ([xem thêm TCVN 11238 \(ISO/IEC 27000\) và ISO/IEC 27005^{\[11\]}](#)).

8.1.2 Quyền sở hữu tài sản thông tin

Kiểm soát

Tài sản được duy trì trong bảng kiểm kê cần phải có chủ sở hữu.

Hướng dẫn thi hành

Cá nhân cũng như tổ chức được phê duyệt trách nhiệm quản lý tài sản đủ điều kiện để xác định là chủ sở hữu tài sản.

Một quy trình để đảm bảo kịp thời chuyển nhượng quyền sở hữu tài sản thường được thực hiện. Quyền sở hữu phải được chỉ định khi tài sản được tạo ra hoặc khi tài sản được chuyển giao cho tổ chức. Các chủ sở hữu tài sản phải chịu trách nhiệm cho việc quản lý thích hợp của một tài sản trong toàn bộ vòng đời của tài sản.

Người sở hữu tài sản cần có trách nhiệm trong việc:

- Đảm bảo tài sản được kiểm kê;
- Đảm bảo rằng tài sản được phân loại một cách thích hợp và được bảo vệ;
- Xác định và định kỳ kiểm tra lại các giới hạn và phân loại truy cập, cân nhắc các chính sách quản lý truy cập có thể áp dụng;
- Đảm bảo xử lý đúng đắn khi các tài sản sẽ bị xóa hoặc bị phá hủy.

Thông tin khác

Các chủ sở hữu được xác định có thể là một cá nhân hoặc một thực thể đã được phê duyệt có trách nhiệm quản lý để kiểm soát toàn bộ vòng đời của một tài sản.

Có thể ủy quyền thực hiện các nhiệm vụ thông thường, ví dụ ủy quyền cho một người chăm sóc tài sản hàng ngày, nhưng người sở hữu vẫn phải duy trì trách nhiệm của họ.

Với các hệ thống thông tin phức tạp, thì có thể gom tài sản vào thành các nhóm, các nhóm hình thành một chức năng đặc biệt giống như "các dịch vụ". Trong trường hợp này, người sở hữu dịch vụ có trách nhiệm phân phối dịch vụ, bao gồm cả việc thực hiện chức năng của các tài sản.

8.1.3 Sử dụng hợp lý tài sản

Kiểm soát

Các quy tắc sử dụng hợp lý thông tin và tài sản gắn với phương tiện xử lý thông tin phải được xác định, lập tài liệu và triển khai.

Hướng dẫn thi hành

Những nhân viên và những người dùng thuộc tổ chức thứ ba đang sử dụng hoặc đang truy cập tới tài sản của tổ chức cần phải biết yêu cầu an toàn thông tin đối với thông tin của tổ chức, các tài sản khác liên quan đến thông tin và các tài nguyên và phương tiện xử lý thông tin. Họ cần có trách nhiệm với việc sử dụng bất kỳ nguồn tài nguyên xử lý thông tin và bất kỳ việc sử dụng nào của họ.

8.1.4 Trả lại tài sản

Kiểm soát

Tất cả nhân viên và người sử dụng của tổ chức bên ngoài cần trả lại tất cả các tài sản của tổ chức mà họ quản lý ngay khi kết thúc làm việc, hợp đồng hoặc thoả thuận.

Hướng dẫn thi hành

Quy trình chấm dứt cần được chính thức hóa bao gồm cả việc hoàn trả tất các tài sản vật lý hoặc điện tử đã phát ra trước kia thuộc sở hữu hoặc ủy nhiệm của tổ chức.

Trong các trường hợp mà một nhân viên hoặc người sử dụng của tổ chức bên ngoài mua thiết bị của tổ chức hoặc sử dụng thiết bị cá nhân thuộc sở hữu của họ thì cần thực hiện các thủ tục nhằm đảm bảo rằng tất cả các thông tin liên quan đều đã được chuyển lại cho tổ chức và đã được xóa khỏi thiết bị này ([xem 11.2.7](#)).

Trong các trường hợp mà một nhân viên hoặc người sử dụng của tổ chức bên ngoài có các kiến thức quan trọng cho các hoạt động tiếp theo thì thông tin đó cần được lập thành tài liệu và chuyển cho tổ chức.

Trong thời gian thông báo chấm dứt, tổ chức phải kiểm soát việc sao chép trái phép thông tin có liên quan (ví dụ như sở hữu trí tuệ) của nhân viên hoặc nhà thầu đang chấm dứt đó.

8.2 Phân loại thông tin

Mục tiêu: Nhằm đảm bảo thông tin có mức độ bảo vệ thích hợp theo đúng mức tầm quan trọng của nó đối với tổ chức.

8.2.1 Phân loại thông tin

Kiểm soát

Thông tin cần được phân loại theo giá trị, các yêu cầu pháp lý, độ quan trọng và nhạy cảm đối với tổ chức.

Hướng dẫn thi hành

Việc phân loại và các biện pháp kiểm soát bảo vệ liên quan cần xem xét đến nhu cầu nghiệp vụ trong việc chia sẻ hoặc hạn chế thông tin, cũng như các yêu cầu pháp lý. Tài sản khác với thông tin có thể được phân loại cho phù hợp với phân loại của thông tin của tài sản trong lưu trữ, xử lý hoặc không xử lý hoặc được bảo vệ.

Chủ sở hữu thông tin tài sản cần chịu trách nhiệm cho việc phân loại chúng.

Các đề án phân loại cần đưa ra các quy ước phân loại và tiêu chí để xem xét việc phân loại theo thời gian. Cấp độ bảo vệ trong đề án này cần được đánh giá bằng cách phân tích an toàn, tính toàn vẹn và tính sẵn sàng và các yêu cầu khác đối với các thông tin được xem xét. Đề án cần được gắn kết với các chính sách kiểm soát truy cập ([xem 9.1.1](#)).

Mỗi cấp độ cần được đặt một cái tên có ý nghĩa trong khuôn khổ sơ đồ phân loại của ứng dụng.

Đề án cần được nhất quán trên toàn bộ tổ chức để mọi người sẽ phân loại thông tin và tài sản liên quan cùng một kiểu, cần có một sự hiểu biết chung về các yêu cầu bảo vệ và áp dụng sự bảo vệ thích hợp.

Các quy trình của tổ chức cần được phân loại, và phải nhất quán và chặt chẽ trong toàn tổ chức. Kết quả phân loại cần chỉ ra giá trị của tài sản phụ thuộc vào mức độ quan trọng và độ nhạy cảm của tổ chức, ví dụ về tính bảo mật, tính toàn vẹn và tính sẵn sàng. Kết quả phân loại cần được cập nhật phù hợp với những thay đổi của giá trị, độ quan trọng và nhạy cảm với chu kỳ sống của nó.

Thông tin khác

Phân loại thông tin cung cấp cho người sử dụng thông tin một chỉ báo ngắn gọn về cách xử lý và bảo vệ nó. Có thể thúc đẩy việc này bằng cách tạo nhóm các thông tin có nhu cầu bảo vệ tương tự và quy định thủ tục an toàn thông tin cụ thể áp dụng cho tất cả các thông tin thuộc mỗi nhóm này.

Thông tin có thể không còn là nhạy cảm hoặc quan trọng sau một thời gian nhất định, ví dụ, khi thông tin đã được công bố công khai. Những khía cạnh này cần được tính đến, do việc phân loại quá mức sẽ dẫn đến việc thực hiện kiểm soát không cần thiết gây ra những chi phí bổ sung hoặc ở chiều ngược lại việc phân loại dưới mức có thể gây nguy hiểm cho việc đạt được các mục tiêu nghiệp vụ.

Một ví dụ về chương trình phân loại thông tin mật có thể được dựa trên 4 cấp độ như sau:

- a) tiết lộ thông tin sẽ không gây hại;
- b) tiết lộ thông tin sẽ gây sự lúng túng nhỏ hoặc gây phiền phức nhỏ cho hoạt động;
- c) tiết lộ thông tin sẽ có tác động đáng kể đến hoạt động ngắn hạn hoặc mục tiêu chiến lược;
- d) tiết lộ thông tin sẽ tác động nghiêm trọng đến mục tiêu chiến lược dài hạn hoặc đẩy tổ chức vào nguy cơ sống còn.

8.2.2 Gắn nhãn thông tin

Kiểm soát

Các thủ tục cần thiết cho việc gắn nhãn và quản lý thông tin cần được phát triển và triển khai phù hợp với lược đồ phân loại thông tin đã được tổ chức chấp nhận.

Hướng dẫn thi hành

Các thủ tục gắn nhãn thông tin cần được xây dựng cho tất cả các tài sản thông tin ở cả dạng vật lý và điện tử. Việc gắn nhãn cần thể hiện phân loại theo các quy tắc đã thiết lập. Các nhãn cần dễ dàng nhận biết. Các thủ tục cần phải đưa ra hướng dẫn về nơi và cách nhãn được gắn trong việc xem xét các cách thức thông tin được truy cập hoặc các tài sản được xử lý tùy thuộc vào các loại phương tiện truyền thông. Các thủ tục có thể xác định trường hợp gắn nhãn được bỏ qua, ví dụ: gắn nhãn thông tin không bí mật để giảm khối lượng công việc. Nhân viên và nhà thầu cần biết về các thủ tục gắn nhãn.

Đầu ra từ hệ thống có chứa thông tin được phân loại là nhạy cảm hoặc quan trọng cần thực hiện gắn nhãn phân loại thích hợp.

Thông tin khác

Gắn nhãn các thông tin mật là một yêu cầu quan trọng đối với thỏa thuận chia sẻ thông tin. Nhãn vật lý và siêu dữ liệu là một dạng phổ biến của nhãn.

Gắn nhãn thông tin và các tài sản liên quan của nó đôi khi có tác động tiêu cực. Các tài sản được phân loại sẽ dễ dàng hơn trong việc nhận diện và tương ứng sẽ dễ bị đánh cắp bởi những kẻ tấn công trong nội bộ hay bên ngoài.

8.2.3 Xử lý tài sản

Kiểm soát

Thủ tục xử lý tài sản phải được phát triển và thực hiện phù hợp với cách thức phân loại thông tin của tổ chức.

Hướng dẫn thi hành

Phải xây dựng thủ tục xử lý, lưu trữ, truyền tải thông tin nhất quán với mức độ phân loại thông tin (xem [8.2.1](#)).

Cần quan tâm đến những điều sau:

- a) hạn chế truy cập để hỗ trợ yêu cầu an toàn với mỗi mức phân loại;
- b) duy trì bản ghi chính thức của người nhận ủy quyền tài sản;
- c) bảo vệ bản sao thông tin cùng với bản gốc ở một mức độ phù hợp;
- d) bảo quản tài sản công nghệ thông tin phù hợp với thông số kỹ thuật của nhà sản xuất;
- e) đánh dấu rõ ràng tất cả bản sao của thiết bị để người nhận ủy quyền có thể biết.

Hệ thống phân loại được sử dụng trong tổ chức có thể không tương đương với hệ thống được sử dụng bởi các tổ chức khác, thậm chí khi tên các mức phân loại là tương tự; ngoài ra, thông tin di chuyển giữa các tổ chức có thể khác nhau về phân loại tùy thuộc vào ngữ cảnh của nó trong mỗi tổ chức, ngay cả khi hệ thống phân loại của chúng là giống hệt nhau.

Thỏa thuận với các tổ chức khác bao gồm chia sẻ thông tin phải bao gồm các thủ tục để xác định phân loại của thông tin đó và để giải thích các nhãn phân loại từ tổ chức khác.

8.3 Xử lý thiết bị lưu trữ

Mục tiêu: Để ngăn chặn việc tiết lộ, sửa đổi, loại bỏ hoặc phá hủy thông tin trên thiết bị lưu trữ một cách trái phép.

8.3.1 Quản lý các phương tiện lưu trữ thông tin có thể di dời

Kiểm soát

Các thủ tục cần được thực hiện đối với việc quản lý các phương tiện lưu trữ thông tin có thể di dời phù hợp với quy trình phân loại đã được tổ chức đặt ra.

Hướng dẫn thi hành

Các hướng dẫn sau đây áp dụng cho việc quản lý các phương tiện lưu trữ thông tin có thể di dời cần được xem xét:

- a) nếu không còn cần thiết, mọi nội dung của bất kỳ phương tiện lưu trữ thông tin tái sử dụng nào trước khi được loại bỏ khỏi tổ chức phải được xóa vĩnh viễn, không thể phục hồi được;
- b) khi cần thiết và thực hiện được, cấp có thẩm quyền cần yêu cầu các phương tiện lưu trữ thông tin cần loại bỏ khỏi tổ chức và một hồ sơ các phương tiện lưu trữ thông tin bị loại bỏ như vậy cần được giữ để duy trì một lưu vết kiểm toán;
- c) tất cả các phương tiện lưu trữ thông tin cần được lưu trữ trong một môi trường an toàn và an ninh, phù hợp với các yêu cầu thông số kỹ thuật của nhà sản xuất;

- d) nếu an toàn thông tin hoặc tính toàn vẹn dữ liệu là những yêu cầu quan trọng, các kỹ thuật mật mã cần được áp dụng để bảo vệ dữ liệu lưu trên phương tiện lưu trữ thông tin có thể di dời;
- e) để giảm thiểu nguy cơ của phương tiện lưu trữ thông tin bị xuống cấp trong khi dữ liệu được lưu trữ vẫn còn cần thiết, các dữ liệu cần được chuyển đổi sang các phương tiện lưu trữ thông tin mới trước khi trở thành không đọc được;
- f) các bản sao của dữ liệu có giá trị cần được lưu trữ trên các phương tiện lưu trữ thông tin riêng biệt để tránh các nguy cơ thiệt hại hay mất mát dữ liệu xảy ra trùng hợp ngẫu nhiên;
- g) đăng ký các thiết bị lưu trữ có thể di dời cần được thực hiện để hạn chế các nguy cơ gây mất mát dữ liệu;
- h) các ổ đĩa lưu trữ có thể di dời chỉ cần được kích hoạt nếu có một lý do nghiệp vụ cần làm như vậy;
- i) khi có nhu cầu sử dụng các phương tiện lưu trữ thông tin có thể di dời, việc chuyển giao thông tin lên các phương tiện lưu trữ thông tin có thể di dời này cần được theo dõi.

Các thủ tục và mức độ phân quyền phải được lập thành tài liệu.

8.3.2 Loại bỏ các phương tiện lưu trữ thông tin

Kiểm soát

Phương tiện lưu trữ thông tin cần được loại bỏ một cách an toàn khi không còn sử dụng nữa, áp dụng các thủ tục chính thức.

Hướng dẫn thi hành

Các thủ tục chính thức cho việc loại bỏ một cách an toàn các phương tiện lưu trữ thông tin cần được thiết lập để giảm thiểu nguy cơ các thông tin bí mật bị rò rỉ cho người ngoài. Số lượng thủ tục loại bỏ một cách an toàn các phương tiện lưu trữ thông tin chứa đựng các thông tin bí mật cần tăng theo tỷ lệ thuận với mức độ nhạy cảm của thông tin đó. Các mục sau đây cần được xem xét:

- a) phương tiện lưu trữ thông tin có chứa thông tin bí mật cần được lưu trữ và loại bỏ một cách an toàn, ví dụ như qua đốt hoặc băm nhỏ, hoặc bị xóa dữ liệu sử dụng bởi một ứng dụng khác của tổ chức;
- b) các thủ tục cần được thực hiện đúng chỗ để xác định danh mục các phương tiện lưu trữ thông tin phải bị loại bỏ một cách an toàn;
- c) sẽ dễ dàng hơn nếu các danh mục phương tiện lưu trữ thông tin được sắp xếp, thu gom và loại bỏ một cách an toàn cùng với nhau, chứ không phải là cố gắng để tách ra các phương tiện lưu trữ thông tin nhạy cảm riêng rẽ;

- d) nhiều tổ chức cung cấp dịch vụ thu gom và loại bỏ đối với phương tiện lưu trữ thông tin; cần quan tâm đúng mức đến việc lựa chọn phù hợp đối tác bên ngoài với đầy đủ các kiểm soát và kinh nghiệm tương ứng;
- e) việc tiêu hủy thông tin nhạy cảm cần phải được ghi chép nhằm lưu vết phục vụ kiểm toán.

Khi tích lũy nhiều phương tiện lưu trữ thông tin để loại bỏ, cần xem xét đến tác động khi ghép các thông tin, trong đó có thể gây ra hiện tượng một số lượng lớn thông tin từ chỗ không nhạy cảm có thể trở thành nhạy cảm.

Thông tin khác

Khi các thiết bị hư hỏng có chứa dữ liệu nhạy cảm có thể cần yêu cầu một đánh giá rủi ro để xác định xem các phương tiện lưu trữ thông tin cần bị phá hủy về mặt vật lý hay là gửi đi sửa chữa hoặc loại bỏ hoàn toàn ([xem 11.2.7](#)).

8.3.3 Vận chuyển phương tiện vật lý

Kiểm soát

Phương tiện chứa thông tin cần được bảo vệ khỏi sự truy cập trái phép, sự lạm dụng hoặc làm sai lệch khi vận chuyển vượt ra ngoài phạm vi địa lý của tổ chức.

Hướng dẫn thi hành

Cần quan tâm đến các hướng dẫn sau nhằm bảo vệ phương tiện chứa thông tin trong quá trình vận chuyển giữa các địa điểm:

- a) sử dụng phương tiện và người vận chuyển tin cậy;
- b) cần thỏa thuận với ban lãnh đạo về danh sách những người được phép vận chuyển;
- c) cần áp dụng các thủ tục kiểm tra lai lịch người vận chuyển;
- d) đóng gói cẩn thận nhằm bảo vệ nội dung của các phương tiện khỏi các hư hại vật lý có khả năng xảy ra trong quá trình vận chuyển và tuân theo các chỉ tiêu kỹ thuật của nhà sản xuất (ví dụ đối với phần mềm), ví dụ bảo vệ chống lại các yếu tố về môi trường có khả năng làm giảm hiệu quả khôi phục dữ liệu của phương tiện như nhiệt độ, độ ẩm hoặc các trường điện từ;
- e) nhật ký phải được giữ, xác định nội dung của các phương tiện truyền thông, bảo vệ được áp dụng cũng như ghi lại những lần chuyển giao cho những người quá cảnh và nhận tại điểm đến.

Thông tin khác

Thông tin có thể dễ bị truy cập trái phép, sử dụng sai hoặc làm sai lệch trong quá trình vận chuyển vật lý, ví dụ khi gửi phương tiện truyền thông qua dịch vụ bưu điện hoặc chuyển phát nhanh.

9 Kiểm soát truy cập

9.1 Yêu cầu nghiệp vụ đối với kiểm soát truy cập

Mục tiêu: Giới hạn việc truy cập thông tin và các phương tiện xử lý thông tin.

9.1.1 Chính sách kiểm soát truy cập

Kiểm soát

Chính sách kiểm soát truy cập cần được thiết lập, lập tài liệu và soát xét dựa trên các yêu cầu nghiệp vụ và an toàn đối với các truy cập.

Hướng dẫn thi hành

Các chủ sở hữu tài sản cần xác định các quy tắc kiểm soát truy cập một cách phù hợp, các quyền truy cập và các hạn chế đối với các vai trò người dùng cụ thể với mức độ chi tiết và chặt chẽ của các biện pháp kiểm soát phản ánh các rủi ro về an toàn thông tin tương ứng.

Các biện pháp kiểm soát truy cập phải bao gồm cả về mặt logic và vật lý (xem điều 11) và chúng phải được xem xét đồng thời. Các nhà cung cấp dịch vụ và người dùng cần được tuyên bố rõ ràng về các yêu cầu nghiệp vụ phải được đáp ứng bởi với các biện pháp kiểm soát truy cập.

Chính sách kiểm soát truy cập cần quan tâm đến các vấn đề sau:

- a) các yêu cầu về an toàn thông của các ứng dụng nghiệp vụ;
- b) các chính sách về cấp phép và phổ biến thông tin, ví dụ nhu cầu phải biết về nguyên tắc và các mức độ an toàn thông tin và phân loại thông tin (xem 8.2);
- c) sự thống nhất các chính sách kiểm soát truy cập và phân loại thông tin của các mạng và các hệ thống khác nhau;
- d) quy định của pháp luật và các nghĩa vụ thỏa thuận bất kỳ liên quan đến việc bảo vệ truy cập dữ liệu hoặc các dịch vụ (xem 18.1);
- e) việc kiểm soát các quyền truy cập trong một môi trường nội mạng và phân tán, môi trường này nhận ra tất cả các dạng kết nối sẵn có;
- f) việc phân tách các vai trò kiểm soát truy cập, ví dụ yêu cầu truy cập, việc cấp phép truy cập, quản trị truy cập;
- g) các yêu cầu đối với việc cấp phép chính thức cho các yêu cầu truy cập (xem 9.2.1 và 9.2.2);
- h) các yêu cầu đối với việc soát xét định kỳ những biện pháp kiểm soát truy cập (xem 9.2.5);
- i) loại bỏ các quyền truy cập (xem 9.2.6);

- j) Lưu trữ các bản ghi của tất cả các sự kiện quan trọng liên quan đến việc sử dụng và kiểm soát định danh người dùng và các thông tin xác thực bí mật;
- k) Các vai trò với các truy cập được cấp quyền (xem 9.2.3).

Thông tin khác

Cần quan tâm tới các vấn đề sau khi xác định các quy tắc kiểm soát truy cập:

- a) thiết lập các quy tắc dựa trên tiêu chí "mọi thứ đều bị cấm trừ khi được cho phép tiết lộ" thay vì quy tắc "Mọi thứ đều được phép trừ những thứ bị cấm tiết lộ";
- b) những thay đổi trong các nhãn thông tin (xem 8.2.2) được khởi tạo tự động bởi các phương tiện xử lý thông tin và do ý muốn của một người dùng;
- c) những thay đổi về việc cho phép người dùng được khởi tạo tự động bởi hệ thống thông tin và bởi một người quản trị hệ thống;
- d) các quy tắc đòi hỏi hoặc không đòi hỏi phải được chấp thuận trước khi ban hành.

Các quy tắc kiểm soát truy cập cần được hỗ trợ bởi các thủ tục chính thức (xem 9.2, 9.3, 9.4) và các trách nhiệm đã được xác định rõ (xem 6.1.1, 9.3).

Dựa trên vai trò kiểm soát truy cập là một phương pháp được sử dụng thành công bởi nhiều tổ chức liên kết quyền truy cập với vai trò nghiệp vụ.

Hai nguyên tắc thường được sử dụng cho chính sách truy cập đó là:

- a) Cần phải biết: bạn chỉ được phép truy cập vào những thông tin thuộc nhiệm vụ bạn cần thực hiện (nhiệm vụ/ vai trò khác nhau có ý nghĩa khác nhau do đó hồ sơ truy cập là khác nhau);
- b) Cần phải dùng: bạn chỉ được phép truy cập vào những công cụ xử lý thông tin (thiết bị công nghệ thông tin, ứng dụng, thủ tục, văn phòng) mà cần cho thực hiện nhiệm vụ/công việc của bạn.

9.1.2 Truy cập mạng và các dịch vụ mạng

Kiểm soát

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

Hướng dẫn thi hành

Chính sách cần thiết lập quy tắc cho các vấn đề sử dụng mạng và các dịch vụ mạng. Chính sách này cần bao phủ:

- a) mạng và các dịch vụ mạng được phép truy cập;
- b) các thủ tục cấp phép nhằm quyết định ai là người được phép truy cập mạng và các dịch vụ mạng;
- c) kiểm soát truy cập và các thủ tục nhằm bảo vệ truy cập tới các kết nối mạng và các dịch vụ mạng;

- d) các phương tiện dùng để truy cập vào mạng và các dịch vụ mạng (ví dụ sử dụng VPN hay mạng không dây);
- e) các yêu cầu xác thực người dùng khi truy cập các dịch vụ mạng khác nhau;
- f) giám sát việc sử dụng các dịch vụ mạng.

Chính sách sử dụng các dịch vụ mạng phải nhất quán với chính sách kiểm soát truy cập của tổ chức ([xem 9.1.1](#))

Thông tin khác

Các kết nối phi xác thực và không an toàn tới các dịch vụ mạng có thể ảnh hưởng đến toàn bộ tổ chức. Biện pháp kiểm soát này đặc biệt quan trọng cho các kết nối mạng nhạy cảm hoặc các ứng dụng nghiệp vụ tối quan trọng hoặc với những người dùng có rủi ro cao về vị trí, như các khu vực công cộng hoặc các khu vực ngoài nằm ngoài phạm vi quản lý và kiểm soát an toàn thông tin của tổ chức.

9.2 Kiểm soát 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 thông tin và dịch vụ.

9.2.1 Đăng ký và hủy thành viên đăng ký

Kiểm soát

Một thủ tục chính thức về đăng ký và hủy đăng ký thành viên cần phải được triển khai nhằm cho phép phân công các quyền truy cập.

Hướng dẫn thi hành

Quy trình kiểm soát tài khoản người dùng cần bao gồm những điều sau:

- a) sử dụng các tài khoản người dùng duy nhất nhằm cho phép nhiều người dùng có thể được liên kết tới và giữ trách nhiệm đối với các hoạt động của họ; việc sử dụng các địa chỉ nhóm chỉ được cho phép nếu chúng cần thiết cho các lý do điều hành hoặc nghiệp vụ, và cần được phê duyệt và biên soạn thành tài liệu;
- b) lập tức vô hiệu hoá hoặc loại bỏ các tài khoản người dùng của những người đã nghỉ việc ([xem 9.2.6](#));
- c) kiểm tra định kỳ và loại bỏ hoặc vô hiệu hoá các tài khoản dự phòng;
- d) đảm bảo rằng các tài khoản thừa không được cấp cho những người dùng khác.

Thông tin khác

Cấp phát hoặc thu hồi truy cập thông tin hoặc phương tiện xử lý thông tin là một thủ tục thường bao gồm hai bước:

- a) chỉ định và cho phép, hoặc thu hồi một tài khoản người dùng;
- b) cấp phát hoặc thu hồi các quyền truy cập đối với người dùng đó ([xem 9.2.2](#)).

9.2.2 Cấp phát quyền truy cập người dùng

Kiểm soát

Một quy trình cấp phát quyền truy cập người dùng chính thức cần được triển khai nhằm chỉ định hoặc thu hồi các quyền truy cập cho tất cả loại người dùng của tất cả các hệ thống và dịch vụ.

Hướng dẫn thi hành

Quy trình cấp phát cho việc chỉ định hoặc thu hồi quyền truy cập đối cho các tài khoản người dùng cần bao gồm:

- a) lấy ủy quyền của chủ sở hữu hệ thống thông tin hoặc dịch vụ đối với việc sử dụng hệ thống thông tin hoặc dịch vụ ([xem 8.1.2](#)); việc phê duyệt riêng rẽ các quyền truy cập từ ban điều hành cũng phù hợp;
- b) xác minh các cấp độ truy cập được cấp phép là phù hợp với các chính sách truy cập ([xem 9.1](#)) và là nhất quán với các yêu cầu khác như phân tách các nhiệm vụ ([xem 6.1.2](#));
- c) đảm bảo rằng các quyền truy cập không được kích hoạt (ví dụ bởi các nhà cung cấp dịch vụ) trước khi các thủ tục ủy quyền được hoàn tất;
- d) duy trì kho lưu trữ trung tâm về các bản ghi của các quyền truy cập đã được cấp phát cho một tài khoản người dùng để truy cập các hệ thống thông tin và dịch vụ;
- e) sửa đổi các quyền truy cập của những người đã được thay đổi vai trò hoặc công việc và loại bỏ hoặc khoá ngay lập tức các quyền truy cập đối với những người nghỉ việc;
- f) định kỳ soát xét các quyền truy cập với các chủ sở hữu các hệ thống thông tin hoặc dịch vụ ([xem 9.2.5](#)).

Thông tin khác

Cần soát xét việc thiết lập các quyền truy cập dựa trên các yêu cầu nghiệp vụ mà tổng hợp một số quyền truy cập thành các hồ sơ truy cập thông dụng. Các yêu cầu truy cập và soát xét ([xem 9.2.4](#)) được kiểm soát ở mức thông dụng này dễ dàng hơn so với cấp độ các quyền truy cập cụ thể.

Cần soát xét lại các hợp đồng tuyển dụng, các hợp đồng dịch vụ với các điều khoản xử phạt nếu người dùng cố gắng truy cập các hệ thống hoặc dịch vụ bất hợp pháp ([xem 7.1.2, 7.2.3, 13.2.4, 15.1.2](#)).

9.2.3 Kiểm soát đặc quyền truy cập

Kiểm soát

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

Hướng dẫn thi hành

Việc cấp phát các đặc quyền truy cập cần phải được kiểm soát thông qua một quy trình trao quyền chính thức cùng với các chính sách kiểm soát truy cập liên quan ([xem 9.1.1](#)). Những bước dưới đây cần được quan tâm:

- a) cần xác định các đặc quyền truy cập gắn liền với mỗi hệ thống, ví dụ hệ điều hành, hệ quản trị cơ sở dữ liệu và mỗi ứng dụng, và những người dùng cần được phân bổ quyền truy cập;
- b) các đặc quyền cần được phân bổ cho những người dùng dựa trên cơ sở cần - sử dụng và trên cơ sở từng sự kiện phù hợp với chính sách kiểm soát truy cập ([xem 9.1.1](#)), nghĩa là yêu cầu tối thiểu đối với vai trò chức năng của họ chỉ khi được yêu cầu;
- c) cần duy trì một quy trình trao quyền và một hồ sơ các đặc quyền đã được phân bổ. Không được cấp phép các đặc quyền cho đến khi việc quá trình trao quyền đã hoàn tất;
- d) cần xác định các yêu cầu về thời hạn được cấp đặc quyền truy cập;
- e) các đặc quyền phải được gán cho một địa chỉ người dùng khác với những được sử dụng cho mục đích nghiệp vụ thông thường;
- f) Cần soát xét định kỳ thẩm quyền của người dùng về các đặc quyền truy cập phù hợp với bỗn phận trách nhiệm của họ;
- g) các thủ tục cụ thể cần phải được thiết lập và duy trì để tránh việc sử dụng bất hợp pháp tài khoản quản trị thông dụng, theo khả năng cấu hình của các hệ thống;
- h) đối với các tài khoản quản trị thông dụng, tính bí mật của các thông tin xác thực bí mật cần được duy trì khi chia sẻ (ví dụ thay đổi mật khẩu thường xuyên và sớm nhất có thể khi một người có đặc quyền truy cập nghỉ việc hoặc thay đổi công việc, việc giao tiếp giữa những người có đặc quyền truy cập cần có các cơ chế phù hợp).

Thông tin khác

Việc sử dụng không phù hợp các đặc quyền quản trị hệ thống (tính năng hay tiện ích bất kỳ của hệ thống thông tin cho phép người dùng bỏ qua các biện pháp kiểm soát hệ thống hoặc ứng dụng) có thể là một yếu tố chính gây ra các lỗi hay các lỗ hổng hệ thống.

9.2.4 Kiểm soát các thông tin xác thực bí mật của người dùng

Kiểm soát

Việc cấp phát các thông tin xác thực bí mật cho người dùng cần được kiểm soát thông qua một quy trình kiểm soát chính thức.

Hướng dẫn thi hành

Quá trình kiểm soát kiểm soát thông tin xác thực bí mật của người dùng cần bao gồm những yêu cầu sau:

- a) người dùng cần được yêu cầu ký vào một tờ in sẵn để giữ bí mật các thông tin xác thực và giữ các thông tin xác thực bí mật của nhóm chỉ trong nội bộ các thành viên của nhóm; bản ký này có thể nằm trong các điều khoản và điều kiện tuyển dụng (xem 7.1.2);
- b) khi người dùng được yêu cầu duy trì các thông tin xác thực bí mật riêng của mình, ban đầu họ cần phải được cung cấp một thông tin xác thực bí mật an toàn tạm thời, thông tin xác thực này sau đó sẽ bị buộc phải được thay đổi ngay;
- c) thiết lập các thủ tục nhằm xác minh danh tính của người dùng trước khi cung cấp một thông tin xác thực bí mật mới, thông tin xác thực bí mật thay thế hoặc thông tin xác thực bí mật tạm thời;
- d) các thông tin xác thực bí mật tạm thời phải được trao cho người dùng một cách an toàn; việc sử dụng của bên thứ ba hoặc các thông điệp thư điện tử không được bảo vệ (bản rõ) cần được tránh;
- e) các thông tin xác thực an toàn tạm thời phải là duy nhất đối với mỗi cá nhân và không thể đoán được;
- f) người dùng cần có kiến thức về việc nhận các thông tin xác thực bí mật;
- g) các thông tin xác thực an toàn tạm thời mặc định của nhà cung cấp cần được thay đổi ngay sau khi cài đặt hệ thống và phần mềm.

Thông tin khác

Mật khẩu là phương tiện phổ biến trong việc xác minh danh tính của người dùng trước khi truy cập tới các hệ thống thông tin hay các dịch vụ. Các công nghệ khác để nhận dạng và xác thực người dùng, chẳng hạn như các khoá an toàn và các dạng lưu trữ dữ liệu trên phần cứng khác, như sử dụng thẻ phần cứng để tạo ra mã xác thực.

9.2.5 Soát xét các quyền truy cập người dùng

Kiểm soát

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

Hướng dẫn thi hành

Việc soát xét các quyền truy cập cần quan tâm đến các hướng dẫn sau đây:

- a) các quyền truy cập của người dùng cần được soát xét định kỳ, và khi có bất kỳ sự thay đổi nào, ví dụ được đề bạt, bị giáng chức, hoặc kết thúc công việc;

- b) các quyền truy cập của người dùng cần được soát xét và phân bổ lại khi người dùng chuyển từ vai trò này sang vai trò khác trong tổ chức;
- c) các cấp phép cho các đặc quyền truy cập đặc biệt cần được soát xét thường xuyên hơn;
- d) các phân bổ đặc quyền cũng phải được kiểm tra định kỳ nhằm đảm bảo rằng những đặc quyền chưa được cấp phép thì không được sử dụng;
- e) những thay đổi của các tài khoản đặc quyền cần được ghi vào nhật ký soát xét định kỳ.

Thông tin khác

Biện pháp kiểm soát này bù cho những lỗ hổng có thể có trong việc thực thi các biện pháp kiểm soát 9.2.1, 9.2.2 và 9.2.6.

9.2.6 Hủy bỏ hoặc chỉnh sửa quyền truy cập

Kiểm soát

Các quyền truy cập của toàn bộ nhân viên và các đối tác bên ngoài đối với thông tin và các phương tiện xử lý thông tin cần phải được huỷ bỏ khi chấm dứt hợp đồng hoặc thoả thuận, hoặc phải được điều chỉnh theo sự thay đổi tương ứng.

Hướng dẫn thi hành

Khi chấm dứt hợp đồng, các quyền truy cập thông tin của các cá nhân đối với thông tin và các tài sản đi kèm với các phương tiện xử lý thông tin và dịch vụ phải được huỷ bỏ hoặc đình chỉ. Biện pháp kiểm soát này sẽ quyết định liệu các quyền truy cập có cần phải bị huỷ bỏ hay không. Các thay đổi về người lao động cần phải phản ánh lên việc huỷ bỏ các quyền truy cập mà chưa được chuáp thuận đối với người lao động mới. Các quyền truy cập cần phải được huỷ bỏ hoặc điều chỉnh bao gồm các truy cập tài sản vật lý và logic. Việc huỷ bỏ hoặc điều chỉnh cần phải được hoàn thành qua việc huỷ bỏ, thu hồi hoặc thay thế các khoá, các thẻ định danh, các phương tiện xử lý thông tin hoặc các thuê bao. Bất kỳ tài liệu nào xác định các quyền truy cập của nhân viên và nhà thầu cần phản ánh sự huỷ bỏ hoặc điều chỉnh của các quyền truy cập. Nếu nhân viên thử việc hoặc đối tác ngoài biết mật khẩu của các tài khoản người dùng vẫn ở trạng thái kích hoạt, những tài khoản này vẫn được thay đổi theo sự chấm dứt hoặc thay đổi của nhân viên theo hợp đồng hoặc thoả thuận.

Các quyền truy cập thông tin và tài sản đi cùng với các phương tiện xử lý thông tin cần phải được giảm thiểu hoặc huỷ bỏ trước khi chấm dứt hợp đồng hoặc thay đổi nhân viên dựa trên các đánh giá về các yếu tố rủi ro như:

- a) liệu sự chấm dứt hoặc thay đổi là do người dùng, đối tác bên ngoài hay do ban kiểm soát, và lý do của việc chấm dứt;
- b) các trách nhiệm hiện tại của nhân viên, đối tác bên ngoài hoặc của bất kỳ người nào khác;

c) giá trị của các tài sản vẫn còn có thể truy cập hiện tại.

Thông tin khác

Trong một số trường hợp quyền truy cập có thể được phân bổ cho nhiều người hơn là các nhân viên rời rạc hoặc người dùng của bên ngoài, ví dụ như các tài khoản nhóm. Trong những hoàn cảnh này, các cá nhân rời rạc cần được loại ra khỏi bất kỳ danh sách truy cập nhóm nào và cần tư vấn tất cả tất cả các nhân viên và người sử dụng bên ngoài khác không chia sẻ thông tin này với người đã loại ra.

Trong trường hợp ban kiểm soát là phía đưa ra việc chấm dứt hợp đồng hoặc thoả thuận, những nhân viên bắt mahn hoặc người sử dụng bên ngoài có thể cố gây hư hỏng thông tin hoặc phá hoại các phương tiện xử lý thông tin. Trong trường hợp người từ chức hay bị sa thải, họ có thể bị cấm dỗ để thu thập thông tin nhằm sử dụng trong tương lai.

9.3 Các trách nhiệm người dùng

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

9.3.1 Sử dụng thông tin xác thực bí mật

Kiểm soát

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

Hướng dẫn thi hành

Tất cả những người dùng cần được tư vấn:

- a) giữ bí mật các thông tin xác thực bí mật, đảm bảo không tiết lộ cho bất kỳ người khác kể cả những người có quyền cao hơn;
- b) tránh giữ hồ sơ (ví dụ giấy, tập tin phần mềm hoặc thiết bị cầm tay) của các thông tin xác thực bí mật, trừ khi hồ sơ này có thể được lưu trữ an toàn và phương pháp lưu trữ đã được phê duyệt;
- c) thay đổi thông tin xác thực bí mật bất cứ khi nào có bất kỳ dấu hiệu về tổn hại về thông tin xác thực này;
- d) khi dùng mật khẩu làm thông tin xác thực, lựa chọn mật khẩu chất lượng với độ dài tối thiểu mà:
 - 1) dễ nhớ
 - 2) không dựa trên bất cứ điều gì mà người khác có thể dễ dàng đoán hoặc có được nhờ các thông tin có liên quan tới cá nhân đó, ví dụ như, tên, số điện thoại, và ngày tháng năm sinh....
 - 3) không dễ bị tổn hại bởi những tấn công có từ điển (tức là không chứa các từ có trong từ điển)
 - 4) không phải là dạng các ký tự hay các số giống nhau liên tiếp;
 - 5) nếu là mật khẩu tạm thời, thay đổi ngay lần đăng nhập đầu tiên.

- e) không chia sẻ mật thông tin xác thực bí mật cá nhân;
- f) khi mật khẩu được sử dụng như là thông tin xác thực bí mật, cần đảm bảo các biện pháp bảo vệ mật khẩu trong các thủ tục truy cập tự động và lưu trữ mật khẩu;
- g) không sử dụng chung một mật khẩu cho tất cả các mục đích nghiệp vụ và không phải nghiệp vụ.

Thông tin khác

Việc cung cấp các công cụ đăng nhập một lần (Single Sign On - SSO) hoặc các công cụ kiểm soát thông tin xác thực khác giảm thiểu số lượng các thông tin xác thực bí mật mà người dùng được yêu cầu để bảo vệ, do đó làm tăng hiệu quả của biện pháp kiểm soát này. Tuy nhiên những công cụ này cũng có thể làm tăng tác động của việc tiết lộ bí mật.

9.4 Kiểm soát truy cập vào hệ thống và ứng dụng

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

9.4.1 Hạn chế truy cập thông tin

Kiểm soát

Việc truy cập thông tin và các chức năng của hệ thống và ứng dụng cần được hạn chế phù hợp với chính sách kiểm soát truy cập đã xác định.

Hướng dẫn thi hành

Những hạn chế truy cập cần dựa trên các yêu cầu ứng dụng nghiệp vụ cụ thể theo các chính sách kiểm soát truy cập đã được xác định trước.

Cần soát xét áp dụng các hướng dẫn sau nhằm hỗ trợ các yêu cầu hạn chế truy cập:

- a) cung cấp các lựa chọn kiểm soát truy cập tới các chức năng của hệ thống và ứng dụng;
- b) kiểm soát việc dữ liệu nào có thể được truy cập bởi một người cụ thể nào;
- c) kiểm soát các quyền truy cập của người dùng, ví dụ: đọc, viết, xóa và thực hiện;
- d) kiểm soát các quyền truy cập của các ứng dụng khác;
- e) giới hạn thông tin đầu ra;
- f) cung cấp kiểm soát truy cập vật lý và logic để cách ly các ứng dụng, dữ liệu ứng dụng hoặc các hệ thống nhạy cảm.

9.4.2 Các thủ tục đăng nhập an toàn

Kiểm soát

Những nơi đòi hỏi có chính sách kiểm soát truy cập, truy cập vào hệ thống và ứng dụng cần được kiểm soát bởi thủ tục đăng nhập an toàn.

Hướng dẫn thi hành

Một kỹ thuật xác thực phù hợp cần được lựa chọn để chứng minh tuyên bố danh tính của người dùng.

Trường hợp xác thực mạnh và xác minh danh tính là cần thiết, cần sử dụng các phương pháp xác thực khác với mật khẩu như mật mã, thẻ thông minh, thẻ hoặc các phương tiện sinh trắc học.

Thủ tục nhằm đăng nhập vào một hệ thống cần được thiết kế để tối giảm cơ hội truy cập trái phép. Vì vậy thủ tục đăng nhập cần tối giảm thông tin về hệ thống nhằm tránh phải cung cấp hỗ trợ không cần thiết cho những người dùng trái phép. Một thủ tục đăng nhập tốt cần:

- a) không hiển thị những nhận dạng ứng dụng hoặc hệ thống cho tới khi quá trình đăng nhập đã được thiết lập thành công;
- b) hiển thị cảnh báo chung rằng chỉ những người dùng đã được cấp phép mới được truy cập vào máy tính;
- c) không cung cấp những thông điệp giúp đỡ hỗ trợ người dùng trái phép trong thủ tục đăng nhập;
- d) kiểm tra tính hợp lệ của thông tin đăng nhập chỉ khi đã hoàn tất tất cả các dữ liệu đầu vào. Nếu xuất hiện một điều kiện sai thì hệ thống không được chỉ ra phần dữ liệu đúng hoặc sai;
- e) bảo vệ chống lại việc thử đăng nhập hàng loạt;
- f) lưu lại những lần cố gắng đăng nhập thành công và thất bại;
- g) nêu ra một sự kiện an toàn nếu phát hiện có vi phạm hoặc nỗ lực tiềm năng vi phạm các biện pháp kiểm soát đăng nhập;
- h) Hiển thị thông tin dưới đây sau khi hoàn thành thủ tục đăng nhập:
 - 1) Ngày và giờ của lần đăng nhập thành công trước đó;
 - 2) Những chi tiết về các lần cố gắng đăng nhập không thành công kể từ lần đăng nhập thành công gần nhất;
- i) không hiển thị mật khẩu đang được nhập vào;
- j) không truyền các mật khẩu dưới dạng ký tự rõ ràng trên mạng;
- k) kết thúc phiên đăng nhập sau một khoảng thời gian xác định không hoạt động, đặc biệt tại các vị trí có rủi ro cao như các nơi công cộng hoặc các khu vực bên ngoài tầm quản lý an toàn của tổ chức hoặc trên các thiết bị di động;
- l) giới hạn số lần kết nối nhằm tăng thêm vòng bảo vệ đối với các ứng dụng có nguy cơ mất an toàn cao và giảm thiểu cơ hội truy cập bất hợp pháp.

Thông tin khác

Mật khẩu là phương thức thông dụng nhằm xác minh và xác thực dựa trên một tiêu chí là bí mật chỉ người dùng biết. Có thể đạt được điều này bằng các công cụ mật mã và các phương thức xác thực. Độ mạnh của xác thực người dùng phải phù hợp với việc phân loại thông tin được truy cập.

Nếu mật khẩu được truyền đi dưới dạng ký tự rõ ràng trong suốt quá trình đăng nhập trên mạng, chúng có thể bị bắt giữ bởi chương trình "nghe lén" trên mạng.

9.4.3 Hệ thống quản lý mật khẩu

Kiểm soát

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

Hướng dẫn thi hành

Một hệ thống quản lý mật khẩu cần:

- a) bắt buộc sử dụng các tài khoản và mật khẩu cá nhân riêng để duy trì khả năng kiểm soát;
- b) cho phép người dùng chọn và thay đổi mật khẩu và có thủ tục xác nhận khi xảy ra lỗi đầu vào;
- c) bắt buộc phải chọn các mật khẩu chất lượng;
- d) bắt buộc người dùng thay đổi các mật khẩu ở lần đăng nhập đầu tiên;
- e) bắt buộc phải thay đổi mật khẩu định kỳ và khi cần thiết;
- f) duy trì hồ sơ gồm các mật khẩu trước đó của người dùng và ngăn chặn việc tái sử dụng;
- g) không hiển thị các mật khẩu trên màn hình khi nó đang được nhập vào hệ thống;
- h) lưu trữ các tệp mật khẩu riêng với dữ liệu hệ thống ứng dụng;
- i) lưu trữ và truyền mật khẩu theo dạng đã được bảo vệ.

Thông tin khác

Một vài ứng dụng yêu cầu mật khẩu người dùng phải được ấn định bởi một cơ quan có thẩm quyền độc lập; trong trường hợp này, điểm b), d) và e) của hướng dẫn trên đây không được áp dụng. Trong hầu hết các trường hợp mật khẩu được lựa chọn và duy trì bởi người dùng.

9.4.4 Sử dụng các chương trình tiện ích đặc quyền

Kiểm soát

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

Hướng dẫn thi hành

Những hướng dẫn sau đây về việc sử dụng các tiện ích hệ thống có khả năng ảnh hưởng tới việc kiểm soát hệ thống và ứng dụng cần được quan tâm:

- a) sử dụng các thủ tục định danh, thủ tục thẩm định và cấp phép cho các tiện ích của hệ thống;
- b) phân tách các tiện ích hệ thống khỏi các ứng dụng phần mềm;
- c) giới hạn sử dụng các tiện ích hệ thống chỉ trong một số lượng nhỏ nhất những người dùng tin cậy và đã được cấp phép (xem 9.2.3);
- d) cấp phép sử dụng đặc biệt các tiện ích hệ thống;
- e) giới hạn sự sẵn sàng của các tiện ích hệ thống, ví dụ trong khoảng thời gian có một sự thay đổi đã được cấp phép;
- f) ghi lại tất cả các lần sử dụng các tiện ích hệ thống;
- g) xác định và lập tài liệu các mức cấp phép cho các tiện ích hệ thống;
- h) loại bỏ hoặc vô hiệu hóa tất cả các chương trình tiện ích không cần thiết;
- i) không để các tiện ích hệ thống sẵn sàng cho những người dùng, người có truy cập vào các ứng dụng trên các hệ thống ở những nơi có yêu cầu phân tách nhiệm vụ.

Thông tin khác

Hầu hết các máy tính đều cài đặt một hoặc nhiều chương trình tiện ích có khả năng làm dừng các biện pháp kiểm soát hệ thống và ứng dụng.

9.4.5 Kiểm soát truy cập vào mã nguồn chương trình

Kiểm soát

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

Hướng dẫn thi hành

Truy cập tới mã nguồn chương trình và các thông tin liên quan (ví dụ các thiết kế, các chỉ tiêu kỹ thuật, các kế hoạch thẩm tra và các kế hoạch kiểm tra tính hợp lệ) cần được kiểm soát chặt chẽ, nhằm ngăn chặn việc đưa thêm chức năng trái phép và tránh những thay đổi không cố ý cũng như duy trì tính tuyệt mật của các tài sản trí tuệ có giá trị. Mã nguồn chương trình có thể được kiểm soát nếu được lưu trữ tập trung, tốt nhất là trong các thư viện nguồn chương trình. Những hướng dẫn sau đây cần được quan tâm trong việc kiểm soát truy cập tới các thư viện nguồn chương trình nhằm làm giảm khả năng làm hỏng các chương trình máy tính:

- a) nếu có thể thì các thư viện nguồn chương trình không giữ trong các hệ thống điều hành;
- b) mã nguồn chương trình và các thư viện nguồn chương trình cần được quản lý phù hợp với các thủ tục đã được thiết lập;

- c) nhân viên hỗ trợ chỉ được truy cập một cách hạn chế tới các thư viện nguồn chương trình;
- d) việc cập nhật các thư viện nguồn chương trình và các thông tin liên quan, và việc phát hành mã nguồn chương trình tới lập trình viên chỉ được thực hiện sau khi đã được cho phép;
- e) các danh sách chương trình cần được giữ trong môi trường an toàn;
- f) nhật ký kiểm toán cần được duy trì cho tất cả các lần truy cập tới các thư viện nguồn hệ thống;
- g) việc duy trì và sao chép các thư viện nguồn chương trình phải tuân theo các thủ tục quản lý thay đổi (xem 14.2.2).

Nếu mã nguồn chương trình được dự định sẽ được tiết lộ, các biện pháp kiểm soát bổ sung nhằm đảm bảo tính toàn vẹn của nó (ví dụ như chữ ký số) cần được soát xét.

10 Mật mã

10.1 Kiểm soát mật mã

Mục tiêu: Nhằm bảo vệ tính bí mật, xác thực và/hoặc tính toàn vẹn của thông tin bằng việc sử dụng hiệu quả và thích hợp mật mã.

10.1.1 Chính sách sử dụng các kiểm soát mật mã

Kiểm soát

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

Hướng dẫn thi hành

Khi xây dựng một chính sách mật mã cần lưu ý những điều sau đây:

- a) phương thức kiểm soát về việc sử dụng các biện pháp kiểm soát mật mã trên toàn tổ chức, bao gồm các nguyên tắc chung mà theo đó thông tin nghiệp vụ cần được bảo vệ;
- b) dựa trên quá trình đánh giá rủi ro, mức bảo vệ yêu cầu cần được xác định có lưu ý đến loại, năng lực và độ mạnh của thuật toán mật mã được yêu cầu;
- c) sử dụng mật mã để bảo vệ thông tin nhạy cảm được truyền bởi các thiết bị, phương tiện di động hoặc phương tiện có thể di dời, hoặc qua các đường truyền thông;
- d) phương thức quản lý khóa, bao gồm các phương pháp bảo vệ khóa mật mã và khôi phục thông tin đã được mã hóa trong trường hợp bị mất, bị tổn hại hoặc hỏng khóa;
- e) các vai trò và trách nhiệm, ví dụ ai phải chịu trách nhiệm về:
 - 1) triển khai chính sách;

2) quản lý khóa, bao gồm cả tạo khóa (xem 10.1.2);

- f) các tiêu chuẩn sẽ được chấp nhận để triển khai hiệu quả trên toàn tổ chức (giải pháp nào sẽ được sử dụng cho các quy trình nghiệp vụ nào);
- g) ảnh hưởng của việc sử dụng thông tin mã hóa lên các biện pháp kiểm soát liên quan đến điều tra nội dung (ví dụ phát hiện mã độc).

Khi triển khai chính sách mật mã của tổ chức thì cần quan tâm đến các quy định và những hạn chế của quốc gia có thể áp dụng cho việc sử dụng các kỹ thuật mật mã ở các khu vực khác nhau trên thế giới và áp dụng đối với các vấn đề về luồng thông tin mật mã qua biên giới giữa các quốc gia (xem 18.1.5).

Các biện pháp kiểm soát bằng mật mã có thể được sử dụng để đạt được các mục tiêu an toàn khác nhau, ví dụ:

- a) tính bí mật: sử dụng mật mã thông tin để bảo vệ thông tin nhạy cảm hoặc quan trọng khi lưu trữ hoặc truyền đi;
- b) tính toàn vẹn/tính xác thực: sử dụng chữ ký số hoặc mã xác thực thông điệp để bảo vệ tính xác thực và tính toàn vẹn của thông tin nhạy cảm hoặc quan trọng được lưu trữ hay truyền đi;
- c) chống chối bỏ: sử dụng kỹ thuật mật mã để cung cấp bằng chứng về sự có mặt hoặc không có mặt của một sự kiện hoặc một hoạt động;
- d) xác thực: sử dụng các kỹ thuật mật mã để xác thực người sử dụng và các tổ chức khác của hệ thống yêu cầu truy cập hoặc giao dịch với hệ thống người sử dụng, các thực thể và nguồn lực.

Thông tin khác

Việc đưa ra quyết định xem một giải pháp mật mã nào đó có phù hợp không cần được xem như là một phần của quá trình đánh giá rủi ro và lựa chọn biện pháp kiểm soát rộng hơn. Vì vậy, sự đánh giá này có thể được sử dụng để xác định xem một biện pháp kiểm soát mật mã có phù hợp không, loại biện pháp kiểm soát nào cần được sử dụng và được sử dụng cho mục đích và quá trình nghiệp vụ nào.

Một chính sách về việc sử dụng các biện pháp kiểm soát mật mã là cần thiết nhằm tối đa lợi ích và giảm thiểu rủi ro khi sử dụng kỹ thuật mật mã, và tránh việc sử dụng không chính xác hoặc không thích hợp.

Nên tìm tư vấn của các chuyên gia khi xác định kiểm soát mật mã thích hợp với các đối tượng trong chính sách an toàn thông tin.

10.1.2 Quản lý khóa

Kiểm soát

Một chính sách về sử dụng, bảo vệ và thời gian sống của các khóa mật mã cần được phát triển và thực hiện thông qua toàn bộ chu kỳ của chúng.

Hướng dẫn thi hành

Chính sách phải bao gồm các yêu cầu cho việc quản lý các khóa mật mã trong suốt toàn bộ chu kỳ của nó bao gồm tạo ra, cất giữ, lưu trữ, tìm kiếm, phân phối, hết hạn và phá hủy các khóa.

Các thuật toán mật mã, độ dài các khóa và sử dụng cần phải được lựa chọn áp dụng các thực hành tốt nhất. Quản lý khóa hợp lý đòi hỏi các quy trình an toàn để tạo ra, cất giữ, lưu trữ, tìm kiếm, phân phối, hết hạn và phá hủy các khóa.

Tất cả các khóa mật mã cần được bảo vệ nhằm khỏi sự sửa đổi, mất cắp và phá hoại. Hơn nữa, các khóa bí mật và khóa riêng cần được bảo vệ khỏi sự tiết lộ trái phép. Thiết bị được sử dụng để tạo, lưu trữ và lấy được các khóa cần được bảo vệ vật lý.

Hệ thống quản lý khóa phải dựa trên bộ các tiêu chuẩn, thủ tục, và phương thức an toàn đã được chấp thuận nhằm:

- a) tạo các khóa cho các hệ thống mật mã khác nhau và các ứng dụng khác nhau;
- b) tạo và nhận được các chứng thư khóa công khai;
- c) phát khóa tới những người dùng nhất định, bao gồm cả cách kích hoạt khóa khi nhận được khóa;
- d) lưu trữ khóa, bao gồm cả cách người dùng được phép đạt có thể truy cập tới các khóa;
- e) thay đổi hoặc cập nhật khóa bao gồm các nguyên tắc về thời gian phải đổi khóa và cách đổi khóa;
- f) xử lý các khóa bị xâm hại;
- g) thu hồi khóa bao gồm cách thu hồi hoặc làm vô hiệu khóa, ví dụ: khi khóa đã bị xâm phạm hoặc khi người dùng không làm việc cho tổ chức nữa (trường hợp nào khóa cần được lưu lại);
- h) khôi phục lại các khóa bị mất hoặc bị sửa đổi như một phần của việc quản lý tính liên tục của nghiệp vụ, ví dụ cho việc khôi phục thông tin đã được mật mã;
- i) lưu trữ các khóa, ví dụ cho thông tin đã được lưu trữ hoặc sao lưu;
- j) phá hủy khóa;
- k) ghi nhật ký và kiểm toán các hoạt động có liên quan đến việc quản lý khóa.

Để giảm khả năng xảy ra bị tổn hại thì ngày kích hoạt và giải kích hoạt các khóa cần được xác định sao cho các khóa có thể chỉ được sử dụng trong một khoảng thời gian giới hạn. Khoảng thời gian này phải tùy thuộc vào các trường hợp sử dụng biện pháp kiểm soát mã và các rủi ro được nhận biết.

Bên cạnh việc quản lý an toàn các khóa riêng và khóa bí mật thì cũng cần quan tâm đến tính xác thực của các khóa công khai. Quá trình xác thực có thể được thực hiện bằng cách sử dụng các chứng thư khóa công khai được phát hành bởi một cơ quan có thẩm quyền, cơ quan này phải là một tổ chức

được công nhận có các biện pháp và thủ tục quản lý phù hợp nhằm cung cấp mức độ tin cậy được yêu cầu.

Nội dung của các thỏa thuận hoặc hợp đồng về mức dịch vụ với những nhà cung cấp các dịch vụ mật mã bên ngoài, ví dụ với một tổ chức chứng thực, cần bao hàm các vấn đề về nghĩa vụ pháp lý, tính tin cậy của các dịch vụ và thời gian đáp ứng cung cấp dịch vụ (xem 15.2).

Thông tin khác

Việc quản lý các khóa mật mã là thiết yếu để sử dụng các kỹ thuật mật mã một cách hiệu quả. ISO/IEC 11770^[2][3][4] cung cấp thông tin sâu hơn về quản lý khóa.

Các kỹ thuật mật mã có thể còn được sử dụng để bảo vệ các khóa mật mã. Có thể còn cần các thủ tục để xử lý các yêu cầu pháp lý đối với truy cập tới các khóa mật mã, ví dụ thông tin mật mã có thể cần phải sẵn sàng ở dạng chưa được mã hóa với vai trò là bằng chứng trong các phiên tòa.

11 An toàn vật lý và môi trường

11.1 Các khu vực an toàn

Mục tiêu: Nhằm ngăn chặn sự truy cập vật lý trái phép, làm hư hại và can thiệp vào thông tin và các phương tiện xử lý thông tin của tổ chức.

11.1.1 Vành đai an toàn vật lý

Kiểm soát

Các vòng đai an toàn (như tường, cổng ra/vào có kiểm soát bằng thẻ hoặc bàn tiếp tân) phải được sử dụng để bảo vệ các khu vực chứa thông tin và phương tiện xử lý thông tin.

Hướng dẫn thi hành

Cần quan tâm và triển khai các hướng dẫn sau đối với vòng đai an toàn vật lý:

- a) các vòng đai an toàn cần được xác định rõ ràng, vị trí và chiều dài của mỗi hàng rào cần tùy thuộc vào các yêu cầu an toàn của các tài sản nằm ở khu vực bên trong hàng rào và các kết quả có được từ đánh giá rủi ro;
- b) các hàng rào của các tòa nhà hoặc các khu vực chứa các phương tiện xử lý thông tin cần vững chắc (tức là không được có lỗ hổng ở hàng rào và các khu vực dễ xảy ra đột nhập); các bức tường bên ngoài địa điểm đó cần có cấu trúc vững chãi và tất cả các cửa ra vào ở bên ngoài cần được bảo vệ bằng các cơ chế điều khiển, (ví dụ thanh chắn, chuông báo, khóa); cửa ra vào và cửa sổ cần được khóa khi không có người bên trong và cầm quan tâm bảo vệ bên ngoài các cửa sổ, đặc biệt tại tầng hầm;

- c) có thể thiết lập khu vực có người đón tiếp hoặc các hình thức quản lý truy cập vật lý tới tòa nhà hoặc địa điểm; cần giới hạn chỉ cho những người được cấp phép đi vào các địa điểm hoặc tòa nhà;
- d) nếu phù hợp thì cần sử dụng các thanh chắn vật lý chắc nhằm ngăn chặn xâm nhập trái phép và làm ô nhiễm môi trường;
- e) tắt cả các cửa chặn lửa (fire door) trên hàng rào an ninh cần được đặt còi báo động, được giám sát và kiểm tra cùng với các bức tường nhằm đạt được mức đảm bảo yêu cầu theo các tiêu chuẩn khu vực, quốc gia và quốc tế phù hợp; chúng cũng cần hoạt động tuân theo quy định báo cháy nội bộ theo phương thức dừng hoạt động nếu lỗi (failsafe);
- f) các hệ thống phát hiện xâm nhập cần được cài đặt theo các tiêu chuẩn quốc gia, khu vực hoặc quốc tế và thường xuyên được kiểm tra bao quát tất cả các cửa bên ngoài và các cửa sổ dễ xâm nhập; các khu vực bỏ trống cũng cần được đặt còi báo động ở mọi lúc; cần bao quát kiểm tra tất cả các khu vực khác, ví dụ phòng máy tính hoặc các phòng truyền thông;
- g) các phương tiện xử lý thông tin được quản lý bởi các tổ chức cần được đặt cách biệt khỏi các thiết bị được quản lý bởi bên thứ ba.

Thông tin khác

Có thể đạt được sự bảo vệ vật lý nếu thiết lập một hoặc nhiều thanh chắn xung quanh trụ sở và các phương tiện xử lý thông tin của tổ chức. Việc sử dụng nhiều thanh chắn sẽ làm tăng khả năng bảo vệ, vì sự cố ở một thanh chắn sẽ không có nghĩa là sẽ lập tức ảnh hưởng đến an toàn tài sản.

Một khu vực an toàn có thể là một văn phòng có khóa hoặc nhiều phòng được bao quanh bởi một thanh chắn liền. Có thể dùng thêm nhiều thanh chắn và hàng rào giữa các khu vực có các yêu cầu an toàn khác nhau nằm bên trong hàng rào an ninh nhằm quản lý xâm nhập. Cần quan tâm đặc biệt đến sự an toàn xâm nhập với các tòa nhà có nhiều tổ chức làm việc.

Việc áp dụng các kiểm soát vật lý, đặc biệt là các khu vực an toàn, cần thích ứng với tùy điều kiện về kỹ thuật và kinh tế của từng tổ chức, như được quy định trong đánh giá rủi ro.

11.1.2 Kiểm soát lỗi vào vật lý

Kiểm soát

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

Hướng dẫn thi hành

Cần quan tâm đến các hướng dẫn sau:

- a) ngày tháng và thời gian vào ra của khách cần được ghi lại, và cần giám sát tất cả những người khách trừ khi trước đây họ đã được chấp nhận cho vào; họ cần được chỉ dẫn các yêu cầu an toàn ở khu vực và các thủ tục khẩn cấp. Định danh của khách cần được xác thực một biện pháp thích hợp;
- b) truy cập đến các khu vực có các thông tin nhạy cảm được xử lý hoặc lưu trữ cần giới hạn với những người được phép bằng cách kiểm soát các truy cập thích hợp. Ví dụ bằng cách thực hiện một cơ chế xác thực hai yếu tố như một thẻ truy cập và PIN bí mật;
- c) một cuốn sách ghi lại lịch sử hoặc truy vết kiểm toán điện tử của tất cả các truy cập cần được duy trì và giám sát an toàn;
- d) tất cả các nhân viên, người của nhà thầu hoặc bên thứ ba và khách đến cần được yêu cầu mang một thẻ nhận dạng dễ nhìn thấy nào đó và phải lập tức thông báo cho nhân viên an ninh nếu họ trông thấy những khách đi một mình và những người không mang thẻ nhận dạng;
- e) tổ chức thứ ba cung cấp nhân viên phục vụ cũng chỉ được truy cập hạn chế đến các khu vực hoặc các phương tiện xử lý thông tin nhạy cảm khi có yêu cầu; truy cập này cần được cấp phép và giám sát;
- f) các quyền truy cập nhằm đảm bảo an toàn cho các khu vực cần được soát xét, cập nhật thường xuyên, và bị thu hồi khi cần thiết (xem 9.2.5 và 9.2.6).

11.1.3 Bảo vệ các văn phòng, phòng làm việc và vật dụng

Kiểm soát

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.

Hướng dẫn thi hành

Nhằm đảm bảo an toàn cho các văn phòng, phòng làm việc và vật dụng, cần quan tâm đến các hướng dẫn sau:

- a) các thiết bị quan trọng cần được đặt tại những vị trí tránh được sự truy cập công cộng;
- b) các tòa nhà cần được bài trí kín đáo và chỉ bộc lộ tối thiểu mục đích của chúng, cả phía ngoài và phía trong tòa nhà đều không có các dấu hiệu rõ ràng về sự hiện diện của các hoạt động xử lý thông tin;
- c) các thiết bị cần được cấu hình để ngăn chặn các thông tin hoặc hoạt động bí mật bị lọt ra ngoài. Sự che chắn điện tử được xem là phù hợp;
- d) các tài liệu hướng dẫn và các quyền danh bạ điện thoại nội bộ thể hiện vị trí của các phương tiện xử lý thông tin không nên ở các vị trí mà nhiều người trái phép dễ dàng lấy được.

11.1.4 Bảo vệ chống lại các mối đe dọa từ bên ngoài và từ môi trường

Kiểm soát

Biện pháp bảo vệ vật lý chống lại những thảm họa thiên nhiên, các cuộc tấn công mã độc hoặc sự cố cần được thiết kế và áp dụng.

Hướng dẫn thi hành

Chuyên gia tư vấn cho biết cần sử dụng cách nào để tránh thiệt hại do lũ lụt, động đất, cháy nổ, tình trạng bất ổn dân sự và các hình thức thảm họa tự nhiên và nhân tạo khác.

11.1.5 Làm việc trong các khu vực an toàn

Kiểm soát

Thủ tục làm việc trong các khu vực an toàn cần được thiết kế và áp dụng.

Hướng dẫn thi hành

Nhân viên làm việc chỉ cần biết đến các khu vực an toàn và các hoạt động ở trong khu vực này ở mức độ cần phải biết;

- a) vì các lý do an toàn và nhằm phòng tránh cơ hội cho các hoạt động có thể gây hại thì cần tránh làm việc mà không có giám sát trong các khu vực an toàn;
- b) các vùng an toàn còn trống cần được khóa cẩn thận và định kỳ kiểm tra;
- c) chụp ảnh, ghi hình, ghi âm hoặc các thiết bị ghi khác, như máy quay phim trong các thiết bị di động đều bị cấm, trừ khi được phép sử dụng.

Bố trí làm việc trong các khu vực an toàn phải bao gồm các biện pháp kiểm soát đối với nhân viên, người của nhà thầu hoặc bên thứ ba làm việc trong các khu vực an toàn, cũng như các hoạt động khác của tổ chức thứ ba thực hiện trong khu vực đó.

11.1.6 Các khu vực phân phối và tập kết hàng

Kiểm soát

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.

Hướng dẫn thi hành

Cần quan tâm đến những hướng dẫn sau:

- a) cần giới hạn chỉ cho những người đã xác định và đã được cho phép truy cập từ bên ngoài tòa nhà đến các khu vực phân phối và tập kết hàng;

- b) khu vực phân phối và tập kết hàng cần được thiết kế sao cho các nguồn hàng có thể được dỡ xuống mà nhân viên phân phối không phải tiếp cận đến các khu vực khác của tòa nhà;
- c) cần đảm bảo an toàn cho các cửa ra vào bên ngoài của khu vực phân phối và tập kết hàng khi các cửa bên trong đang mở;
- d) vật liệu đầu vào cần được kiểm tra các mối đe dọa tiềm ẩn trước khi vật liệu này được chuyển từ khu vực phân phối và tập kết hàng đến điểm sử dụng;
- e) vật liệu đầu vào cần được đăng ký theo các thủ tục quản lý tài sản (xem điều 8) ở lối vào khu vực đó;
- f) nếu có thể thì hàng vào và hàng ra cần đặt cách xa nhau;
- g) Vật liệu đầu vào cần làm rõ sự giả mạo ngay từ trên đường. Nếu phát hiện có sự giả mạo báo ngay cho nhân viên an ninh.

11.2 Đảm bảo an toàn trang thiết bị

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

11.2.1 Bố trí và bảo vệ thiết bị

Kiểm soát

Thiết bị phải được bố trí tại các địa điểm an toàn hoặc được bảo vệ nhằm giảm thiểu các rủi ro do các đe dọa, hiểm họa từ môi trường hay các truy cập trái phép.

Hướng dẫn thi hành

Nhằm bảo vệ thiết bị, cần quan tâm tới những hướng dẫn sau đây:

- a) cần lựa chọn vị trí đặt thiết bị nhằm giảm thiểu truy cập không cần thiết vào các khu vực làm việc;
- b) các phương tiện xử lý thông tin thực hiện công việc xử lý dữ liệu nhạy cảm cũng cần được bố trí vị trí đặt và được đặt ở góc quan sát hạn chế nhằm giảm rủi ro thông tin bị quan sát bởi các cá nhân không được phép, và các thiết bị lưu trữ được an toàn nhằm tránh truy cập trái phép;
- c) Các cơ sở lưu trữ cần được bảo vệ tránh truy cập trái phép;
- d) các thiết bị yêu cầu bảo vệ đặc biệt cần được đặt riêng nhằm giảm mức độ yêu cầu bảo vệ chung;
- e) cần thực hiện các biện pháp kiểm soát nhằm giảm thiểu rủi ro do các mối đe dọa vật lý tiềm ẩn, ví dụ đánh cắp, cháy, nổ, khói, nước (hoặc hỏng nguồn cung cấp nước), bụi, chấn động, các ảnh hưởng của hóa chất, nhiều nguồn điện; nhiều truyền thông, phát xạ điện tử, và các hành động phá hoại;

- f) phải thiết lập các hướng dẫn đối với việc ăn, uống, và hút thuốc ở khu vực lân cận các phương tiện xử lý thông tin;
- g) các điều kiện môi trường, như nhiệt độ và độ ẩm, cũng cần được giám sát, vì chúng có thể ảnh hưởng bất lợi đến các phương tiện xử lý thông tin;
- h) cần sử dụng các biện pháp chống sét cho tất cả các toàn nhà và các bộ lọc sét sử dụng cần phù hợp với tất cả các đường dây thông tin và đường dây cấp nguồn;
- i) cần quan tâm đến việc sử dụng các biện pháp bảo vệ đặc biệt, ví dụ keyboard membrane, đối với các thiết bị sử dụng trong các môi trường công nghiệp;
- j) cần bảo vệ phương tiện xử lý thông tin nhạy cảm nhằm giảm thiểu rủi ro rò rỉ thông tin do sự phát xạ điện tử.

11.2.2 Các tiện ích hỗ trợ

Kiểm soát

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

Hướng dẫn thi hành

Hỗ trợ các tiện ích (ví dụ như điện, viễn thông, cấp nước, khí đốt, nước thải, hệ thống thông gió và điều hòa không khí) cần:

- a) phù hợp với thông số kỹ thuật của nhà sản xuất thiết bị và các yêu cầu pháp lý của địa phương;
- b) thường xuyên thẩm định khả năng của chúng nhằm đáp ứng sự phát triển nghiệp vụ và tương tác với các tiện ích hỗ trợ khác;
- c) kiểm tra và thường xuyên kiểm tra nhằm đảm bảo sự hoạt động chính xác;
- d) nếu cần thiết, cần báo động khi phát hiện trực trặc;
- e) nếu cần thiết, có nhiều nguồn cung cấp với tuyển vật lý đa dạng.

Cần cung cấp hệ thống chiếu sáng và thông tin liên lạc khẩn cấp khi cần. Công tắc khẩn cấp và van để cắt điện nước, ga hoặc các tiện ích khác cần đặt gần lối thoát hiểm khẩn cấp hoặc phòng thiết bị.

Thông tin khác

Bổ sung các kết nối mạng dự phòng bằng nhiều đường truyền từ nhà cung cấp hơn là cung cấp từ một nhà cung cấp dịch vụ tiện ích.

11.2.3 An toàn cho dây cáp

Kiểm soát

Dây dẫn nguồn điện và cáp truyền thông mang dữ liệu hoặc các hỗ trợ các dịch vụ thông tin cần được bảo vệ khỏi sự xâm phạm hoặc làm hư hại.

Hướng dẫn thi hành

Cần quan tâm tới các hướng dẫn sau:

- a) các đường dây điện và đường cáp viễn thông dẫn tới các phương tiện xử lý thông tin nếu có thể cần được đặt ngầm, hoặc được bảo vệ theo phương thức phù hợp;
- b) cần tách riêng đường cáp điện và đường cáp viễn thông nhằm ngăn chặn nhiễu;
- c) cần sử dụng cách đánh dấu dễ nhận biết cho cáp và thiết bị nhằm giảm thiểu các lỗi khi sửa chữa, ví dụ như vô tình đấu sai đường cáp mạng;
- d) cần sử dụng tài liệu danh sách đấu nối nhằm làm giảm khả năng xảy ra lỗi;
- e) đối với các hệ thống nhạy cảm hoặc quan trọng, cần quan tâm đến các biện pháp khác như:
 - 1) lắp đặt ống dẫn bằng cốt sắt và sử dụng các phòng hoặc hộp có khóa tại các điểm kết cuối và điểm có nghi ngờ;
 - 2) sử dụng các tuyến cáp và/hoặc môi trường truyền dẫn khác nhau nhằm đảm bảo độ an toàn;
 - 3) kiểm tra kỹ thuật và rà soát vật lý đối với các thiết bị trái phép được gắn vào đường cáp;
 - 4) quản lý truy cập tới các bảng điều khiển và các buồng cáp.

11.2.4 Bảo dưỡng thiết bị

Kiểm soát

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

Hướng dẫn thi hành

Cần quan tâm tới các hướng dẫn sau trong việc bảo dưỡng thiết bị:

- a) thiết bị cần được bảo dưỡng tuân theo các chu kỳ bảo dưỡng và các chỉ tiêu kỹ thuật dịch vụ được nhà cung cấp khuyến nghị;
- b) chỉ người bảo dưỡng được cấp phép mới được thực hiện các công việc sửa chữa và bảo dưỡng thiết bị;
- c) cần giữ lại các báo cáo về các lỗi thực sự hoặc lỗi khả nghi, và toàn bộ quá trình bảo dưỡng phòng ngừa và bảo dưỡng khắc phục;
- d) cần triển khai các biện pháp kiểm soát phù hợp khi thiết bị được lập lịch cho bảo trì, trong đó cần quan tâm xem nhân viên bảo trì là người thuộc tổ chức hay ngoài tổ chức; khi cần thiết thi thông tin nhạy cảm cần bị xóa khỏi thiết bị, hoặc nhân viên bảo dưỡng cần được giải thích rõ ràng;

- e) cần tuân thủ tất cả các yêu cầu được áp dụng bởi các chính sách bảo hiểm.
- f) trước khi đưa thiết bị trở lại sau hoạt động bảo trì, thiết bị cần được kiểm tra để đảm bảo không bị giả mạo và không bị hỏng.

11.2.5 An toàn khi di chuyển thiết bị

Kiểm soát

Trang thiết bị, thông tin hoặc phần mềm không được mang ra ngoài khu vực mà không được sự cho phép trước.

Hướng dẫn thi hành

Cần quan tâm đến những hướng dẫn sau:

- a) cần xác định thẩm quyền của nhân viên và những người sử dụng bên ngoài khi di chuyển thiết bị bên ngoài;
- b) cần thiết lập thời gian di chuyển và trả về thiết bị phù hợp;
- c) cần ghi nhận khi thiết bị di chuyển bên ngoài và khi mang trở về, điều này là thích hợp và cần thiết;
- d) danh tính, vai trò và liên kết của người xử lý hoặc sử dụng các tài sản phải được lập hồ sơ và hồ sơ này phải bao gồm các thiết bị, thông tin hoặc phần mềm.

Thông tin khác

Kiểm tra tại chỗ, phát hiện loại bỏ các thiết bị trái phép, cũng có thể thực hiện để phát hiện các thiết bị ghi âm trái phép, vũ khí... và để ngăn chặn chúng được mang vào hay ra khỏi khu vực. Kiểm tra đột xuất như vậy cần được thực hiện phù hợp với pháp luật cũng như các quy định liên quan. Các cá nhân cần phải nhận thức được rằng việc kiểm tra đột xuất cũng như xác minh chỉ cần được thực hiện với sự cho phép của pháp luật cũng như các quy định.

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

Kiểm soát

Phải đảm bảo an toàn cho các thiết bị sử dụng bên ngoài, tính đến các rủi ro khác nhau khi thiết bị làm việc bên ngoài trụ sở của tổ chức.

Hướng dẫn thi hành

Việc sử dụng thiết bị lưu trữ và xử lý thông tin bên ngoài trụ sở của tổ chức cần được cấp phép bởi ban lãnh đạo. Điều này áp dụng cho thiết bị do tổ chức sở hữu và thiết bị do cá nhân sở hữu được sử dụng nhân danh tổ chức.

Cần quan tâm đến các hướng dẫn sau để bảo vệ các thiết bị sử dụng bên ngoài trụ sở:

- a) thiết bị và phương tiện khi mang ra ngoài trụ sở không được bỏ quên theo dõi ở nơi công cộng;
- b) luôn luôn thực thi các hướng dẫn bảo vệ thiết bị của nhà sản xuất, ví dụ bảo vệ khỏi phơi nhiễm các trường điện từ mạnh;
- c) các biện pháp kiểm soát khi làm việc ở các vị trí bên ngoài tổ chức chẳng hạn như làm việc tại nhà, làm việc từ xa và những vị trí tạm thời cần được xác định qua đánh giá rủi ro và áp dụng các biện pháp kiểm soát phù hợp, ví dụ các tủ hồ sơ có khóa, chính sách bàn làm việc sạch, quản lý truy cập máy tính và truyền thông an toàn với văn phòng (xem thêm ISO/IEC 27033 [15] [16] [17] [18] [19]);
- d) khi thiết bị sử dụng bên ngoài được chuyển giao giữa các cá nhân hoặc các đối tác bên ngoài, cần phải thường xuyên ghi nhật ký để có chuỗi giám sát thiết bị bao gồm ít nhất là tên và tổ chức của những người chịu trách nhiệm về thiết bị.

Các rủi ro về an toàn, ví dụ hư hại, trộm cắp hoặc nghe trộm, có thể khác nhau tùy theo địa điểm và cần được quan tâm xem xét khi xác định các biện pháp kiểm soát phù hợp nhất.

Thông tin khác

Thiết bị lưu trữ và xử lý thông tin bao gồm tất cả các loại máy tính cá nhân, các loại điện thoại di động, thẻ thông minh, giấy tờ hoặc các hình thức khác được sử dụng khi làm việc tại nhà hoặc được mang ra ngoài vị trí làm việc thông thường.

Để tìm hiểu thêm về những khía cạnh khác của quá trình bảo vệ thiết bị di động, xem [6.2](#).

Để tránh rủi ro, tốt nhất là không khuyến khích nhân viên làm việc bên ngoài hoặc hạn chế sử dụng thiết bị công nghệ thông tin xách tay.

11.2.7 Xử lý khi loại bỏ hoặc tái sử dụng thiết bị

Kiểm soát

Tất cả các hạng mục của thiết bị có chứa phương tiện lưu trữ cần được xác nhận để đảm bảo an toàn rằng bất kỳ dữ liệu nhạy cảm và phần mềm có bản quyền đã bị xóa hoặc ghi đè trước khi hủy bỏ hoặc tái sử dụng.

Hướng dẫn thi hành

Thiết bị cần được đảm bảo xác nhận có chứa phương tiện lưu trữ trước khi xử lý hay tái sử dụng. Phương tiện lưu trữ có chứa thông tin bí mật hoặc có bản quyền cần phá hủy bằng phương pháp vật lý hoặc thông tin cần được phá hủy, xóa hoặc ghi đè sử dụng các kỹ thuật làm cho các tổ chức thông tin không thể được phục hồi hơn là sử dụng xóa chuẩn hoặc các chức năng định dạng.

Thông tin khác

Các thiết bị chứa phương tiện lưu trữ bị hư hỏng có thể yêu cầu đánh giá rủi ro để xác định xem các hạng mục được phá hủy kiểu vật lý hơn là gửi sửa chữa hay loại bỏ. Thông tin có thể bị xâm phạm qua

việc xử lý bắt cần hoặc tái sử dụng thiết bị. Ngoài ra để đảm bảo đĩa được tẩy xóa, mật mã toàn bộ đĩa làm giảm nguy cơ lộ thông tin bí mật khi thiết bị đã bị loại bỏ hay tái sử dụng, với điều kiện:

- a) tiến trình mật mã phải đủ mạnh và bao gồm toàn bộ đĩa (bao gồm không gian chung, các tập tin trao đổi,...);
- b) khóa mật mã đủ dài để chống lại các cuộc tấn công;
- c) bản thân khóa mật mã phải được giữ bí mật (ví dụ như không bao giờ được lưu trữ trên cùng một đĩa).

Để được tư vấn thêm về mật mã (xem điều 10).

Kỹ thuật để ghi đè an toàn các phương tiện lưu trữ khác nhau sẽ theo những kỹ thuật phương tiện lưu trữ khác nhau. Công cụ ghi đè cần được soát xét để đảm bảo rằng chúng có thể áp dụng cho công nghệ của phương tiện lưu trữ.

11.2.8 Thiết bị người dùng không giám sát

Kiểm soát

Người dùng cần đảm bảo rằng thiết bị không giám sát phải có bảo mật thích hợp.

Hướng dẫn thi hành

Tất cả người dùng cần phải nhận thức được yêu cầu an toàn và các thủ tục bảo vệ thiết bị không giám sát, cũng như trách nhiệm của mình trong việc thực hiện bảo vệ. Người dùng phải được hướng dẫn:

- a) kết thúc hoạt động của phiên làm việc khi hoàn thành, trừ khi họ có thể đảm bảo được có một cơ chế khóa thích hợp, ví dụ như mật khẩu an toàn trên màn hình chờ;
- b) thoát ra khỏi các ứng dụng hoặc dịch vụ mạng khi không cần;
- c) bảo đảm an toàn các máy tính hoặc thiết bị di động khỏi các hành động sử dụng trái phép bằng khóa hoặc một kiểm soát tương đương, ví dụ mật khẩu truy cập, khi không sử dụng.

11.2.9 Chính sách màn hình sạch và bàn làm việc sạch

Kiểm soát

Chính sách bàn làm việc sạch không có giấy và các phương tiện lưu trữ di động và chính sách màn hình sạch cho các phương tiện xử lý thông tin phải được thực hiện.

Hướng dẫn thi hành

Chính sách màn hình sạch và bàn làm việc sạch cần lưu ý đến việc phân loại thông tin (xem 7.2), các yêu cầu pháp lý và yêu cầu hợp đồng (xem 15.1), các rủi ro tương ứng và các khía cạnh văn hóa của tổ chức. Những hướng dẫn sau đây cần được quan tâm:

- a) thông tin nghiệp vụ quan trọng hoặc nhạy cảm, ví dụ trên giấy tờ hay trên các thiết bị lưu trữ điện tử, cần được khóa lại (lý tưởng là được giữ trong két sắt, tủ hoặc các phương tiện an toàn khác) khi không cần dùng tới, đặc biệt là khi phòng làm việc bị bỏ trống;
- b) máy tính và các thiết bị đầu cuối cần được thoát hoặc được bảo vệ bằng màn hình bảo vệ hoặc cơ chế khóa bàn phím bằng mật khẩu, thẻ hoặc cơ chế xác thực người dùng tương tự khi không sử dụng nữa;
- c) việc sử dụng trái phép các máy chụp và các kỹ thuật sao chép khác (ví dụ các máy quét, máy ảnh kỹ thuật số) phải được ngăn chặn;
- d) các thiết bị đa phương tiện chứa thông tin nhạy cảm hay thông tin đã được phân loại cần được lấy khỏi máy in ngay lập tức.

Thông tin khác

Chính sách màn hình/bàn làm việc sạch sẽ giảm thiểu các rủi ro do truy cập trái phép, mất cắp, và hư hại thông tin trong và ngoài giờ làm việc. Các két sắt hay các phương tiện chứa an toàn khác cũng có thể bảo vệ thông tin trước các thảm họa như cháy nổ, động đất, lụt lội.

Cần quan tâm sử dụng các máy in có chức năng mã pin, khi đó chỉ những người được phép sử dụng mới có thể nhận các bản in của họ, và chỉ khi họ đứng cạnh máy in.

12 An toàn vận hành

12.1 Thủ tục và trách nhiệm vận hành

Mục tiêu: Nhằm đảm bảo sự thao tác các phương tiện xử lý thông tin đúng đắn và an toàn.

12.1.1 Các thủ tục vận hành được lập tài liệu

Kiểm soát

Các thủ tục vận hành cần được lập tài liệu, duy trì, và luôn sẵn sàng đối với mọi người cần dùng đến.

Hướng dẫn thi hành

Cần chuẩn bị các tài liệu thủ tục cho các hoạt động hệ thống có liên quan đến các thiết bị trao đổi và xử lý thông tin, ví dụ các thủ tục khởi động và tắt máy tính, sao lưu, bảo dưỡng thiết bị, điều khiển thiết bị, vấn đề an toàn và quản lý thư từ và phòng máy tính,

Các thủ tục khai thác cần đưa ra các hướng dẫn thực hiện chi tiết từng công việc gồm:

- a) Cài đặt và cấu hình các hệ thống;
- b) chế biến và xử lý thông tin cả hai cách tự động và thủ công;
- c) sao lưu (xem 12.3);

- d) lên lịch cho các yêu cầu, bao gồm sự phụ thuộc với các hệ thống khác, các thời điểm bắt đầu công việc sớm nhất và các thời điểm kết thúc công việc muộn nhất;
- e) các hướng dẫn xử lý các sự cố hoặc các điều kiện ngoại lệ khác, những vấn đề này có thể xuất hiện trong khi thực hiện công việc, bao gồm các giới hạn sử dụng các tiện ích của hệ thống (xem 9.4.4);
- f) hỗ trợ liên lạc trong các trường hợp có trở ngại không mong muốn về khai thác hoặc kỹ thuật;
- g) các hướng dẫn xử lý thiết bị và đầu ra đặc biệt, như sử dụng đồ dùng văn phòng đặc biệt hoặc quản lý đầu ra bảo mật bao gồm các thủ tục loại bỏ một cách an toàn đầu ra từ các công việc bị lỗi (xem 8.3 và 11.2.7);
- h) các thủ tục khởi động và khôi phục hệ thống trong trường hợp có lỗi hệ thống;
- i) quản lý tìm vết và thông tin nhật ký của hệ thống (xem 12.4);
- j) các thủ tục giám sát.

Các thủ tục vận hành và các thủ tục được lập thành tài liệu cho các hoạt động của hệ thống cần được coi như các tài liệu chính thức và được cấp phép thay đổi bởi ban lãnh đạo. Nếu điều kiện kỹ thuật cho phép thì các hệ thống thông tin cần được quản lý liên tục bằng các thủ tục, công cụ và các tiện ích giống nhau.

12.1.2 Quản lý thay đổi

Kiểm soát

Các thay đổi đối với tổ chức, quy trình nghiệp vụ, các phương tiện và hệ thống xử lý thông tin có ảnh hưởng đến an toàn thông tin phải được kiểm soát.

Hướng dẫn thi hành

Đặc biệt, các mục sau đây cần được soát xét:

- a) định danh và ghi lại các thay đổi lớn;
- b) lập kế hoạch và kiểm tra các thay đổi;
- c) đánh giá các tác động tiềm năng, bao gồm cả tác động an toàn thông tin của những thay đổi đó;
- d) thủ tục phê duyệt chính thức cho các đề nghị thay đổi;
- e) xác minh rằng các yêu cầu an toàn thông tin đã được đáp ứng;
- f) thông báo chi tiết các thay đổi đến tất cả những người có liên quan;
- g) các thủ tục thu hồi, bao gồm cả thủ tục và trách nhiệm hủy bỏ và phục hồi từ những thay đổi không thành công và sự kiện bất khả kháng;

h) cung cấp một quy trình thay đổi khẩn cấp để cho phép thực hiện nhanh chóng và kiểm soát các thay đổi cần thiết để giải quyết một vụ việc (xem 16.1).

Các thủ tục và trách nhiệm quản lý chính thức cần phải được thực hiện đúng lúc để đảm bảo kiểm soát thỏa đáng tất cả thay đổi. Khi có thay đổi, một nhật ký kiểm toán có chứa tất cả các thông tin có liên quan cần được giữ lại.

Thông tin khác

Kiểm soát không đầy đủ các thay đổi đối với các thiết bị xử lý thông tin và hệ thống là một nguyên nhân phổ biến của thất bại kiểm soát an toàn thông tin. Những thay đổi trong môi trường hoạt động, đặc biệt là khi chuyển một hệ thống từ phát triển đến giai đoạn vận hành, có thể ảnh hưởng đến độ tin cậy của các ứng dụng (xem 14.2.2).

12.1.3 Quản lý năng lực

Kiểm soát

Việc sử dụng các nguồn tài nguyên cần được theo dõi, điều chỉnh và thực hiện dự báo các yêu cầu năng lực trong tương lai để đảm bảo hiệu quả vận hành hệ thống.

Hướng dẫn thi hành

Yêu cầu năng lực cần được xác định, có tính đến tính các nghiệp vụ quan trọng của hệ thống liên quan. Hệ thống điều chỉnh và giám sát cần được áp dụng để đảm bảo khi cần thiết, cải tiến được tính sẵn sàng và hiệu quả của hệ thống. Các kiểm soát phát hiện cần được đặt đúng chỗ để chỉ ra các vấn đề đúng thời điểm. Dự báo các yêu cầu năng lực trong tương lai cần tính đến các nghiệp vụ mới và yêu cầu hệ thống và xét đến xu hướng hiện tại và tương lai trong khả năng xử lý thông tin của tổ chức.

Chú ý đặc biệt cần phải được áp dụng cho bất kỳ tài nguyên nào có thủ tục mua sắm dài hoặc chi phí cao; do đó các nhà quản lý cần theo dõi việc tận dụng tài nguyên hệ thống quan trọng. Họ cần xác định xu hướng sử dụng, đặc biệt liên quan đến các ứng dụng nghiệp vụ hoặc các công cụ quản lý hệ thống thông tin.

Các nhà quản lý cần sử dụng các thông tin này để xác định và tránh các điểm nghẽn tiềm tàng và sự phụ thuộc vào cán bộ chủ chốt có thể thể hiện một mối đe dọa cho an toàn hệ thống hoặc dịch vụ, và có kế hoạch hành động thích hợp.

Việc cung cấp đầy đủ năng lực có thể đạt được bằng cách tăng dung lượng hoặc giảm nhu cầu. Ví dụ quản lý nhu cầu năng lực bao gồm:

- a) xóa bỏ các dữ liệu (không gian đĩa) cũ;
- b) ngừng hoạt động các ứng dụng, hệ thống, cơ sở dữ liệu hoặc các môi trường;
- c) tối ưu hóa các tập quy trình và tiến độ;

- d) tối ưu hóa logic ứng dụng hoặc các truy vấn cơ sở dữ liệu;
- e) từ chối hoặc hạn chế băng thông cho các dịch vụ thiếu tài nguyên nếu đây không phải là nghiệp vụ quan trọng (ví dụ: video streaming).

Một tài liệu về kế hoạch quản lý năng lực cần được xây dựng cho các hệ thống mang nhiệm vụ quan trọng.

Thông tin khác

Kiểm soát này cũng đề cập đến năng lực của nguồn nhân lực, cũng như các văn phòng và các trang thiết bị.

12.1.4 Phân tách các chức năng phát triển, kiểm thử và môi trường vận hành

Kiểm soát

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

Hướng dẫn thi hành

Cần xác định mức độ phân tách giữa các môi trường vận hành, kiểm thử và phát triển cần cho việc phòng chống các sự cố về khai thác và thực thi các biện pháp kiểm soát thích hợp.

Cần quan tâm đến các vấn đề sau:

- a) các quy tắc chuyển đổi phần mềm từ trạng thái phát triển sang khai thác cần được xác định và lập thành tài liệu;
- b) phần mềm phát triển và vận hành cần chạy trên các hệ thống hoặc các bộ xử lý máy tính khác nhau và nằm trong các thư mục miền khác nhau;
- c) thay đổi đối với hệ thống vận hành và các ứng dụng cần phải được thử nghiệm trong một môi trường thử nghiệm hoặc dàn dựng trước khi được áp dụng cho hệ thống vận hành;
- d) trừ trường hợp ngoại lệ, thử nghiệm không cần được thực hiện trên hệ thống đang vận hành;
- e) nếu không có yêu cầu thì các trình biên dịch, trình biên soạn, công cụ phát triển và các tiện ích hệ thống không thể truy cập được vào các hệ thống vận hành;
- f) người dùng cần sử dụng các bản khai lý lịch người dùng khác nhau cho các hệ thống thử nghiệm và vận hành, và các tùy chọn trong bản khai cũng cần hiển thị các thông tin nhận dạng phù hợp nhằm giảm rủi ro mắc lỗi;
- g) Không được sao chép dữ liệu nhạy cảm vào môi trường hệ thống thử nghiệm trừ khi các kiểm soát tương đương được áp dụng cho các hệ thống thử nghiệm (xem 14.3).

Thông tin khác

Các hoạt động phát triển và thử nghiệm có thể gây ra các vấn đề nghiêm trọng, ví dụ làm sửa đổi không mong muốn các tệp hoặc môi trường hệ thống, hoặc gây ra sự cố hệ thống. Trong trường hợp này, cần duy trì một môi trường ổn định nhằm có thể thực hiện thử nghiệm theo mục đích và ngăn chặn truy cập không phù hợp.

Khi nhân viên phát triển và nhân viên thử nghiệm truy cập vào hệ thống điều hành và các thông tin của nó thì họ có khả năng đưa vào mã trái phép và chưa được kiểm tra hoặc làm thay đổi dữ liệu hoạt động. Ở một số hệ thống, khả năng này có thể bị lợi dụng nhằm gian lận, hoặc đưa vào mã chưa được kiểm tra hoặc độc hại, và gây ra các sự cố nghiêm trọng.

Các nhân viên phát triển và thử nghiệm cũng có mối đe dọa tới độ tin cậy của thông tin khai thác. Các hoạt động thử nghiệm và phát triển có thể gây ra những thay đổi không định trước đối với phần mềm hoặc thông tin nếu họ cùng chia sẻ môi trường hoạt động máy tính. Việc phân tách các thiết bị hỗ trợ phát triển, thử nghiệm và vận hành do vậy rất cần thiết trong việc giảm rủi ro do vô tình thay đổi hoặc truy cập trái phép tới phần mềm khai thác và dữ liệu nghiệp vụ ([xem 14.3](#) về vấn đề bảo vệ dữ liệu kiểm tra).

12.2 Bảo vệ khỏi phần mềm độc hại

Mục tiêu: Để đảm bảo rằng các thông tin và hệ thống xử lý thông tin được bảo vệ chống lại phần mềm độc hại.

12.2.1 Kiểm soát chống lại phần mềm độc hại

Kiểm soát

Phát hiện, phòng ngừa và phục hồi quyền điều khiển để bảo vệ chống lại phần mềm độc hại cần được thực hiện, kết hợp với nhận thức đúng đắn của người sử dụng.

Hướng dẫn thi hành

Bảo vệ chống lại phần mềm độc hại dựa trên sự phát hiện phần mềm độc hại và sửa chữa phần mềm, nhận thức về an toàn thông tin, truy cập hệ thống thích hợp và việc quản lý thay đổi có kiểm soát. Các hướng dẫn sau đây cần được soát xét:

- a) thiết lập một chính sách chính thức ngăn cản việc sử dụng phần mềm trái phép ([xem 12.6.2](#) và [14.2](#));
- b) thực hiện các kiểm soát ngăn ngừa hoặc phát hiện sử dụng phần mềm trái phép (ví dụ như sử dụng danh sách trắng);
- c) thực hiện các kiểm soát ngăn ngừa hoặc phát hiện việc sử dụng các trang web độc hại đã được biết đến hoặc nghi ngờ (ví dụ: danh sách đen);

- d) thiết lập một chính sách chính thức nhằm bảo vệ chống lại các rủi ro liên quan đến việc sử dụng các tập tin và phần mềm đến từ hoặc đi qua các mạng bên ngoài, hoặc bất kỳ môi trường nào khác, chỉ ra các biện pháp bảo vệ cần thực hiện;
- e) giảm các lỗ hổng mà có thể bị khai thác bởi phần mềm độc hại, ví dụ như thông qua các quản lý lỗ hổng kỹ thuật;
- f) tiến hành đánh giá thường xuyên các phần mềm và nội dung dữ liệu của hệ thống hỗ trợ quy trình nghiệp vụ quan trọng; sự hiện diện của bất kỳ tập tin nào không được chấp thuận hoặc bị sửa đổi trái phép cần được chính thức điều tra;
- g) cài đặt và cập nhật thường xuyên bộ phát hiện phần mềm độc hại và sửa chữa phần mềm nhằm quét máy tính và phương tiện lưu trữ thông tin như một biện pháp phòng ngừa, hoặc trên cơ sở định kỳ; việc quét được thực hiện bao gồm:
 - 1) quét bất kỳ tập tin nhận qua mạng hoặc nhận qua bất kỳ loại hình phương tiện lưu trữ nào, nhằm phát hiện phần mềm độc hại trước khi sử dụng;
 - 2) quét tệp đính kèm thư điện tử và các tệp tải về nhằm phát hiện phần mềm độc hại trước khi sử dụng; việc quét này cần được thực hiện tại nhiều nơi khác nhau, ví dụ tại máy chủ thư điện tử, máy tính để bàn và khi đăng nhập vào mạng của tổ chức;
 - 3) quét phần mềm độc hại trên các trang web;
- h) xác định thủ tục và trách nhiệm để đối phó với phần mềm độc hại trên hệ thống, đào tạo việc sử dụng, báo cáo và phục hồi sau các cuộc tấn công của phần mềm độc hại;
- i) chuẩn bị kế hoạch nghiệp vụ liên tục thích hợp để phục hồi sau các cuộc tấn công của phần mềm độc hại, bao gồm tất cả dữ liệu cần thiết, phần mềm sao lưu và các sáp xếp phục hồi ([xem 12.3](#));
- j) Thực hiện các thủ tục để thường thu thập thông tin, chẳng hạn như đăng ký vào danh sách gửi thư hoặc kiểm tra các trang web cung cấp thông tin về phần mềm độc hại mới;
- k) Thực hiện các thủ tục để xác minh các thông tin liên quan đến phần mềm độc hại, và đảm bảo rằng các bản tin cảnh báo là chính xác và đầy đủ thông tin; các nhà quản lý phải đảm bảo rằng các nguồn thông tin có chất lượng, ví dụ như các tạp chí uy tín, các trang web Internet đáng tin cậy hay các nhà cung cấp, sẵn xuất phần mềm bảo vệ chống lại phần mềm độc hại, đã được sử dụng để phân biệt, không nhầm lẫn giữa thông tin giả và phần mềm độc hại thật; tất cả người sử dụng cần được nhận thức rõ vấn đề của thông tin giả và phải làm gì khi nhận được thông tin giả;
- l) cô lập vùng quan trọng, nơi tác động thảm khốc có thể xảy ra.

Thông tin khác

Sử dụng hai hoặc nhiều hơn các sản phẩm phần mềm bảo vệ chống lại phần mềm độc hại trên môi trường xử lý thông tin từ các nhà cung cấp và sử dụng các công nghệ khác nhau có thể nâng cao hiệu quả bảo vệ chống lại phần mềm độc hại.

Chú ý cẩn thận để bảo vệ chống lại sự xâm nhập của phần mềm độc hại trong quá trình bảo dưỡng và thực hiện thủ tục cứu hộ, các trường hợp có thể bỏ qua các điều kiện bảo vệ phần mềm độc hại thông thường.

Dưới những điều kiện nhất định, việc bảo vệ chống phần mềm độc hại có thể gây ra sự xáo trộn trong hoạt động.

Sử dụng công cụ phát hiện phần mềm độc hại và sửa chữa phần mềm riêng biệt như một công cụ kiểm soát phần mềm độc hại thường không đầy đủ và thường cần phải được đi kèm với các thủ tục giúp ngăn chặn việc tạo điều kiện cho các phần mềm độc hại hoạt động.

12.3 Sao lưu

Mục tiêu: để bảo vệ dữ liệu, chống lại sự mất mát dữ liệu.

12.3.1 Thông tin sao lưu

Kiểm soát

Bản sao lưu các thông tin, phần mềm và hình ảnh hệ thống phải được thực hiện và kiểm tra thường xuyên nhằm đảm bảo phù hợp với chính sách sao lưu của tổ chức, đơn vị.

Hướng dẫn thi hành

Một chính sách sao lưu cần được xây dựng để xác định các yêu cầu, chính sách sao lưu của tổ chức phù hợp với hoạt động và tổ chức bộ máy của tổ chức đó. Chính sách sao lưu nhằm sao lưu các thông tin, dữ liệu, phần mềm và hệ thống.

Các chính sách sao lưu cần xác định các yêu cầu lưu giữ và bảo vệ.

Các phương tiện sao lưu cần được cung cấp tương ứng để đảm bảo rằng tất cả các thông tin và phần mềm thiết yếu nhất, cần thiết nhất có thể được phục hồi sau một sự cố, thảm họa hoặc lỗi của phương tiện truyền thông tin.

Khi thiết kế một kế hoạch sao lưu, các nội dung sau đây cần được xem xét:

- a) tính chính xác và tính đầy đủ của các bản sao lưu và thủ tục phục hồi phải được thiết lập dưới dạng văn bản;
- b) mức độ mở rộng (ví dụ sao lưu đầy đủ hoặc sao lưu bộ phận) và tần suất của các bản sao lưu cần phản ánh các yêu cầu hoạt động của tổ chức, các yêu cầu an toàn của các thông tin có liên quan và mức độ quan trọng của các thông tin để tiếp tục vận hành tổ chức;

- c) các bản sao lưu sẽ được lưu trữ trong một vị trí từ xa, ở một khoảng cách đủ để thoát khỏi bất kỳ thiệt hại nào từ một thảm họa xảy ra tại hệ thống chính;
- d) Các thông tin sao lưu cần được cung cấp một mức độ bảo vệ thích hợp về mặt vật lý và môi trường đảm bảo phù hợp với các tiêu chuẩn áp dụng tại hệ thống chính;
- e) phương tiện sao lưu cần được thường xuyên kiểm tra để đảm bảo rằng chúng có thể được đưa vào sử dụng khẩn cấp khi cần thiết; điều này cần được kết hợp với một bài kiểm tra của các thủ tục phục hồi và kiểm tra so với thời gian khôi phục cần thiết. Kiểm tra khả năng khôi phục dữ liệu sao lưu cần thực hiện trên phương tiện kiểm tra chuyên dụng, không ghi đè các phương tiện thông tin ban đầu, dự phòng cho trường hợp quá trình sao lưu hoặc phục hồi không thành công và gây ra mất mát hoặc hư hỏng dữ liệu không thể khắc phục;
- f) trong các tình huống mà sự bí mật là quan trọng, sao lưu cần được bảo vệ bằng phương tiện mật mã.

Thủ tục vận hành cần theo dõi việc thực hiện các bản sao lưu và giải quyết các thất bại trong sao lưu theo lịch trình để đảm bảo lưu đầy đủ các bản sao theo chính sách sao lưu.

Kế hoạch dự phòng cho từng hệ thống và dịch vụ phải được thường xuyên được kiểm tra để đảm bảo rằng chúng đáp ứng các yêu cầu của kế hoạch nghiệp vụ liên tục. Đối với các hệ thống và dịch vụ quan trọng, kế hoạch dự phòng cần bao gồm tất cả các hệ thống thông tin, ứng dụng và dữ liệu cần thiết để phục hồi hoàn chỉnh hệ thống trong trường hợp có thảm họa.

Thời gian lưu giữ các thông tin nghiệp vụ quan trọng cần được xác định, có tính đến các yêu cầu để lưu giữ các bản sao được vĩnh viễn.

12.4 Ghi nhật ký và giám sát

Mục tiêu: Để ghi lại các sự kiện và tạo ra các bằng chứng.

12.4.1 Ghi nhật ký các sự kiện

Kiểm soát

Nhật ký các sự kiện ghi lại các thao tác người sử dụng, các trường hợp ngoại lệ, lỗi và sự cố an toàn thông tin cần được tạo ra, lưu giữ và thường xuyên soát xét lại.

Hướng dẫn thi hành

Nhật ký sự kiện cần bao gồm các thông tin sau, khi có liên quan:

- a) Định danh người dùng;
- b) Các thao tác hệ thống;
- c) Ngày tháng, thời gian và các chi tiết về các sự kiện quan trọng, ví dụ đăng nhập vào và thoát ra;

- d) Định danh thiết bị hoặc vị trí nếu có thẻ và bộ nhận dạng hệ thống;
- e) Hồ sơ các lần nỗ lực truy cập hệ thống thành công và thất bại;
- f) Hồ sơ các lần nỗ lực truy cập dữ liệu và tài nguyên khác thành công và thất bại;
- g) Thay đổi cấu hình hệ thống;
- h) Sử dụng đặc quyền ưu tiên;
- i) Sử dụng các tiện ích hệ thống và các ứng dụng;
- j) Các tập tin bị truy cập và loại truy cập;
- k) Các địa chỉ và giao thức mạng;
- l) Các cảnh báo của hệ thống kiểm soát truy cập;
- m) Kích hoạt và hủy kích hoạt của hệ thống bảo vệ, chẳng hạn như hệ thống chống virus và hệ thống phát hiện xâm nhập;
- n) Hồ sơ các giao dịch được thực hiện bởi người sử dụng trong các ứng dụng.

Nhật ký sự kiện đặt nền tảng cho các hệ thống giám sát tự động có khả năng tạo ra các báo cáo tổng hợp và cảnh báo về an toàn hệ thống.

Thông tin khác

Các nhật ký sự kiện có thể chứa dữ liệu nhạy cảm và thông tin định danh cá nhân. Các biện pháp thích hợp bảo vệ quyền riêng tư cá nhân cần được thực hiện ([xem 18.1.4](#)).

Nếu có thẻ, các quản trị viên hệ thống không cần có quyền xóa hoặc hủy kích hoạt nhật ký sự kiện cho các hoạt động riêng của họ ([xem 12.4.3](#)).

12.4.2 Bảo vệ các thông tin nhật ký

Kiểm soát

Các thiết bị lưu vết và thông tin nhật ký cần được bảo vệ chống sửa đổi và truy cập trái phép.

Hướng dẫn thi hành

Các kiểm soát nhằm mục đích bảo vệ chống lại các thay đổi trái phép thông tin nhật ký và các vấn đề thao tác với thiết bị nhật ký gồm có:

- a) Thay đổi chủng loại thông tin được ghi lại;
- b) Các tập tin nhật ký bị chỉnh sửa hoặc xóa;
- c) Dung lượng lưu trữ của các phương tiện lưu trữ tệp thông tin nhật ký bị vượt quá kích thước, dẫn đến lỗi ghi lại các sự kiện hoặc ghi đè lên các thông tin nhật ký của các sự kiện xảy ra trong quá khứ;

d) Một số thông tin nhạy cảm có thể được yêu cầu phải được lưu trữ như một phần của chính sách lưu giữ hồ sơ hoặc vì yêu cầu để thu thập và giữ lại bằng chứng (xem 16.1.7).

Thông tin khác

Các hệ thống nhạy cảm thường chứa một lượng lớn thông tin, phần lớn trong số chúng lại không liên quan đến việc giám sát an toàn. Để dễ dàng nhận diện các sự kiện quan trọng cho các mục đích giám sát an toàn thì cần quan tâm đến việc tự động sao chép lại các loại thông điệp phù hợp vào một nhạy kí thứ hai và/hoặc sử dụng các tiện ích hệ thống phù hợp hoặc các công cụ kiểm tra nhằm thực hiện điều tra và hợp lý hóa tệp.

Các nhạy kí hệ thống cần được bảo vệ, vì nếu dữ liệu có thể bị sửa đổi hoặc dữ liệu trong nhạy kí bị xóa bỏ thì sự tồn tại của chúng có thể gây ra lỗi an toàn thông tin. Sao chép thời gian thực các nhạy kí vào một hệ thống bên ngoài được đặt dưới sự kiểm soát của một quản trị viên hệ thống hay nhà điều hành cần được sử dụng để bảo vệ các nhạy kí.

12.4.3 Nhạy kí của người điều hành và người quản trị

Kiểm soát

Các hoạt động của người quản trị và người điều hành hệ thống cần được ghi vào nhạy kí và các nhạy kí cần được bảo vệ an toàn và thường xuyên rà soát.

Hướng dẫn thi hành

Các chủ tài khoản có thẩm quyền đặc biệt có thể thao tác trên nhạy kí dựa trên công cụ xử lý thông tin được đặt dưới sự kiểm soát trực tiếp của họ, do đó đây là điều cần thiết để bảo vệ và soát xét các nhạy kí để duy trì trách nhiệm đối với những người sử dụng có thẩm quyền đặc biệt.

Thông tin khác

Một hệ thống phát hiện xâm nhập được quản lý bên ngoài sự kiểm soát của hệ thống và quản trị mạng có thể được sử dụng để giám sát hoạt động của hệ thống và quản trị mạng cho phù hợp.

12.4.4 Đồng bộ thời gian

Kiểm soát

Các đồng hồ của tất cả các hệ thống xử lý thông tin liên quan trong tổ chức hoặc khu vực an toàn cần được đồng bộ hóa với một nguồn thời gian tham khảo duy nhất.

Hướng dẫn thi hành

Các yêu cầu bên trong và bên ngoài về biểu diễn thời gian, đồng bộ và độ chính xác cần được lập thành tài liệu. Các yêu cầu này có thể là quy định pháp luật, yêu cầu hợp đồng, tiêu chuẩn tuân thủ

hoặc các yêu cầu giám sát nội bộ. Một thời gian tham chiếu chuẩn để sử dụng trong tổ chức cần được xác định.

Cách tiếp cận của tổ chức để có được một thời gian tham chiếu từ các nguồn bên ngoài và làm thế nào để đồng bộ hóa các đồng hồ nội bộ một cách tin cậy cần được lập thành tài liệu và thực hiện.

Thông tin khác

Đặt các đồng hồ máy tính một cách chính xác là vấn đề quan trọng nhằm đảm bảo tính chính xác của các nhật ký kiểm soát, các nhật ký kiểm soát này có thể cần cho việc điều tra hoặc là bằng chứng trong các trường hợp vi phạm pháp luật hoặc kỷ luật. Các nhật ký không chính xác có thể gây trở ngại cho các cuộc điều tra và làm ảnh hưởng đến độ tin cậy của các bằng chứng. Đồng hồ được liên kết đến một chương trình phát thanh vô tuyến từ một đồng hồ nguyên tử quốc gia có thể được sử dụng như đồng hồ chủ đối với các hệ thống ghi nhật ký. Có thể sử dụng một giao thức thời gian mạng để giữ cho tất cả các đồng hồ phụ đều đồng bộ với đồng hồ chủ.

12.5 Kiểm soát phần mềm điều hành

Mục tiêu: Để đảm bảo tính toàn vẹn của các hệ thống hoạt động.

12.5.1 Cài đặt phần mềm trên các hệ thống vận hành

Kiểm soát

Các thủ tục cần được thực hiện để kiểm soát việc cài đặt phần mềm trên các hệ thống hoạt động.

Hướng dẫn thi hành

Các hướng dẫn sau đây cần được soát xét để kiểm soát những thay đổi của phần mềm trên hệ thống hoạt động:

- a) Việc cập nhật các phần mềm điều hành, các ứng dụng và thư viện chương trình chỉ cần được thực hiện bởi các quản trị viên được đào tạo và có thẩm quyền quản lý thích hợp;
- b) Hệ thống hoạt động chỉ cần thao tác với mã thực thi được phê duyệt và không thao tác với mã mới phát triển hoặc trình biên dịch;
- c) Các ứng dụng và phần mềm hệ điều hành chỉ cần được thực hiện sau khi thử nghiệm mở rộng và thành công; các bài kiểm tra cần bao gồm khả năng sử dụng, an toàn, tác động trên các hệ thống khác và thân thiện người sử dụng và cần được thực hiện trên các hệ thống riêng biệt (xem 12.1.4); cần đảm bảo rằng tất cả thư viện mã nguồn chương trình tương ứng đã được cập nhật;
- d) Một hệ thống điều khiển cấu hình cần được sử dụng để giữ quyền kiểm soát tất cả các phần mềm đã thực hiện cũng như các tài liệu của hệ thống;
- e) Một chiến lược quay lại như cũ cần có trước khi các thay đổi được thực hiện;

- f) Một nhật ký kiểm soát cần được duy trì cho tất cả các bản cập nhật về các thư viện chương trình hoạt động;
- g) Các phiên bản trước của phần mềm ứng dụng cần được giữ lại như một biện pháp dự phòng;
- h) Các phiên bản cũ của phần mềm cần được lưu trữ, cùng với tất cả các thông tin và các thông số cần thiết, các thủ tục, các chi tiết cấu hình và phần mềm hỗ trợ với thời gian kéo dài như các dữ liệu được lưu giữ trong kho lưu trữ. Công ty cung cấp phần mềm được sử dụng trong các hệ thống vận hành cần được duy trì một mức độ hỗ trợ từ nhà cung cấp. Theo thời gian, các nhà cung cấp phần mềm sẽ ngừng hỗ trợ các phiên bản phần mềm cũ hơn. Tổ chức cần soát xét các rủi ro của việc lựa chọn phần mềm không được hỗ trợ.

Bất kỳ quyết định nâng cấp lên một phiên bản mới cần tính đến các yêu cầu nghiệp vụ cho việc thay đổi và độ an toàn của bản mới phát hành, ví dụ việc giới thiệu các chức năng an toàn thông tin mới hoặc số lượng và mức độ nghiêm trọng của vấn đề an toàn thông tin bị ảnh hưởng trong phiên bản này. Bản vá lỗi phần mềm cần được áp dụng khi chúng có thể giúp loại bỏ hoặc giảm bớt lỗi hỏng an toàn thông tin.

Quyền truy cập vật lý hay truy cập lô gic chỉ cần được trao cho các nhà cung cấp cho các mục đích hỗ trợ khi cần thiết và phù hợp với chính sách quản lý. Các hoạt động của nhà cung cấp cần được theo dõi.

Phần mềm máy tính có thể dựa vào việc cung cấp phần mềm và các module từ bên ngoài, nhưng cần được theo dõi và kiểm soát để tránh bị thay đổi trái phép, điều mà có thể làm phát sinh những lỗi hỏng an toàn.

12.6 Quản lý lỗi hỏng kỹ thuật

Mục tiêu: Để ngăn chặn việc khai thác các lỗi hỏng kỹ thuật.

12.6.1 Quản lý các lỗi hỏng kỹ thuật

Kiểm soát

Thông tin về các lỗi hỏng kỹ thuật của hệ thống thông tin cần được thu thập một cách kịp thời, tổ chức có các lỗi hỏng kỹ thuật phải được đánh giá và đưa ra các biện pháp thích hợp để đối phó với các rủi ro liên quan.

Hướng dẫn thi hành

Một hệ thống kiểm kê đầy đủ tài sản hiện có ([xem điều 8](#)) là một điều kiện tiên quyết cho việc quản lý các lỗi hỏng kỹ thuật một cách hiệu quả. Thông tin cụ thể và cần thiết để hỗ trợ quản lý lỗi hỏng kỹ thuật bao gồm thông tin về nhà cung cấp phần mềm, số phiên bản, hiện trạng triển khai (ví dụ như phần mềm nào được cài đặt vào hệ thống nào) và các cá nhân trong tổ chức chịu trách nhiệm về phần mềm.

Các hành động thích hợp và kịp thời cần được thực hiện nhằm định danh các lỗ hổng kỹ thuật tiềm ẩn. Cần tuân theo các hướng dẫn sau đây để thiết lập được một quy trình quản lý các lỗ hổng kỹ thuật hiệu quả:

- a) tổ chức cần xác định và thiết lập các nguyên tắc và trách nhiệm liên quan đến việc quản lý các lỗ hổng kỹ thuật, gồm việc giám sát các lỗ hổng, đánh giá rủi ro của các lỗ hổng, bัน vá, theo dõi tài sản và bất kỳ trách nhiệm phối hợp nào được yêu cầu;
- b) các tài nguyên thông tin sẽ được sử dụng để định danh các lỗ hổng kỹ thuật liên quan và để duy trì mối quan tâm về chúng, điều này cần được xác định đối với các phần mềm và các công nghệ khác (dựa trên danh sách kiểm kê tài sản, xem 8.1.1); những tài nguyên thông tin này cần được cập nhật khi có những thay đổi trong bảng kiểm kê, hoặc khi tìm ra các nguồn tài nguyên mới hoặc hữu dụng;
- c) cần xác định thời hạn phản ứng lại mỗi khi có các thông báo về các lỗ hổng kỹ thuật tiềm ẩn;
- d) mỗi khi có một lỗ hổng kỹ thuật tiềm ẩn được xác định, tổ chức cần xác định các rủi ro liên quan và có các hành động cần thực hiện; hành động đó có thể chỉ là bัน vá các hệ thống bị tổn hại và/hoặc sử dụng các biện pháp kiểm soát khác;
- e) tùy thuộc sự khẩn cấp cần giải quyết các lỗ hổng kỹ thuật mà hoạt động đã được xác định phải được thực hiện theo các biện pháp kiểm soát liên quan tới việc quản lý sự thay đổi (xem 12.1.2) hoặc bằng cách tuân theo các thủ tục đối phó với sự cố an toàn thông tin (xem 16.1.5);
- f) nếu bัน vá có sẵn thì các rủi ro liên quan tới việc cài đặt bัน vá cần được đánh giá (các rủi ro xuất phát từ lỗ hổng đó cần được so sánh với rủi ro do cài đặt bán vá);
- g) các bัน vá cần được kiểm tra và đánh giá trước khi chúng được cài đặt nhằm đảm bảo sự hiệu quả và không dẫn tới những tác dụng phụ quá sức chịu đựng của hệ thống; nếu không có bัน vá nào sẵn sàng thì cần quan tâm đến các biện pháp kiểm soát khác, ví dụ:
 - 1) tắt các dịch vụ hoặc các khả năng có liên quan tới lỗ hổng;
 - 2) sửa lại hoặc đưa thêm các biện pháp kiểm soát truy cập, ví dụ đặt các tường lửa tại các biên giới mạng (xem 13.1);
 - 3) tăng cường giám sát nhằm phát hiện hoặc ngăn chặn các tấn công thực sự;
 - 4) nâng cao nhận thức về lỗ hổng;
- h) duy trì một nhật ký kiểm tra đối với tất cả các thủ tục đã thực hiện;
- i) quy trình quản lý các lỗ hổng kỹ thuật cần được giám sát và đánh giá định kỳ nhằm đảm bảo ảnh hưởng và hiệu quả của nó;
- j) các hệ thống có mức rủi ro cao cần được tập trung xử lý trước tiên.

- k) một quy trình quản lý lỗ hổng kỹ thuật hiệu quả cần phải gắn với các hoạt động quản lý sự cố, để trao đổi dữ liệu về các lỗ hổng với bộ phận có chức năng ứng phó sự cố và cung cấp các thủ tục kỹ thuật cần thực hiện khi một sự cố xảy ra;
- l) xác định một thủ tục để giải quyết các tình huống nơi một lỗ hổng đã được xác định nhưng không có biện pháp đối phó thích hợp. Trong tình huống này, tổ chức cần phải đánh giá các rủi ro liên quan đến các lỗ hổng đã biết và xác định các hành động kiểm tra và khắc phục thích hợp.

Thông tin khác

Việc quản lý các lỗ hổng kỹ thuật có thể được coi như là một chức năng phụ của việc quản lý sự thay đổi và vì thế nó có thể tận dụng được các thủ tục và các quy trình quản lý sự thay đổi ([xem 12.1.2](#) và [14.2.2](#)).

Các nhà cung cấp thường phải chịu áp lực lớn trong việc ban hành các bản vá càng sớm càng tốt. Vì vậy, một bản vá có thể không giải quyết được vấn đề một cách thỏa đáng và có thể gây ra những ảnh hưởng tiêu cực. Hơn nữa, trong một số trường hợp, việc gỡ các bản vá có thể lại không dễ dàng nếu bản vá đã được áp dụng.

Nếu không thể kiểm tra các bản vá một cách thỏa đáng, ví dụ do chi phí hoặc do thiếu tài nguyên, thì cũng có thể cân nhắc đến việc trì hoãn vá để đánh giá các rủi ro liên quan dựa trên kinh nghiệm đã được báo cáo bởi những người dùng khác. Việc sử dụng tiêu chuẩn ISO/IEC 27031 có thể có lợi.

12.6.2 Hạn chế cài đặt phần mềm

Kiểm soát

Cần thiết lập và thực hiện quy định điều chỉnh cài đặt phần mềm bởi những người sử dụng.

Hướng dẫn thi hành

Các tổ chức cần xác định và thực thi chính sách nghiêm ngặt với những phần mềm mà người dùng cài đặt.

Các nguyên tắc đặc quyền tối thiểu cần được áp dụng. Nếu được cấp quyền nhất định, người dùng có khả năng cài đặt phần mềm. Các tổ chức cần xác định những loại phần mềm cho phép được cài đặt (ví dụ như các bản cập nhật và bản vá lỗi bảo mật cho phần mềm hiện có) và những loại cài đặt bị cấm (ví dụ phần mềm của riêng cá nhân sử dụng và phần mềm thuộc họ với các loại mã độc hại mà có thể biết hoặc nghi ngờ). Những đặc quyền này phải được cấp dựa trên vai trò của người sử dụng có liên quan.

Thông tin khác

Không kiểm soát được cài đặt phần mềm trên thiết bị máy tính có thể dẫn đến lỗ hổng đã giới thiệu, và sau đó để rò rỉ thông tin, mất tính toàn vẹn, sự cố an toàn thông tin khác hoặc vi phạm đến quyền sở hữu trí tuệ.

12.7 Soát xét việc đánh giá các hệ thống thông tin

Mục tiêu: Để giảm thiểu tác động của các hành động đánh giá trên các hệ thống hoạt động.

12.7.1 Các kiểm soát đánh giá hệ thống thông tin

Kiểm soát

Yêu cầu đánh giá và các hành động liên quan đến việc xác thực hệ thống hoạt động cần được lên kế hoạch cẩn thận và thống nhất để giảm thiểu sự gián đoạn các quy trình nghiệp vụ.

Hướng dẫn thi hành

Các hướng dẫn sau đây cần được quan tâm:

- a) các yêu cầu đánh giá có truy cập vào hệ thống và dữ liệu cần tuân thủ quy định quản lý phù hợp;
- b) phạm vi của thử nghiệm đánh giá kỹ thuật cần được thống nhất và có kiểm soát;
- c) các thử nghiệm đánh giá cần được giới hạn truy cập chỉ đọc (read-only) đến phần mềm và dữ liệu;
- d) các kiểm tra hệ thống chỉ cần được phép tiến hành cho bản ghi khi cô lập các tập tin hệ thống, và cần được xóa khi việc kiểm tra được hoàn thành, hoặc được bảo vệ thích hợp nếu có một nghĩa vụ giữ các tập tin đó theo yêu cầu về tài liệu kiểm tra;
- e) các truy cập khác ngoài truy cập chỉ đọc chỉ được cho phép đối với các bản sao đã được phân tách khỏi các tập tin hệ thống, các bản sao này phải được xóa bỏ khi việc đánh giá đã hoàn tất hoặc được bảo vệ phù hợp nếu có nghĩa vụ phải giữ lại các tập tin đó theo các yêu cầu của hồ sơ đánh giá;
- f) các yêu cầu về xử lý đặc biệt hoặc xử lý thêm cũng cần được xác định rõ và được thông qua;
- g) các thử nghiệm đánh giá có thể ảnh hưởng đến sự sẵn sàng của hệ thống cần tiến hành ngoài giờ làm việc;
- h) tất cả các truy cập cần được theo dõi và ghi lại để tạo ra nhật ký tham khảo.

13 An toàn truyền thông

13.1 Quản lý an toàn mạng

Mục tiêu: Nhằm đảm bảo việc bảo vệ thông tin trên các mạng và các phương tiện xử lý thông tin.

13.1.1 Các biện pháp kiểm soát mạng

Kiểm soát

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

Hướng dẫn thi hành

Các biện pháp kiểm soát cần được triển khai nhằm đảm bảo sự an toàn của thông tin trên mạng, và đảm bảo bảo vệ các dịch vụ kết nối trước sự truy cập trái phép. Cụ thể là, cần quan tâm đến các vấn đề sau:

- a) cần thiết lập các trách nhiệm và thủ tục quản lý các thiết bị mạng;
- b) nếu cần, cần tách bạch trách nhiệm về mặt khai thác mạng với việc vận hành máy tính (xem 6.1.2);
- c) cần thiết lập các biện pháp kiểm soát đặc biệt nhằm bảo vệ an toàn thông tin và sự toàn vẹn của dữ liệu đi qua các mạng công cộng hoặc qua các mạng vô tuyến, và bảo vệ các hệ thống được kết nối và các ứng dụng (xem 10 và 13.2); các biện pháp bảo vệ đặc biệt có thể được yêu cầu nhằm duy trì khả năng sẵn sàng của các dịch vụ mạng và các máy tính được kết nối;
- d) cần áp dụng hình thức ghi nhật ký và giám sát phù hợp nhằm phát hiện và ghi lại các hoạt động có thể ảnh hưởng, hoặc liên quan đến, an toàn thông tin;
- e) cần phối hợp chặt chẽ các hoạt động quản lý nhằm tối ưu dịch vụ đồng thời đảm bảo rằng các biện pháp kiểm soát đã được áp dụng nhất quán qua hạ tầng xử lý thông tin;
- f) các hệ thống trên mạng cần được xác thực;
- g) cần hạn chế kết nối từ các hệ thống tới mạng.

Thông tin khác

Các thông tin khác về an toàn mạng có thể xem thêm trong ISO/IEC 27033^{[15][16][17][18][19]}.

13.1.2 An toàn các dịch vụ mạng

Kiểm soát

Các tính năng cơ chế đảm bảo an toàn, các mức dịch vụ và các yêu cầu quản lý của tất cả các dịch vụ mạng cần được xác định và ghi rõ trong thỏa thuận về các dịch vụ mạng, bao gồm dịch vụ là do nội bộ cấp hay phần mềm thuê ngoài.

Hướng dẫn thi hành

Cần xác định và thường xuyên giám sát khả năng của nhà cung cấp dịch vụ mạng trong việc quản lý an toàn các dịch vụ đã thỏa thuận, và cũng cần thỏa thuận về quyền kiểm toán.

Cũng cần xác định các yêu cầu về an toàn cần thiết cho các dịch vụ cụ thể, ví dụ như các tính năng an toàn, các mức dịch vụ, và các yêu cầu về quản lý. Tổ chức cần đảm bảo rằng các nhà cung cấp dịch vụ có triển khai các biện pháp này.

Thông tin khác

Các dịch vụ mạng bao gồm cung cấp kết nối, các dịch vụ mạng riêng, và các mạng cung cấp dịch vụ giá trị gia tăng và các giải pháp an toàn mạng được quản lý ví dụ các hệ thống tường lửa và các hệ thống phát hiện xâm nhập. Các dịch vụ này có thể đi từ dạng có băng tần không được quản lý đến dạng các dịch vụ giá trị gia tăng phức tạp.

Tính năng an toàn của dịch vụ mạng có thể là:

- a) áp dụng công nghệ an toàn dịch vụ mạng, ví dụ như chứng thực, mật mã và kiểm soát kết nối mạng;
- b) các kết nối với các dịch vụ mạng cần phải có thông số kỹ thuật phù hợp với các quy tắc an toàn và kết nối mạng;
- c) cần có thủ tục cho việc sử dụng dịch vụ mạng để hạn chế quyền truy cập vào các dịch vụ mạng hoặc các ứng dụng khi cần thiết.

13.1.3 Phân tách mạng

Kiểm soát

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

Hướng dẫn thi hành

Một phương pháp kiểm soát an toàn cho các mạng lớn là phân tách chúng thành các vùng mạng khác nhau. Các vùng mạng này có thể được xây dựng dựa trên cấp độ tin cậy (ví dụ vùng truy cập chung, vùng máy trạm, vùng máy chủ), cùng với đơn vị trong tổ chức (như bộ phận nguồn nhân lực, tài chính, thị trường) hoặc theo sự kết hợp nhiều thành phần (như vùng máy chủ kết nối tới các đơn vị quản lý). Việc phân tách mạng có thể được thực hiện ở cả các mạng mức vật lý và mức logic (như mạng riêng ảo).

Vành đai mỗi miền mạng cần được định nghĩa một cách rõ ràng. Việc truy cập giữa các vùng miền có thể được thực hiện nhưng phải được kiểm soát tại các vành đai thông qua các cổng (như tường lửa hoặc bộ lọc định tuyến). Các tiêu chí để phân tách mạng thành các vùng miền và việc truy cập thông qua cổng cần dựa trên một đánh giá về yêu cầu an toàn của từng vùng miền. Đánh giá cần dựa theo chính sách quản lý truy cập ([xem 9.1.1](#)), và cũng cần soát xét chi phí tương đối và ảnh hưởng của định tuyến mạng hợp lý hoặc công nghệ cổng lên chất lượng mạng.

Các mạng không dây cần được soát xét một cách đặc biệt hơn do sự khó khăn trong việc định nghĩa vành đai mạng. Đối với những môi trường nhạy cảm, cần soát xét việc coi tất cả các truy cập không dây là những kết nối bên ngoài và phân tách truy cập này khỏi mạng nội bộ cho đến khi truy cập đi qua một cổng an toàn theo chính sách quản lý quản lý mạng ([xem 13.1.1](#)) trước khi cấp quyền truy cập các hệ thống bên trong.

Khi được thực hiện đúng, việc sử dụng các công nghệ hiện đại về kiểm soát xác thực, mật mã và mức độ sử dụng truy cập mạng và tiêu chuẩn dựa trên mạng không dây có thể là đủ để kết nối trực tiếp vào mạng nội bộ của tổ chức.

Thông tin khác

Mạng càng ngày càng có xu hướng mở rộng ra ngoài ranh giới của tổ chức, vì các quan hệ đối tác kinh doanh được hình thành có thể yêu cầu kết nối hoặc chia sẻ các phương tiện mạng và phương tiện xử lý thông tin. Các mạng mở rộng có thể làm tăng nguy cơ truy cập trái phép vào các hệ thống thông tin hiện đang sử dụng mạng, một số mạng mở rộng có thể đòi hỏi phải được bảo vệ trước những người dùng mạng khác vì tính chất quan trọng hay độ nhạy cảm của các mạng này.

13.2 An toàn truyền tải thông tin

Mục tiêu: Nhằm duy trì an toàn thông tin thông tin được truyền trong một tổ chức hay với bất kỳ thực thể nào bên ngoài.

13.2.1 Các chính sách và thủ tục truyền tải thông tin

Kiểm soát

Các chính sách, thủ tục và biện pháp kiểm soát chính thức cần phải sẵn có để bảo vệ sự trao đổi thông tin thông qua hệ thống truyền thông.

Hướng dẫn thi hành

Các biện pháp và thủ tục cần tuân thủ khi sử dụng các phương tiện truyền thông điện tử trong truyền tải thông tin cần quan tâm đến các vấn đề sau:

- a) các thủ tục được thiết kế nhằm bảo vệ thông tin được truyền tải khỏi sự nghe lén, sao chép, sửa đổi, sai địa chỉ, và phá hủy;
- b) các thủ tục nhằm phát hiện và bảo vệ chống lại mã độc hại bị phát tán khi sử dụng các phương tiện truyền thông điện tử (xem 12.2.1);
- c) các thủ tục nhằm bảo vệ thông tin điện tử nhạy cảm được truyền tải có file đính kèm;
- d) chính sách hoặc các hướng dẫn sơ lược về sử dụng các phương tiện truyền thông điện tử (xem 8.1.3);
- e) trách nhiệm nhân viên, người tham gia bên ngoài và bắt cứ cá nhân nào trong công việc không làm ảnh hưởng xấu đến tổ chức. Ví dụ qua phỉ báng, quấy rối, mạo danh, chuyển tiếp chuỗi các thư, thu mua trái phép...;
- f) có thể sử dụng các kỹ thuật mật mã nhằm bảo vệ sự an toàn, tính toàn vẹn và tính xác thực của thông tin (xem điều 10);

- g) hướng dẫn ngăn chặn và hủy bỏ các thư từ giao dịch, bao gồm cả các thông điệp, theo các quy định và quy chế nội bộ và quốc gia có liên quan;
- h) các biện pháp kiểm soát và các hạn chế liên quan đến việc chuyển tiếp các phương tiện truyền thông, ví dụ tự động chuyển tiếp thư điện tử vào các địa chỉ hộp thư bên ngoài;
- i) Nhắc nhở nhân viên để có biện pháp phòng ngừa thích hợp không tiết lộ thông tin bí mật;
- j) không để lại các thông điệp chứa thông tin nhạy cảm ở các máy trả lời vì các thông điệp này có thể bị những người không có quyền nghe lại, cắt giữ trên các hệ thống công cộng hoặc cắt giữ không đúng quy cách do quay nhầm số;
- k) nhắc nhở với mọi người về các sự cố do sử dụng máy sao chép, cụ thể là:
 - 1) truy cập trái phép vào các bộ lưu giữ thông điệp bên trong nhằm lấy các thông điệp;
 - 2) cố ý hoặc vô tình lập trình cho các máy thực hiện gửi các thông điệp đến các số cụ thể nào đó;
 - 3) do quay số sai hoặc sử dụng số lưu trữ sai mà gửi nhầm các tài liệu và các thông điệp;

Ngoài ra, cần phải nhắc nhở nhân viên không cần có cuộc nói chuyện bí mật ở nơi công cộng hoặc trên các kênh truyền thông, văn phòng và những địa điểm họp không an toàn.

Các dịch vụ truyền tải thông tin cần tuân thủ với các yêu cầu pháp lý liên quan ([xem 18.1](#)).

Thông tin khác

Có thể xảy ra truyền tải thông tin khi sử dụng nhiều loại phương tiện truyền thông khác nhau, bao gồm thư điện tử, thoại, sao chụp, và video.

Có thể truyền tải phần mềm qua nhiều phương thức khác nhau, bao gồm tải thông tin từ trên mạng và tải thông tin được các nhà cung cấp các sản phẩm mua có sẵn yêu cầu.

Cần quan tâm đến những vấn đề về an toàn, pháp lý và nghiệp vụ liên quan đến việc truyền tải dữ liệu điện tử, thương mại điện tử, truyền thông điện tử và các yêu cầu về các biện pháp kiểm soát.

13.2.2 Các thỏa thuận truyền tải thông tin

Kiểm soát

Các thỏa thuận cần đề cập đến việc đảm bảo truyền tải thông tin nghiệp vụ giữa tổ chức và các đối tác bên ngoài.

Hướng dẫn thi hành

Các thỏa thuận trao đổi thông tin cần quan tâm đến các điều kiện sau đây:

- a) các trách nhiệm của ban lãnh đạo trong việc quản lý và thông báo về việc truyền, gửi và nhận thông tin chuyển giao;

- b) các thủ tục đảm bảo khả năng truy vết và không thể chối bỏ;
- c) các tiêu chuẩn kỹ thuật tối thiểu cho việc đóng gói và truyền;
- d) các thỏa thuận giao kèo;
- e) các tiêu chuẩn nhận dạng người chuyển;
- f) các trách nhiệm và nghĩa vụ khi có các sự kiện an toàn thông tin, như mất dữ liệu;
- g) sử dụng hệ thống dán nhãn đã thỏa thuận đối với các thông tin quan trọng hoặc nhạy cảm, đảm bảo rằng ý nghĩa của các nhãn có thể được hiểu ngay và thông tin đó đã được bảo vệ phù hợp (xem 8.2);
- h) các tiêu chuẩn kỹ thuật cho ghi và đọc thông tin và phần mềm;
- i) bất kỳ các biện pháp kiểm soát đặc biệt được yêu cầu nhằm bảo vệ các thông tin nhạy cảm, như sử dụng mật mã (xem điều 10);
- j) duy trì một chuỗi giám sát cho thông tin trong khi truyền;
- k) các mức độ chấp nhận của kiểm soát truy cập.

Các chính sách, thủ tục, và tiêu chuẩn cần được thiết lập và được quản lý nhằm bảo vệ thông tin và phương tiện vật lý trong quá trình truyền (xem 8.3.3), và cần được tham chiếu trong các thỏa thuận truyền tải.

Nội dung về an toàn của các thỏa thuận cần thể hiện độ nhạy cảm của thông tin kinh doanh liên quan.

Thông tin khác.

Các thỏa thuận có thể ở dạng điện tử hoặc viết tay, và hình thức có thể như các bản hợp đồng chính thức. Đối với thông tin tuyệt mật thì các cơ chế đặc biệt sử dụng cho trao đổi thông tin đó cần phù hợp với tất cả các tổ chức và các loại thỏa thuận.

13.2.3 Thông điệp điện tử

Kiểm soát

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

Hướng dẫn thi hành

Cần quan tâm đến các vấn đề an toàn sau đối với thông điệp điện tử:

- a) bảo vệ thông điệp khỏi sự truy cập trái phép, sửa đổi hoặc từ chối dịch vụ tương ứng với các chương trình phân loại của tổ chức;
- b) đảm bảo đánh đúng địa chỉ và gửi đúng địa chỉ thông điệp;

- c) độ tin cậy và độ sẵn sàng của dịch vụ;
- d) các vấn đề pháp lý, ví dụ các yêu cầu về chữ ký điện tử;
- e) được chấp thuận trước khi sử dụng các dịch vụ công cộng bên ngoài như nhắn tin tức thời, mạng xã hội hoặc chia sẻ tệp;
- f) truy cập từ các mạng công cộng dễ truy cập phải được quản lý bằng mức xác thực cao hơn.

Thông tin khác.

Có rất nhiều loại thông điệp điện tử như thư điện tử, trao đổi dữ liệu điện tử và mạng xã hội đóng một vai trò trong các giao dịch thương mại.

13.2.4 Các thỏa thuận an toàn hay không tiết lộ

Kiểm soát

Các yêu cầu về an toàn hoặc các thỏa thuận không tiết lộ phản ánh nhu cầu của tổ chức đối với việc bảo vệ thông tin phải được xác định rõ và thường xuyên soát xét và ghi lại.

Hướng dẫn thi hành

Các thỏa thuận an toàn hoặc không tiết lộ cần tập trung vào các yêu cầu nhằm bảo vệ thông tin mật với các điều khoản có khả năng thực thi về mặt pháp lý. Các thỏa thuận an toàn hay không tiết lộ được áp dụng với các đối tác bên ngoài và các nhân viên trong tổ chức. Các yếu tố cần được lựa chọn hoặc bổ sung trong cân nhắc về thể loại và khả năng truy cập hoặc xử lý thông tin bí mật của bên kia. Khi xác định các yêu cầu đối với các thỏa thuận an toàn hoặc không tiết lộ, cần quan tâm đến các yếu tố sau:

- a) định nghĩa về thông tin cần được bảo vệ (ví dụ, thông tin mật);
- b) khoảng thời gian mong muốn của thỏa thuận, bao gồm cả các trường hợp yêu cầu an toàn không thời hạn;
- c) các hoạt động được yêu cầu khi kết thúc thỏa thuận;
- d) các trách nhiệm và các hoạt động ký kết nhằm tránh tiết lộ thông tin trái phép;
- e) quyền sở hữu thông tin, các bí mật giao dịch và quyền sở hữu trí tuệ, và mối quan hệ của chúng với việc bảo vệ thông tin mật;
- f) cách thức sử dụng được phép thông tin mật và quyền sử dụng thông tin mật;
- g) quyền kiểm toán và giám sát các hoạt động liên quan đến thông tin mật;
- h) quy trình thông báo và báo cáo về việc tiết lộ trái phép hoặc những lỗ hổng thông tin mật;
- i) các điều khoản đối với thông tin được trả về hoặc bị hủy khi chấm dứt thỏa thuận;
- j) các hoạt động được mong đợi trong trường hợp có vi phạm thỏa thuận.

Dựa trên các yêu cầu về an toàn thông tin của tổ chức, có thể đưa thêm một số điều khoản khác vào thỏa thuận an toàn hoặc thỏa thuận không tiết lộ.

Các thỏa thuận an toàn và không tiết lộ cần tuân thủ tất cả những quy định và điều luật phù hợp ([xem 18.1](#)).

Các yêu cầu đối với các thỏa thuận an toàn và không tiết lộ cần được soát xét định kỳ và tại các thời điểm xảy ra thay đổi làm ảnh hưởng đến các yêu cầu này.

Thông tin khác.

Các thỏa thuận an toàn hoặc không tiết lộ sẽ bảo vệ thông tin của tổ chức và thông báo các bên ký kết về trách nhiệm của họ trong bảo vệ, sử dụng, và tiết lộ thông tin theo một phương thức cho phép và có trách nhiệm.

Mỗi tổ chức cũng có thể cần sử dụng các hình thức thỏa thuận an toàn hoặc không tiết lộ khác nhau trong các từng tình huống khác nhau.

14 Tiếp nhận, phát triển và bảo trì hệ thống

14.1 Yêu cầu đảm bảo an toàn cho các hệ thống thông tin

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

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

Kiểm soát

Các yêu cầu về an toàn thông tin cần được bao gồm trong các yêu cầu nghiệp vụ đối với các hệ thống thông tin mới hoặc cải tiến từ các hệ thống thông tin sẵn có.

Hướng dẫn thi hành

Yêu cầu an toàn thông tin cần phải được xác định bằng các phương pháp khác nhau như xuất phát từ yêu cầu tuân thủ các chính sách hay quy định, mô hình hóa mối đe dọa, soát xét các sự cố, hoặc sử dụng các ngưỡng lỗi hỏng. Kết quả của việc xác định cần được lập tài liệu và soát xét bởi tất cả các bên liên quan.

Các yêu cầu an toàn thông tin và biện pháp kiểm soát cần phản ánh giá trị nghiệp vụ của các tài sản thông tin liên quan ([xem 8.2](#)) và những thiệt hại nghiệp vụ tiềm ẩn có thể xảy ra do lỗi hoặc do sự thiếu an toàn.

Xác định và quản lý các yêu cầu về an toàn thông tin và các quá trình liên quan cần được tích hợp trong giai đoạn đầu của dự án hệ thống thông tin. Cần soát xét sớm các yêu cầu về an toàn thông tin, ví dụ trong giai đoạn thiết kế, có thể dẫn đến các giải pháp hiệu quả hơn và ít chi phí hơn.

Yêu cầu an toàn thông tin cần quan tâm:

- a) mức độ tin cậy cần thiết đối với các khẳng định danh tính người sử dụng, để lấy được các yêu cầu xác thực người sử dụng;
- b) các quy trình ủy quyền và cấp phép truy cập, cho người dùng doanh nghiệp cũng như cho người sử dụng đặc quyền hoặc kỹ thuật;
- c) thông báo trách nhiệm và nhiệm vụ cho người dùng và các nhà khai thác;
- d) các yêu cầu bảo vệ cần thiết của các tài sản liên quan, đặc biệt là liên quan đến tính sẵn sàng, an toàn thông tin và toàn vẹn;
- e) các yêu cầu bắt nguồn từ quá trình kinh doanh, như ghi nhật ký và giám sát giao dịch, các yêu cầu chống chối bỏ;
- f) các yêu cầu bắt buộc bởi các biện pháp kiểm soát an toàn khác, ví dụ như giao diện để ghi nhật ký và giám sát hoặc hệ thống phát hiện rò rỉ dữ liệu.

Đối với các ứng dụng cung cấp dịch vụ trên các mạng công cộng hoặc có thực hiện giao dịch, các biện pháp kiểm soát dành riêng ([xem 14.1.2](#) và [14.1.3](#)) cần được xem xét.

Nếu sản phẩm được mua, phải tuân theo một quá trình thử nghiệm và mua chính thức. Hợp đồng với các nhà cung cấp phải giải quyết các yêu cầu an toàn được xác định. Trường hợp chức năng an toàn trong một sản phẩm để xuất không đáp ứng được yêu cầu quy định, các rủi ro và kiểm soát liên quan cần được soát xét lại trước khi mua sản phẩm.

Hướng dẫn có sẵn cho cấu hình an toàn của sản phẩm phù hợp với các phần mềm/ dịch vụ của hệ thống cần được đánh giá và thực hiện.

Các tiêu chí chấp nhận sản phẩm phải được xác định, ví dụ về chức năng, sẽ đảm bảo rằng các yêu cầu an toàn xác định được đáp ứng. Sản phẩm cần được đánh giá trên theo những tiêu chí này trước khi mua. Chức năng bổ sung cần được soát xét để đảm bảo nó không đưa ra thêm những rủi ro không thể chấp nhận.

Thông tin khác

ISO/IEC 27005^[11] và ISO 31000^[27] cung cấp hướng dẫn về việc sử dụng các quy trình quản lý rủi ro để xác định các biện pháp kiểm soát nhằm đáp ứng các yêu cầu an toàn thông tin.

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

Kiểm soát

Thông tin liên quan trong các dịch vụ ứng dụng truyền tải trên các mạng công cộng cần được bảo vệ trước các hoạt động lừa đảo, tranh chấp hợp đồng, tiết lộ và sửa đổi trái phép.

Hướng dẫn thi hành

Cân nhắc an toàn thông tin cho các dịch vụ ứng dụng truyền tải trên các mạng công cộng cần bao hàm các nội dung sau:

- a) mức độ tin cậy mỗi bên yêu cầu về định danh của nhau, ví dụ thông qua xác thực;
- b) các quy trình ủy quyền liên quan đến những người có thể phê duyệt nội dung, phát hành hoặc ký các văn bản giao dịch chủ chốt;
- c) đảm bảo rằng các đối tác liên lạc được thông báo đầy đủ về việc ủy quyền cung cấp hoặc sử dụng dịch vụ;
- d) xác định các yêu cầu về tính bí mật, tính toàn vẹn, chứng minh việc gửi và nhận tài liệu quan trọng và không thoái thác hợp đồng, ví dụ như gắn liền với quá trình đấu thầu và hợp đồng;
- e) mức độ tin cậy yêu cầu trong sự toàn vẹn của tài liệu quan trọng;
- f) các yêu cầu bảo vệ của bất kỳ thông tin bí mật;
- g) sự an toàn và tính toàn vẹn của bất kỳ giao dịch đặt hàng, thông tin thanh toán, địa chỉ giao hàng chi tiết và xác nhận biên lai thu tiền;
- h) mức độ xác minh thích hợp để xác minh thông tin thanh toán được cung cấp bởi khách hàng;
- i) lựa chọn các hình thức thanh toán phù hợp của thanh toán để bảo vệ chống lại gian lận;
- j) mức độ bảo vệ cần thiết để duy trì sự an toàn và tính toàn vẹn của thông tin được đặt hàng;
- k) chống thất thoát hay sao chép thông tin giao dịch;
- l) trách nhiệm liên quan với bất kỳ giao dịch gian lận;
- m) các yêu cầu bảo hiểm.

Nhiều trong số những điều ở trên có thể giải quyết bằng việc áp dụng biện pháp kiểm soát mật mã (xem điều 10), có tính đến sự tuân thủ các yêu cầu pháp lý (xem điều 18, đặc biệt xem 18.1.5 cho pháp luật về mật mã).

Dàn xếp dịch vụ ứng dụng giữa các đối tác cần được hỗ trợ bởi một thỏa thuận trong đó hai bên đã đồng ý các điều khoản dịch vụ, bao gồm chi tiết về ủy quyền (xem b) bên trên.

Nên xem xét các yêu cầu mềm dẻo chống lại các cuộc tấn công, trong đó có thể bao gồm các yêu cầu về bảo vệ các máy chủ ứng dụng có liên quan hoặc đảm bảo các mối liên kết mạng cần thiết để cung cấp các dịch vụ.

Thông tin khác

Các ứng dụng có thể truy cập thông qua mạng công cộng là đối tượng của một loạt các mối đe dọa mạng liên quan, chẳng hạn như hoạt động lừa đảo, tranh chấp hợp đồng hoặc tiết lộ thông tin rộng khắp. Vì vậy, đánh giá rủi ro chi tiết và lựa chọn chuẩn xác các biện pháp kiểm soát là không thể thiếu. Các biện pháp kiểm soát thường bao gồm các phương thức mật mã để xác thực và đảm bảo truyền dữ liệu.

Dịch vụ ứng dụng có thể sử dụng phương pháp xác thực an toàn, ví dụ như sử dụng mật mã khóa công khai và chữ ký số ([xem điều 10](#)) để giảm rủi ro. Ngoài ra, các bên thứ ba tin cậy có thể được sử dụng, nơi những dịch vụ như vậy là cần thiết.

14.1.3 Bảo vệ các giao dịch dịch vụ ứng dụng

Kiểm soát

Thông tin liên quan đến các giao dịch của dịch vụ ứng dụng phải được bảo vệ để ngăn ngừa truyền tải không đầy đủ, định tuyến sai, thay đổi thông điệp trái phép, tiết lộ trái phép, sao chép hoặc phát lại trái phép.

Hướng dẫn thi hành

Cân nhắc an toàn thông tin cho các giao dịch của dịch vụ ứng dụng cần bao gồm những điều sau:

- a) mỗi bên tham gia giao dịch sử dụng chữ ký số;
- b) tất cả các khía cạnh của giao dịch, đảm bảo rằng:
 - 1) thông tin xác thực bí mật của người sử dụng của tất cả các bên đều hợp lệ và được xác minh;
 - 2) các giao dịch được giữ bí mật;
 - 3) tính riêng tư của tất cả các bên liên quan được giữ lại;
- c) đường truyền thông giữa tất cả các bên liên quan được mã hóa;
- d) các giao thức sử dụng để truyền thông giữa tất cả các bên liên quan được đảm bảo;
- e) đảm bảo các chi tiết giao dịch nằm ngoài bất kỳ môi trường nào được lưu trữ, ví dụ trên một nền tảng lưu trữ hiện có trong mạng nội bộ của tổ chức, và không lưu lại và làm lộ môi trường lưu trữ có thể được truy cập trực tiếp từ mạng;
- f) khi sử dụng một tổ chức tin cậy (ví dụ cho các mục đích cấp và duy trì chữ ký số hoặc chứng thư số), an toàn được tích hợp và nhúng trong toàn bộ tiến trình quản lý từ khi bắt đầu đến kết thúc chứng thư/chữ ký.

Thông tin khác

Mức độ của các kiểm soát cần phải tương ứng với mức độ rủi ro gắn liền với từng loại hình giao dịch dịch vụ ứng dụng.

Các giao dịch có thể cần phải tuân thủ các yêu cầu pháp lý và quy định pháp luật về giao dịch trong các khâu tạo, xử lý, hoàn thành hoặc lưu trữ.

14.2 Bảo đảm an toàn trong các quá trình hỗ trợ và phát triển

Mục tiêu: Đảm bảo an toàn thông tin được thiết kế và thực hiện trong vòng đời phát triển của các hệ thống thông tin.

14.2.1 Chính sách phát triển an toàn

Kiểm soát

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

Hướng dẫn thi hành

Phát triển an toàn là một yêu cầu để xây dựng dịch vụ, kiến trúc, phần mềm và hệ thống an toàn. Trong chính sách phát triển an toàn, các khía cạnh sau cần được quan tâm:

- a) an toàn của môi trường phát triển;
- b) hướng dẫn về an toàn trong vòng đời phát triển của phần mềm;
 - 1) an toàn trong các phương thức phát triển phần mềm;
 - 2) hướng dẫn viết lệnh an toàn cho mỗi ngôn ngữ lập trình được sử dụng.
- c) yêu cầu an toàn trong giai đoạn thiết kế;
- d) điểm kiểm soát an toàn trong các mốc quan trọng của dự án;
- e) an toàn các kho lưu trữ;
- f) an toàn trong kiểm soát phiên bản;
- g) yêu cầu kiến thức về an toàn ứng dụng;
- h) khả năng của người phát triển trong việc tìm kiếm, tránh được và sửa các lỗ hổng.

Kỹ thuật lập trình an toàn cần được sử dụng cho cả phát triển mã nguồn mới và trong trường hợp tái sử dụng mã nguồn khi các tiêu chuẩn áp dụng cho phát triển có thể là không biết hoặc không phù hợp với thực tiễn tốt nhất hiện nay.

Nếu việc phát triển được thuê ngoài, tổ chức cần đảm bảo rằng việc phát triển từ bên ngoài phù hợp với các quy tắc cho phát triển an toàn (xem 14.2.7).

Thông tin khác

Việc phát triển cũng có thể diễn ra bên trong các ứng dụng, chẳng hạn như các ứng dụng văn phòng, các mã script, các trình duyệt và cơ sở dữ liệu.

14.2.2 Các thủ tục kiểm soát thay đổi hệ thống

Kiểm soát

Những thay đổi của hệ thống trong vòng đời phát triển cần được kiểm soát sử dụng các thủ tục kiểm soát thay đổi chính thức.

Hướng dẫn thi hành

Các thủ tục kiểm soát thay đổi chính thức cần được lập thành tài liệu và thi hành để đảm bảo tính toàn vẹn của hệ thống, các ứng dụng và sản phẩm, từ giai đoạn thiết kế ban đầu và đi qua tất cả các nỗ lực duy trì tiếp theo.

Việc đề xuất các hệ thống mới và những thay đổi quan trọng cho hệ thống hiện tại cần tuân theo một quá trình chính thức về lập tài liệu, đặc tả, kiểm tra, quản lý chất lượng và triển khai dưới sự quản lý.

Quá trình này cần bao gồm đánh giá rủi ro, phân tích những ảnh hưởng của các thay đổi, và đặc tả các biện pháp kiểm soát an toàn cần thiết. Quá trình này cũng phải đảm bảo rằng các thủ tục kiểm soát và an toàn hiện tại không bị ảnh hưởng, các lập trình viên hỗ trợ chỉ được phép truy cập đến các bộ phận hệ thống cần thiết cho công việc của họ, phải tuân theo và các thay đổi đều phải được chấp thuận và phê chuẩn chính thức.

Nếu khả thi thì các thủ tục kiểm soát thay đổi ứng dụng và vận hành cần được tích hợp ([xem 12.1.2](#)).

Các thủ tục kiểm soát thay đổi cần bao gồm nhưng không giới hạn những điều sau:

- a) duy trì hồ sơ về các mức cấp phép đã được chấp thuận;
- b) đảm bảo các thay đổi đều được thực thi bởi những người dùng được phép;
- c) soát xét các biện pháp kiểm soát và toàn bộ các thủ tục nhằm đảm bảo rằng chúng sẽ không bị ảnh hưởng bởi các thay đổi;
- d) xác định tất cả phần mềm, thông tin, các cơ sở dữ liệu, và phần cứng có yêu cầu sửa đổi;
- e) xác định và kiểm tra an toàn mã nguồn quan trọng để giảm thiểu khả năng xảy ra các lỗ hổng an toàn phổ biến;
- f) có được sự phê chuẩn chính thức cho các đề xuất chi tiết trước khi triển khai;
- g) đảm bảo rằng những người dùng hợp pháp chấp nhận các thay đổi trước khi triển khai;
- h) đảm bảo rằng bộ tài liệu hệ thống được cập nhật mỗi khi hoàn tất từng thay đổi và tài liệu cũ được lưu trữ hoặc bị loại bỏ;

- i) duy trì việc quản lý phiên bản đối với tất cả các cập nhật phần mềm;
- j) duy trì truy vết kiểm toán của tất cả các yêu cầu thay đổi;
- k) đảm bảo rằng tài liệu vận hành ([xem 12.1.1](#)) và các thủ tục người dùng được thay đổi khi cần thiết để duy trì sự phù hợp;
- l) đảm bảo rằng việc triển khai các thay đổi diễn ra đúng thời điểm và không làm ảnh hưởng đến các quá trình nghiệp vụ liên quan.

Thông tin khác

Việc thay đổi phần mềm có thể ảnh hưởng tới môi trường điều hành.

Kiểm nghiệm thực tiễn tốt sẽ bao hàm việc kiểm tra phần mềm mới trong một môi trường tách biệt với môi trường sản xuất và môi trường phát triển ([xem 12.1.4](#)). Đó cũng là một cách để quản lý phần mềm mới và cho phép bảo vệ sâu thêm các thông tin điều hành được sử dụng cho các mục đích kiểm tra. Các đối tượng cần bảo vệ bao gồm các bản vá, các gói dịch vụ và bản cập nhật khác.

Cập nhật bằng hình thức tự động có nguy cơ ảnh hưởng đến tính toàn vẹn và sẵn sàng của hệ thống và cần được cân nhắc với lợi ích của việc triển khai được nhanh các bản cập nhật. Không được sử dụng các cập nhật tự động trên các hệ thống quan trọng vì một số cập nhật có thể gây lỗi trên các ứng dụng quan trọng.

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

Kiểm soát

Khi nền tảng hệ điều hành thay đổi, các ứng dụng nghiệp vụ quan trọng cần được soát xét và kiểm tra lại nhằm đảm bảo không xảy ra các ảnh hưởng bất lợi tới hoạt động cũng như an toàn của tổ chức.

Hướng dẫn thi hành

Quá trình này cần bao gồm:

- a) soát xét biện pháp kiểm soát ứng dụng và toàn bộ các thủ tục nhằm đảm bảo rằng chúng không bị ảnh hưởng bởi các thay đổi của nền tảng hệ điều hành;
- b) đảm bảo rằng thông báo về các thay đổi hệ thống điều hành được đưa ra đúng thời điểm để cho phép thực hiện các kiểm tra và soát xét phù hợp trước khi triển khai;
- c) đảm bảo rằng những thay đổi phù hợp được triển khai cho các kế hoạch về liên tục của hoạt động nghiệp vụ ([xem điều 17](#)).

Thông tin khác

Các nền tảng hệ điều hành bao gồm hệ điều hành, cơ sở dữ liệu và các nền tảng trung gian. Việc kiểm soát này cũng cần áp dụng cho những thay đổi của các ứng dụng.

14.2.4 Hạn chế thay đổi các gói phần mềm

Kiểm soát

Việc sửa đổi các gói phần mềm là không được khuyến khích, cần hạn chế và chỉ thực hiện đối với các thay đổi rất cần thiết. Trong trường hợp này, mọi thay đổi cần phải được quản lý chặt chẽ.

Hướng dẫn thi hành

Miễn là có thể và khả thi, các gói phần mềm được nhà cung cấp hỗ trợ phải được sử dụng mà không bị sửa đổi. Nếu một gói phần mềm cần được sửa đổi thì phải quan tâm tới các vấn đề sau đây:

- a) rủi ro của các biện pháp kiểm soát được cài đặt sẵn và toàn bộ các quá trình đang bị ảnh hưởng;
- b) liệu có nhận được sự cho phép của nhà cung cấp không;
- c) khả năng nhận được các thay đổi được yêu cầu từ nhà cung cấp dưới dạng các cập nhật chương trình chuẩn;
- d) tác động nếu tổ chức phải có trách nhiệm trong việc bảo hành phần mềm trong tương lai do xảy ra các thay đổi;
- e) khả năng tương thích với các phần mềm sử dụng khác.

Nếu những thay đổi là cần thiết thì phần mềm gốc cần được lưu lại và những thay đổi phải được thực hiện trên một bản sao đã được xác định rõ. Một quá trình quản lý cập nhật phần mềm cần được thực hiện nhằm đảm bảo các bản vá đã được chấp thuận cập nhật gần nhất và các bản cập nhật ứng dụng đã được cài đặt cho tất cả phần mềm đã được cấp phép ([xem 12.6.1](#)). Tất cả các thay đổi cần được kiểm tra đầy đủ và được lập thành tài liệu để chúng có thể được áp dụng lại nếu cần thiết cho các nâng cấp phần mềm trong tương lai. Nếu được yêu cầu, các thay đổi phải được kiểm tra và được xác nhận bởi một tổ chức đánh giá độc lập.

14.2.5 Các nguyên tắc kỹ thuật an toàn hệ thống

Kiểm soát

Các nguyên tắc thiết kế hệ thống an toàn kỹ thuật cần được thiết lập, lập thành tài liệu, duy trì và áp dụng cho bất kỳ hệ thống thông tin nào đang cố gắng triển khai.

Hướng dẫn thi hành

Các thủ tục thiết kế kỹ thuật hệ thống thông tin an toàn dựa trên các nguyên tắc thiết kế kỹ thuật an toàn cần phải được thiết lập, lập thành tài liệu và áp dụng trong các hoạt động bên trong của hệ thống thông tin. Vấn đề an toàn cần phải được thiết kế vào tất cả các lớp kiến trúc (nghiệp vụ, dữ liệu, các ứng dụng và công nghệ) cân bằng các nhu cầu an toàn thông tin với sự cần thiết cho khả năng tiếp

cận. Công nghệ mới cần phải được phân tích rủi ro an toàn và thiết kế cần soát xét lại các mô hình tấn công đã được biết đến.

Các nguyên tắc và thủ tục thiết lập kỹ thuật cần thường xuyên soát xét để đảm bảo rằng chúng đang đóng góp có hiệu quả để nâng cao tiêu chuẩn an toàn trong quy trình kỹ thuật. Chúng cần thường xuyên được soát xét để đảm bảo rằng chúng vẫn cập nhật về các điều khoản chống lại bất kỳ mối đe dọa mới nào và còn áp dụng các tiến bộ trong công nghệ và giải pháp.

Các nguyên tắc kỹ thuật về an toàn được thiết lập cần được áp dụng, nếu có thể, cho các hệ thống thông tin thuê ngoài thông qua hợp đồng và các thỏa thuận ràng buộc khác giữa tổ chức và nhà cung cấp thuê ngoài. Tổ chức cần xác nhận các nguyên tắc kỹ thuật an toàn của nhà cung cấp là so sánh được với các nguyên tắc của tổ chức.

Thông tin khác

Các thủ tục phát triển ứng dụng cần áp dụng các kỹ thuật an toàn trong việc phát triển các ứng dụng có giao diện vào và ra. Các kỹ thuật an toàn cung cấp các hướng dẫn về xác thực người dùng, kiểm soát phiên và xác nhận dữ liệu an toàn, rà soát và loại bỏ các đoạn mã được dùng cho bẫy lối.

14.2.6 Môi trường phát triển an toàn

Kiểm soát

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

Hướng dẫn thi hành

Một môi trường phát triển an toàn bao gồm con người, quy trình và công nghệ gắn sự phát triển và hợp nhất hệ thống.

Các tổ chức cần phải đánh giá rủi ro liên quan tới sự phát triển của hệ thống và thiết lập môi trường an toàn trong nỗ lực phát triển hệ thống:

- a) độ nhạy cảm của dữ liệu được xử lý, lưu trữ và truyền qua hệ thống;
- b) áp dụng các yêu cầu cho bên ngoài và nội bộ, ví dụ từ các quy định và chính sách;
- c) các kiểm soát an toàn được thực hiện bởi các tổ chức hỗ trợ phát triển hệ thống;
- d) độ tin cậy của các nhân viên trong môi trường làm việc;
- e) trình độ gia công phần mềm gắn với sự phát triển của hệ thống;
- f) cần có sự phân biệt giữa các môi trường khác nhau;
- g) kiểm soát truy cập vào các môi trường phát triển;

- h) giám sát các thay đổi đối với môi trường và mã nguồn được lưu tại chỗ;
- i) các bản sao lưu được lưu trữ tại các địa điểm an toàn bên ngoài;
- j) kiểm soát sự di chuyển của dữ liệu gửi đến và xuất phát từ môi trường.

Một khi đã xác định được mức độ bảo vệ đối với một môi trường phát triển cụ thể, các tổ chức cần lập tài liệu các quy trình tương ứng theo các thủ tục phát triển an toàn và cung cấp cho tất cả các cá nhân và những người cần chúng.

14.2.7 Phát triển phần mềm thuê ngoài

Kiểm soát

Việc phát triển các phần mềm thuê ngoài cần được quản lý và giám sát bởi tổ chức.

Hướng dẫn thi hành

Trường hợp hệ thống là phần mềm thuê ngoài, các điểm sau đây cần được lưu ý trong toàn bộ chuỗi cung ứng bên ngoài tổ chức:

- a) các vấn đề liên quan đến bản quyền, quyền sở hữu mã, và quyền sở hữu trí tuệ liên quan đến các nội dung thuê ngoài ([xem 18.1.2](#));
- b) yêu cầu hợp đồng cho hoạt động thiết kế an toàn, lập trình và kiểm định ([xem 14.2.1](#));
- c) cung cấp mô hình mối đe dọa đã được phê duyệt cho các nhà phát triển bên ngoài;
- d) kiểm tra chấp nhận về chất lượng và độ chính xác của sản phẩm;
- e) cung cấp các bằng chứng cho thấy các ngưỡng an toàn đã được sử dụng để xác định các mức tối thiểu có thể chấp nhận về chất lượng an toàn và sự riêng tư;
- f) cung cấp bằng chứng cho thấy kiểm thử đầy đủ đã được áp dụng khi giao hàng để bảo vệ chống lại mã độc có hoặc không có chủ đích;
- g) cung cấp bằng chứng cho thấy kiểm thử đầy đủ đã được áp dụng để bảo vệ chống lại sự xuất hiện của các lỗ hổng đã biết;
- h) các thỏa thuận giao kèo, nếu mã nguồn không có sẵn;
- i) quyền theo hợp đồng để kiểm toán các quá trình phát triển và các biện pháp kiểm soát;
- j) tài liệu có hiệu lực của môi trường sử dụng để tạo ra các sản phẩm;
- k) tổ chức có trách nhiệm tuân thủ pháp luật và xác minh hiệu quả của các biện pháp kiểm soát.

Thông tin khác

Thông tin thêm về các mối quan hệ với nhà cung cấp có thể được tìm thấy trong ISO/IEC 27036 ^[21] ^[22] ^[23].

14.2.8 Kiểm thử an toàn của hệ thống

Kiểm soát

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

Hướng dẫn thi hành

Hệ thống mới hay cập nhật đều được yêu cầu kiểm thử và xác minh kỹ lưỡng trong suốt quá trình phát triển, bao gồm cả việc chuẩn bị một lịch trình chi tiết các hoạt động và đầu vào thử nghiệm và kết quả đầu ra dự kiến theo một chuỗi các điều kiện. Đối với các phát triển trong nhà, kiểm thử như vậy cần được thực hiện đầu tiên bởi đội ngũ phát triển. Kiểm thử chấp nhận độc lập sau đó cần thực hiện (cho cả phát triển trong nhà và thuê ngoài) để đảm bảo hệ thống hoạt động như mong đợi và chỉ như mong đợi (xem 14.1.1 và 14.2.9). Mức độ kiểm thử cần được cân đối với tầm quan trọng và tính chất của hệ thống.

14.2.9 Kiểm thử chấp nhận hệ thống

Kiểm soát

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

Hướng dẫn thi hành

Kiểm thử chấp nhận hệ thống cần bao gồm kiểm thử các yêu cầu an toàn thông tin (xem 14.1.1 và 14.1.2) và tuân thủ thực hành phát triển hệ thống an toàn (xem 14.2.1). Các kiểm thử cũng cần được tiến hành trên các thành phần nhận được và các hệ thống tích hợp. Các tổ chức có thể tận dụng công cụ tự động, chẳng hạn như các công cụ phân tích mã nguồn hoặc máy quét các lỗ hổng, và cần kiểm tra khắc phục các khiếm khuyết về an toàn liên quan.

Quá trình kiểm thử cần được thực hiện trong một môi trường thử nghiệm thực tế để đảm bảo rằng hệ thống sẽ không đưa các lỗ hổng vào môi trường của tổ chức và các kiểm thử này là đáng tin cậy.

14.3 Dữ liệu kiểm thử

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

14.3.1 Bảo vệ dữ liệu kiểm thử

Kiểm soát

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

Hướng dẫn thi hành

Việc sử dụng các dữ liệu điều hành chứa các thông tin cá nhân hay bất kỳ thông tin nhạy cảm nào khác cho các mục đích kiểm thử cần phải được ngăn chặn. Nếu thông tin cá nhân hay thông tin nhạy cảm khác được sử dụng cho các mục đích kiểm thử thì tất cả các chi tiết và nội dung nhạy cảm phải được xóa bỏ hoặc sửa đổi (xem ISO/IEC 29101^[26]).

Các hướng dẫn sau đây cần được áp dụng để bảo vệ dữ liệu điều hành khi chúng được sử dụng cho các mục đích kiểm thử:

- a) các thủ tục kiểm soát truy cập áp dụng cho các hệ thống ứng dụng điều hành cũng phải được áp dụng để kiểm thử các hệ thống ứng dụng;
- b) cần được chấp thuận mỗi khi thông tin điều hành được sao chép vào một môi trường kiểm thử;
- c) thông tin điều hành cần được xóa khỏi môi trường kiểm thử ngay khi việc kiểm thử đã hoàn tất;
- d) việc sao chép và sử dụng thông tin điều hành cần được ghi vào nhật ký nhằm cung cấp dấu vết cho việc kiểm toán.

Thông tin khác

Kiểm thử chấp nhận hệ thống thường yêu cầu lượng dữ liệu kiểm thử lớn gần sát với dữ liệu điều hành.

15 Các mối quan hệ với nhà cung cấp

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

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

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

Kiểm soát

Các yêu cầu an toàn thông tin để giảm thiểu những rủi ro gắn liền với quyền truy cập của nhà cung cấp đến tài sản của tổ chức cần được thỏa thuận với các nhà cung cấp và ghi thành văn bản.

Hướng dẫn thi hành

Tổ chức cần xác định và đưa ra chính sách kiểm soát an toàn thông tin đối với các nhà cung cấp đặc thù có quyền truy cập đến thông tin của tổ chức. Những kiểm soát này cần đề cập tới các quá trình và thủ tục cần được thực hiện bởi tổ chức, cũng như những quá trình và thủ tục mà tổ chức cần yêu cầu các nhà cung cấp thực hiện, bao gồm:

- a) xác định và lập hồ sơ các chủng loại nhà cung cấp, ví dụ như nhà cung cấp dịch vụ công nghệ thông tin, dịch vụ hậu cần, dịch vụ tài chính, các thành phần cơ sở hạ tầng công nghệ thông tin, các đối tượng mà tổ chức cho phép truy cập thông tin của mình;
- b) một quy trình và vòng đời được chuẩn hóa để quản lý các mối quan hệ nhà cung cấp;

- c) xác định các loại hình truy cập thông tin mà các chủng loại nhà cung cấp khác nhau sẽ được cho phép truy cập, và giám sát và kiểm soát truy cập;
- d) yêu cầu an toàn thông tin tối thiểu cho mỗi loại thông tin và mỗi loại truy cập để phục vụ như là cơ sở cho thỏa thuận với từng nhà cung cấp riêng dựa trên nhu cầu nghiệp vụ của tổ chức và các yêu cầu và hồ sơ rủi ro của nhà cung cấp;
- e) các quy trình, thủ tục giám sát việc tuân thủ các yêu cầu về an toàn thông tin được thiết lập cho từng loại hình nhà cung cấp và các loại hình hình truy cập, bao gồm đánh giá của bên thứ ba và xác nhận sản phẩm;
- f) các biện pháp kiểm soát chính xác và đầy đủ để đảm bảo tính toàn vẹn của thông tin hoặc xử lý thông tin được cung cấp bởi một trong hai bên;
- g) các loại nghĩa vụ áp dụng đối với nhà cung cấp để bảo vệ thông tin của tổ chức;
- h) việc xử lý sự cố và những dự phòng liên quan đến việc truy cập của nhà cung cấp bao gồm trách nhiệm của cả tổ chức và nhà cung cấp;
- i) khả năng hồi phục và, trong trường hợp cần thiết, việc phục hồi và sắp xếp dự phòng để đảm bảo sự sẵn sàng của các thông tin hay việc xử lý thông tin được cung cấp bởi một trong hai bên;
- j) đào tạo nâng cao nhận thức cho nhân viên của tổ chức có liên quan đến mua sắm theo các chính sách, quá trình và thủ tục đang áp dụng;
- k) đào tạo nâng cao nhận thức cho nhân viên của tổ chức trong quá trình làm việc với nhân viên của nhà cung cấp liên quan đến các quy định phù hợp cho việc tham gia và ứng xử dựa trên các chủng loại nhà cung cấp và mức độ truy cập của nhà cung cấp vào hệ thống và thông tin của tổ chức;
- l) các điều kiện để đảm bảo yêu cầu an toàn thông tin và các kiểm soát cần được ghi lại trong một thỏa thuận ký kết giữa hai bên;
- m) quản lý việc chuyển đổi thông tin, phương tiện xử lý thông tin cần thiết và tất cả các đồ cần phải được di chuyển, và đảm bảo rằng vấn đề an toàn thông tin được duy trì trong suốt giai đoạn di chuyển.

Thông tin khác

Thông tin có thể bị đặt vào nguy hiểm bởi các nhà cung cấp có quy trình quản lý an toàn thông tin không đầy đủ. Các kiểm soát cần phải được xác định và áp dụng để quản lý quyền truy cập của nhà cung cấp vào các trang thiết bị xử lý thông tin. Ví dụ, nếu có một nhu cầu đặc biệt về an toàn của các thông tin, một thỏa thuận không tiết lộ có thể được sử dụng đến. Một ví dụ khác là việc bảo vệ rủi ro dữ liệu khi thỏa thuận với các nhà cung cấp liên quan đến việc chuyển nhượng hoặc truy cập thông tin

qua biên giới. Các tổ chức cần phải nhận thức được rằng các quy định pháp luật hoặc quy định trong hợp đồng phải nêu rõ trách nhiệm bảo vệ thông tin trong tổ chức.

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

Kiểm soát

Tất cả các yêu cầu an toàn thông tin liên quan cần được thiết lập và thống nhất với từng nhà cung cấp về việc truy cập, xử lý, lưu trữ, giao tiếp, cung cấp các thành phần cơ sở hạ tầng công nghệ thông tin đối với thông tin của tổ chức.

Hướng dẫn thi hành

Thỏa thuận cung cấp cần được thiết lập và được lập thành tài liệu để đảm bảo rằng không có sự hiểu lầm nào giữa tổ chức và nhà cung cấp liên quan đến nghĩa vụ của hai bên để thực hiện các yêu cầu liên quan đến an toàn thông tin.

Các điều khoản sau đây cần được soát xét để đưa vào các thỏa thuận để đáp ứng các yêu cầu an toàn thông tin:

- a) mô tả về các thông tin được cung cấp hoặc truy cập và phương thức cung cấp hoặc truy cập thông tin;
- b) phân loại các thông tin theo hệ thống phân loại của tổ chức (xem 8.2); trong trường hợp cần thiết, cần lập sơ đồ ánh xạ giữa sơ đồ phân loại của tổ chức và sơ đồ phân loại của nhà cung cấp;
- c) yêu cầu pháp lý và quy định, bao gồm cả bảo vệ dữ liệu, quyền sở hữu trí tuệ và bản quyền, và có mô tả cụ thể các yêu cầu để đảm bảo rằng các quy định đó được đáp ứng;
- d) nghĩa vụ của mỗi bên tham gia hợp đồng đã thống nhất để thực hiện một tập hợp các kiểm soát bao gồm kiểm soát truy cập, đánh giá hiệu quả, giám sát, báo cáo và kiểm toán;
- e) quy tắc sử dụng thông tin đã thỏa thuận, bao gồm cả sử dụng thông tin chưa thỏa thuận trong trường hợp cần thiết;
- f) có danh sách rõ ràng các nhân viên nhà cung cấp có quyền truy cập hoặc nhận thông tin của tổ chức; có các thủ tục hoặc các điều kiện cho quyền và loại bỏ việc cấp quyền truy cập hoặc tiếp nhận thông tin của tổ chức đối với nhân viên nhà cung cấp;
- g) chính sách an toàn thông tin liên quan đến các hợp đồng cụ thể;
- h) yêu cầu và thủ tục quản lý sự cố (đặc biệt là việc thông báo và phối hợp trong quá trình khắc phục sự cố);
- i) yêu cầu về đào tạo và nâng cao nhận thức đối với các thủ tục đặc thù và yêu cầu an toàn thông tin, ví dụ cho việc ứng phó sự cố, thủ tục cấp quyền;
- j) các quy định có liên quan đối với thầu phụ, bao gồm các kiểm soát phải được thực hiện;

- k) thỏa thuận có liên quan đến đối tác, trong đó quy định một người liên lạc cho các vấn đề an toàn thông tin;
- l) các yêu cầu sàng lọc, nếu có, đối với nhân viên của nhà cung cấp bao gồm cả trách nhiệm tiến hành sàng lọc và các thủ tục thông báo nếu việc sàng lọc không được hoàn thành hoặc nếu kết quả gây ra sự nghi ngờ hoặc lo lắng;
- m) quyền kiểm toán các quy trình của nhà cung cấp và các kiểm soát liên quan đến thỏa thuận;
- n) các quy trình giải quyết lỗi và giải quyết xung đột;
- o) nghĩa vụ của nhà cung cấp định kỳ cung cấp một báo cáo độc lập về hiệu quả của các kiểm soát theo thỏa thuận và chấn chỉnh kịp thời các vấn đề có liên quan được nêu ra trong báo cáo;
- p) các nghĩa vụ của nhà cung cấp phải thực hiện theo các yêu cầu an toàn của tổ chức.

Thông tin khác

Các thỏa thuận có thể thay đổi đáng kể giữa các tổ chức khác nhau và giữa các nhà cung cấp khác nhau. Vì vậy, cần thận trọng để đảm bảo thỏa thuận đã bao gồm tất cả các rủi ro an toàn thông tin có liên quan và các yêu cầu. Thỏa thuận với nhà cung cấp cũng có thể liên quan đến các bên khác (ví dụ như nhà cung cấp phụ).

Các thủ tục để xử lý liên tục trong tình huống nhà cung cấp không thể tiếp tục cung cấp sản phẩm hoặc dịch vụ của họ cần phải được đề cập trong các thỏa thuận để tránh bất kỳ sự chậm trễ nào trong việc thu xếp các sản phẩm hoặc dịch vụ thay thế.

15.1.3 Chuỗi cung ứng công nghệ thông tin và truyền thông

Kiểm soát

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

Hướng dẫn thi hành

Các vấn đề sau đây cần được xem xét để đưa vào các thỏa thuận với nhà cung cấp liên quan đến đảm bảo an toàn chuỗi cung ứng:

- a) xác định các yêu cầu an toàn thông tin để áp dụng cho mua sắm các sản phẩm hay dịch vụ công nghệ thông tin và truyền thông, bổ sung vào trong các yêu cầu an toàn thông tin chung theo các mối quan hệ nhà cung cấp;
- b) đối với các dịch vụ công nghệ thông tin và truyền thông, yêu cầu các nhà cung cấp truyền bá yêu cầu an toàn của tổ chức trong suốt chuỗi cung ứng nếu nhà cung ứng có hợp đồng phụ với các bộ phận cung cấp dịch vụ công nghệ thông tin và truyền thông cho tổ chức;

- c) đối với các sản phẩm công nghệ thông tin và truyền thông, yêu cầu các nhà cung cấp truyền bá các thực hành an toàn thích hợp trong suốt chuỗi cung ứng nếu các sản phẩm này bao gồm các thành phần được mua từ các nhà cung cấp khác;
- d) triển khai một quy trình giám sát và các phương pháp có thể chấp nhận để xác nhận rằng sản phẩm và dịch vụ công nghệ thông tin và truyền thông đã đáp ứng các yêu cầu an toàn;
- e) triển khai một quy trình để xác định các thành phần sản phẩm hoặc dịch vụ rất quan trọng cho việc duy trì chức năng của tổ chức và do đó đòi hỏi tăng cường sự chú ý và soát xét kỹ lưỡng khi thuê bên ngoài tổ chức thực hiện, đặc biệt trong trường hợp nhà cung cấp chính cho tổ chức lại tiếp tục thuê ngoài một vài khía cạnh của thành phần sản phẩm hoặc dịch vụ đó cho nhà cung cấp khác;
- f) có được sự đảm bảo rằng các thành phần quan trọng và nguồn gốc của chúng có thể được truy vết suốt chuỗi cung ứng;
- g) có được sự đảm bảo rằng các sản phẩm công nghệ thông tin và truyền thông khi chuyển giao ngoài việc hoạt động đúng như tổ chức mong muốn còn phải không có bất kỳ tính năng bất thường hoặc chức năng không mong muốn nào khác;
- h) xác định các quy tắc rõ ràng cho việc chia sẻ các thông tin liên quan đến chuỗi cung ứng và bất kỳ vấn đề tiềm năng nào và các thỏa hiệp giữa các tổ chức và các nhà cung cấp;
- i) triển khai các quy trình đặc thù để quản lý vòng đời và tính sẵn sàng của các thành phần công nghệ thông tin và truyền thông liên quan đến vấn đề rủi ro an toàn. Điều này cũng bao gồm quy trình quản lý rủi ro đối với các thành phần không còn sẵn sàng cho các nhà cung cấp, không còn trong quy trình nghiệp vụ, hay các nhà cung cấp không còn cung cấp các thành phần này do tiến bộ của công nghệ thông tin và truyền thông.

Thông tin khác

Các bài thực hành quản lý rủi ro chuỗi cung ứng công nghệ thông tin và truyền thông được xây dựng ở vị trí quan trọng hàng đầu trong chính sách an toàn thông tin chung, quản lý chất lượng, quản lý dự án và kỹ thuật hệ thống, nhưng không được thay thế chúng.

Tổ chức cần làm việc với nhà cung cấp để hiểu được rõ chuỗi cung ứng công nghệ thông tin và truyền thông và các vấn đề có ảnh hưởng quan trọng trên các sản phẩm và dịch vụ được cung cấp. Tổ chức có thể gây ảnh hưởng đến thực hành an toàn thông tin trong chuỗi cung ứng công nghệ thông tin và truyền thông bằng cách làm rõ trong thỏa thuận với các nhà cung cấp tất cả những vấn đề cần được giải quyết bởi các nhà cung cấp khác trong chuỗi cung ứng công nghệ thông tin và truyền thông.

Chuỗi cung ứng công nghệ thông tin và truyền thông được đề cập ở đây bao gồm cả dịch vụ điện toán đám mây.

15.2 Quản lý chuyển giao dịch vụ của nhà cung cấp

Mục tiêu: Để duy trì một mức độ đồng thuận về an toàn thông tin và cung cấp dịch vụ phù hợp thỏa thuận với nhà cung cấp.

15.2.1 Giám sát và soát xét dịch vụ của nhà cung cấp

Kiểm soát

Các tổ chức cần thường xuyên theo dõi, soát xét và kiểm toán nhà cung cấp dịch vụ giao hàng.

Hướng dẫn thi hành

Theo dõi và soát xét các nhà cung cấp dịch vụ phải đảm bảo rằng các điều khoản an toàn thông tin và điều kiện của thỏa thuận đang được tôn trọng và các sự cố an toàn thông tin và các vấn đề được quản lý một cách đúng đắn.

Điều này sẽ liên quan đến một quy trình quản lý mối quan hệ về dịch vụ giữa các tổ chức và các nhà cung cấp để:

- a) giám sát mức độ hiệu quả của dịch vụ để xác nhận việc tuân thủ các thỏa thuận;
- b) soát xét báo cáo dịch vụ được lập bởi các nhà cung cấp và thường xuyên sắp xếp các cuộc họp về tiến độ theo yêu cầu của thỏa thuận;
- c) tiến hành kiểm toán các nhà cung cấp, kết hợp với đánh giá của báo cáo kiểm toán độc lập, nếu có, và theo sát các vấn đề đã được xác định;
- d) cung cấp thông tin về sự cố an toàn thông tin và soát xét thông tin này theo yêu cầu của các thỏa thuận và các hướng dẫn và thủ tục hỗ trợ;
- e) soát xét những dấu vết kiểm toán nhà cung cấp và hồ sơ về các sự kiện an toàn thông tin, các vấn đề hoạt động, các lỗi, truy tìm các lỗi và sự gián đoạn liên quan đến các dịch vụ giao hàng;
- f) giải quyết và quản lý bất kỳ vấn đề nào đã được xác định;
- g) soát xét các khía cạnh an toàn thông tin trong mối quan hệ của nhà cung cấp với các nhà cung cấp riêng của họ;
- h) đảm bảo rằng các nhà cung cấp duy trì khả năng phục vụ đầy đủ cùng với một kế hoạch khả thi được xây dựng để đảm bảo rằng mức độ cung cấp dịch vụ liên tục theo đúng thỏa thuận sẽ được duy trì kể cả trong trường hợp dịch vụ chính bị lỗi hay gặp thảm họa (xem điều 17).

Trách nhiệm quản lý các mối quan hệ với nhà cung cấp cần được giao cho một cá nhân được chỉ định hoặc đội ngũ quản lý dịch vụ. Ngoài ra, tổ chức phải đảm bảo rằng các nhà cung cấp bị gắn trách nhiệm với việc soát xét sự tuân thủ và thực thi các yêu cầu của thỏa thuận. Các cán bộ phải có kỹ năng chuyên môn đầy đủ và nguồn lực cần được đảm bảo sẵn sàng để giám sát các yêu cầu của thỏa

thuận, đặc biệt là các yêu cầu về an toàn thông tin, phải được đáp ứng. Hành động thích hợp cần được thực hiện khi quan sát thấy có thiếu hụt trong việc cung cấp dịch vụ.

Tổ chức cần giữ lại kiểm soát tổng thể đầy đủ và khả năng hiển thị tất cả các khía cạnh an toàn cho thông tin nhạy cảm hoặc quan trọng hoặc phương tiện xử lý thông tin được truy cập, xử lý hoặc quản lý bởi một nhà cung cấp. Tổ chức cần giữ lại thông tin quan sát được về các hoạt động an toàn như: quản lý thay đổi, xác định các lỗ hổng và các báo cáo sự cố an toàn thông tin và ứng phó thông qua một quy trình báo cáo đã xác định trước.

15.2.2 Quản lý thay đổi của dịch vụ cung cấp

Kiểm soát

Các thay đổi đối với việc cung cấp dịch vụ của nhà cung cấp, bao gồm việc duy trì và cải tiến chính sách an toàn thông tin, các thủ tục và kiểm soát, cần được quản lý, có tính đến các mức độ quan trọng của các thông tin nghiệp vụ, các hệ thống và các quy trình có liên quan và đánh giá lại các rủi ro.

Hướng dẫn thi hành

Các khía cạnh sau đây cần được soát xét đến:

- a) các thay đổi về thỏa thuận với nhà cung cấp;
- b) các thay đổi được thực hiện bởi tổ chức nhằm:
 - 1) cải tiến các dịch vụ đang được cung cấp;
 - 2) phát triển các ứng dụng và hệ thống mới;
 - 3) chỉnh sửa hoặc cập nhật các chính sách và thủ tục của tổ chức;
 - 4) các kiểm soát mới hoặc bị thay đổi để giải quyết các sự cố an toàn thông tin và cải tiến an toàn;
- c) các thay đổi trong nhà cung cấp dịch vụ để thực hiện:
 - 1) thay đổi và cải tiến mạng lưới;
 - 2) sử dụng các công nghệ mới;
 - 3) áp dụng các sản phẩm mới hoặc phiên bản/xuất bản mới hơn;
 - 4) các công cụ và môi trường phát triển mới;
 - 5) thay đổi đối với vị trí vật lý của các cơ sở dịch vụ;
 - 6) thay đổi nhà cung cấp;
 - 7) ký hợp đồng phụ với nhà cung cấp khác.

16 Quản lý sự cố an toàn thông tin

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

Mục tiêu: Để đảm bảo một cách tiếp cận phù hợp và hiệu quả nhằm quản lý sự cố an toàn thông tin, bao gồm thông tin về các sự kiện an toàn thông tin và lỗ hổng.

16.1.1 Trách nhiệm và thủ tục

Kiểm soát

Các thủ tục và trách nhiệm 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.

Hướng dẫn thi hành

Các hướng dẫn sau đây về trách nhiệm và quy trình quản lý liên quan đến hoạt động quản lý sự cố an toàn thông tin cần phải được quan tâm:

- a) Trách nhiệm quản lý cần được thiết lập để đảm bảo rằng các thủ tục sau đây được phát triển và truyền đạt đầy đủ trong tổ chức:
 - 1) Thủ tục lập kế hoạch và chuẩn bị ứng phó sự cố;
 - 2) Thủ tục giám sát, phát hiện, phân tích và báo cáo các sự kiện an toàn thông tin và sự cố;
 - 3) Thủ tục cho việc ghi nhật ký các hoạt động quản lý sự cố;
 - 4) Thủ tục xử lý các bằng chứng pháp lý;
 - 5) Thủ tục đánh giá, quyết định về sự kiện an toàn thông tin và đánh giá lỗ hổng an toàn thông tin;
 - 6) Thủ tục cho việc ứng phó, bao gồm các vấn đề leo thang sự cố, phục hồi có kiểm soát từ một sự cố và thông tin với những người ở trong hay ngoài tổ chức;
- b) Thủ tục thiết lập phải đảm bảo rằng:
 - 1) nhân viên có chuyên môn xử lý các vấn đề liên quan đến sự cố an toàn thông tin ở trong tổ chức;
 - 2) một đầu mối liên lạc để phát hiện và báo cáo sự cố an toàn cần được triển khai thực hiện;
 - 3) việc liên lạc phù hợp với các cơ quan có thẩm quyền, các nhóm lợi ích bên ngoài hoặc các diễn đàn có thể xử lý các vấn đề liên quan đến sự cố an toàn thông tin cần được duy trì;
- c) các thủ tục báo cáo phải bao gồm:

- 1) chuẩn bị biểu mẫu báo cáo về sự cố an toàn thông tin để hỗ trợ các hoạt động báo cáo và giúp người báo cáo nhớ tất cả các hành động cần thiết trong trường hợp xảy ra một sự cố an toàn thông tin;
- 2) các thủ tục được thực hiện trong trường hợp xảy ra một sự cố an toàn thông tin, ví dụ như ghi lại các chi tiết ngay lập tức, chẳng hạn như loại không tuân thủ hoặc có vi phạm, thực hiện sai chức năng, các thông điệp trên màn hình và ngay lập tức báo cáo với đầu mối liên lạc và chỉ thực hiện những hành động phối hợp;
- 3) tham chiếu đến một quy trình xử lý kỷ luật chính thức được thiết lập để áp dụng với những nhân viên vi phạm cam kết an toàn;
- 4) quy trình phản hồi phù hợp để đảm bảo rằng những người báo cáo các sự kiện an toàn thông tin được thông báo về kết quả sau khi vấn đề đã được xử lý và đóng lại.

Các mục tiêu của việc quản lý sự cố an toàn thông tin cần được ban lãnh đạo thông qua, và cũng cần đảm bảo rằng những người có trách nhiệm trong việc quản lý sự cố an toàn thông tin đều hiểu rõ quyền ưu tiên của tổ chức đối với việc xử lý các sự cố an toàn thông tin.

Thông tin khác

Các sự cố an toàn thông tin có thể vượt ra ngoài ranh giới của tổ chức và ranh giới quốc gia. Để phản ứng lại các sự cố như vậy cần nâng cao yêu cầu phối hợp ứng cứu và chia sẻ thông tin về các sự cố với các tổ chức bên ngoài một cách phù hợp.

Hướng dẫn chi tiết về quản lý sự cố an toàn thông tin được cung cấp trong ISO/IEC 27035^[20].

16.1.2 Báo cáo các sự kiện an toàn thông tin

Kiểm soát

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.

Hướng dẫn thi hành

Toàn bộ nhân viên và những người thuộc các nhà thầu đều phải nhận thức được các trách nhiệm của họ trong việc báo cáo các sự kiện an toàn thông tin theo cách nhanh nhất có thể. Họ cũng cần biết rõ các thủ tục báo cáo các sự kiện an toàn thông tin và đầu mối liên lạc.

Các tình huống được soát xét để báo cáo sự kiện an toàn thông tin bao gồm:

- a) kiểm soát an toàn không hiệu quả;
- b) vi phạm mức mong đợi về tính toàn vẹn, tính bí mật hoặc tính sẵn sàng thông tin;
- c) lỗi của con người;
- d) không tuân thủ các chính sách hoặc hướng dẫn;

- e) vi phạm các thỏa thuận an ninh về mặt vật lý;
- f) thay đổi hệ thống không kiểm soát được;
- g) trực trặc của phần mềm hoặc phần cứng;
- h) vi phạm truy cập.

Thông tin khác

Hành vi sai chức năng hoặc bất thường của hệ thống có thể là một chỉ báo về một cuộc tấn công an toàn thông tin hoặc một vi phạm an toàn thông tin thực tế và vì thế cần được báo cáo như là một sự kiện an toàn thông tin.

16.1.3 Báo cáo các lỗ hổng an toàn thông tin

Kiểm soát

Mọi nhân viên, nhà thầu sử dụng các dịch vụ và hệ thống thông tin cần được yêu cầu ghi lại và báo cáo bất kỳ lỗ hổng nào về an toàn quan sát được hoặc cảm thấy nghi ngờ trong các hệ thống hoặc dịch vụ.

Hướng dẫn thi hành

Tất cả các nhân viên và nhà thầu đều phải báo cáo về những vấn đề này tới đầu mối liên lạc theo cách nhanh nhất có thể nhằm ngăn chặn các sự cố an toàn thông tin. Cơ cấu báo cáo cần phải dễ dàng, dễ truy cập và sẵn sàng tối đa.

Thông tin khác

Các nhân viên và nhà thầu cần được tư vấn không cần cỗ gắng chứng minh về các lỗ hổng bị nghi ngờ. Việc kiểm tra các lỗ hổng có thể được hiểu như một sự tiềm ẩn lạm dụng hệ thống và cũng có thể gây thiệt hại cho các hệ thống hoặc dịch vụ thông tin và dẫn đến trách nhiệm pháp lý của cá nhân thực hiện việc kiểm tra.

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

Kiểm soát

Các sự kiện an toàn thông tin cần được đánh giá và cần được quyết định phân loại là sự cố an toàn thông tin.

Hướng dẫn thi hành

Đầu mối liên hệ cần đánh giá mỗi sự kiện an toàn thông tin bằng cách sử dụng thang phân loại sự kiện an toàn thông tin và sự cố an toàn thông tin đã nhất trí để quyết định xem liệu sự kiện này có được

phân loại như một sự cố an toàn thông tin. Việc phân loại và xếp ưu tiên các sự cố có thể giúp xác định các tác động và phạm vi ảnh hưởng của sự cố.

Trong trường hợp tổ chức đã có một đội ứng phó sự cố an toàn thông tin (ISIRT), các đánh giá và quyết định có thể được chuyển tiếp đến các ISIRT để xác nhận hoặc đánh giá lại.

Kết quả của việc đánh giá và quyết định cần phải được ghi lại chi tiết cho mục đích tham chiếu và xác minh trong tương lai.

16.1.5 Ứng phó sự cố an toàn thông tin

Kiểm soát

Sự cố an toàn thông tin cần được ứng phó phù hợp với các thủ tục đã được lập tài liệu.

Hướng dẫn thi hành

Sự cố an toàn thông tin cần được ứng phó bởi một đầu mối liên hệ được đề cử và những người khác có liên quan trong hoặc bên ngoài tổ chức (xem 16.1.1).

Các ứng phó cần bao gồm những điều sau đây:

- a) thu thập bằng chứng càng sớm càng tốt sau khi xảy ra;
- b) tiến hành phân tích pháp lý an toàn thông tin, theo yêu cầu (xem 16.1.7);
- c) leo thang, theo yêu cầu;
- d) đảm bảo rằng tất cả các hoạt động ứng phó liên quan được ghi nhật ký đúng cách phục vụ phân tích sau này;
- e) thông tin về sự tồn tại của các sự cố an toàn thông tin hoặc bất kỳ thông tin chi tiết nào có liên quan đến người bên trong và bên ngoài tổ chức có nhu cầu để biết;
- f) giải quyết (các) lỗ hổng an toàn thông tin đã được phát hiện gây ra hoặc góp phần gây ra sự cố;
- g) một khi sự cố đã được xử lý thành công, cần chính thức đóng lại và lập hồ sơ.

Phân tích sau sự cố cần được thực hiện, khi cần thiết, để xác định nguồn gốc của sự cố.

Thông tin khác

Mục đích trước tiên của ứng phó sự cố là trở lại "mức độ an toàn thông thường" và sau đó khởi tạo quá trình phục hồi cần thiết.

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

Kiểm soát

Kiến thức thu được từ việc phân tích và giải quyết các sự cố an toàn thông tin cần được sử dụng để giảm thiểu khả năng xảy ra hoặc giảm thiểu ảnh hưởng của các sự cố trong tương lai.

Hướng dẫn thi hành

Cần có cơ chế hợp lý để cho phép phân loại, xác định khối lượng, chi phí liên quan đến sự cố an toàn thông tin để định lượng và theo dõi. Thông tin thu được từ việc đánh giá sự cố an toàn thông tin cần được sử dụng để xác định các sự cố lặp lại và sự cố có tác động lớn.

Thông tin khác

Việc đánh giá các sự cố an toàn thông tin có thể chỉ ra sự cần thiết phải tăng cường hoặc bổ sung các biện pháp kiểm soát nhằm hạn chế tần suất, thiệt hại và chi phí của các sự cố trong tương lai, hoặc phải xem xét sử dụng quy trình soát xét chính sách an toàn (xem 5.1.2)

Với sự quan tâm xứng đáng cho khía cạnh an toàn, những thông tin có được từ những sự cố an toàn thông tin thực tế có thể được sử dụng trong đào tạo nhận thức người dùng (xem 7.2.2) như là ví dụ về những gì có thể xảy ra, cách thức ứng phó đối với các sự cố như vậy và làm thế nào để tránh các sự cố tương tự trong tương lai.

16.1.7 Thu thập bằng chứng

Kiểm soát

Các tổ chức phải xác định và áp dụng các thủ tục cho việc xác định, tập hợp, thu nhận, bảo quản thông tin có thể phục vụ làm bằng chứng.

Hướng dẫn thi hành

Các thủ tục nội bộ cần được phát triển và tuân thủ khi làm việc với bằng chứng cho mục đích xử lý kỷ luật và hoạt động pháp lý.

Nói chung, các thủ tục về bằng chứng cần cung cấp các quy trình xác định, tập hợp, thu nhận và bảo quản bằng chứng tuân thủ tương ứng với các loại lưu trữ, thiết bị và trạng thái thiết bị khác nhau, ví dụ bật nguồn hoặc tắt nguồn. Các thủ tục này cần phải tính đến:

- a) chuỗi giám sát;
- b) an toàn của bằng chứng;
- c) an toàn của nhân viên;
- d) vai trò và trách nhiệm của nhân viên tham gia;
- e) năng lực của nhân viên;
- f) lập tài liệu;
- g) báo cáo tóm tắt.

Trường hợp sẵn có, các chứng nhận hoặc các thẻ loại khác phản ánh trình độ của nhân viên và các công cụ cần được tìm kiếm, để cung cấp giá trị của bằng chứng bảo quản.

Bằng chứng pháp lý có thể vượt qua ranh giới tổ chức hoặc cấp có thẩm quyền phán quyết. Trong trường hợp như vậy, phải đảm bảo rằng tổ chức có quyền thu thập các thông tin cần thiết như là bằng chứng pháp lý. Các yêu cầu mức độ pháp lý khác nhau cũng cần được soát xét để tối đa hóa cơ hội tiếp nhận trên các lĩnh vực pháp lý có liên quan.

Thông tin khác

Xác định là quá trình liên quan đến việc tìm kiếm, nhận diện và lập tài liệu về các bằng chứng tiềm năng. Tập hợp là quá trình thu thập các đối tượng vật lý mà có thể chứa các bằng chứng tiềm năng. Thu nhận là quá trình tạo ra một bản sao của dữ liệu trong một tập hợp xác định. Bảo quản là quá trình duy trì và bảo vệ sự toàn vẹn và các điều kiện ban đầu của bằng chứng tiềm năng.

Khi một sự kiện an toàn thông tin được phát hiện lần đầu, có thể không xác định rõ ràng liệu sự kiện đó có phải đưa ra tòa hay không. Vì vậy, tồn tại một nguy cơ rằng bằng chứng cần thiết có thể vô tình hoặc cố ý bị phá hủy trước khi mức độ nghiêm trọng của vụ việc được nhận ra. Do vậy, cần sớm có tham gia của một luật sư hoặc cảnh sát trong mọi hành động pháp lý dự kiến thực hiện và được tư vấn về bằng chứng.

ISO/IEC 27037^[24] cung cấp hướng dẫn cho việc xác định, tập hợp, thu nhận và bảo quản bằng chứng số.

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

17.1 An toàn thông tin liên tục

Mục tiêu: An toàn thông tin liên tục cần phải được đặt trong hệ thống quản lý hoạt động nghiệp vụ liên tục của tổ chức.

17.1.1 Lập kế hoạch an toàn thông tin liên tục

Kiểm soát

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

Hướng dẫn thi hành

Một tổ chức phải xác định sự liên tục của an toàn thông tin được thiết lập trong quy trình quản lý hoạt động nghiệp vụ liên tục hoặc trong quy trình quản lý phục hồi sau thảm họa. Các yêu cầu an toàn thông tin cần được xác định khi lập kế hoạch cho hoạt động nghiệp vụ liên tục và khôi phục sau thảm họa.

Trong trường hợp thiếu các kế hoạch nghiệp vụ liên tục và kế hoạch khắc phục thảm họa an toàn thông tin, cần giả định rằng các yêu cầu an toàn thông tin vẫn như cũ, trong điều kiện hoạt động bình

thường, và đáp ứng yêu cầu hoạt động nghiệp vụ liên tục trong điều kiện hoạt động bình thường. Ngoài ra, một tổ chức có thể thực hiện phân tích tác động nghiệp vụ cho các khía cạnh an toàn thông tin để xác định các yêu cầu an toàn thông tin đối với các tình huống bất lợi.

Thông tin khác

Để giảm thời gian và nỗ lực của việc thêm một phân tích tác động nghiệp vụ cho an toàn thông tin, tổ chức được khuyến khích nắm bắt các khía cạnh an toàn thông tin trong quản lý nghiệp vụ liên tục bình thường hoặc đánh giá tác động quản lý nghiệp vụ phục hồi sau thảm họa. Điều này thể hiện rằng các yêu cầu an toàn thông tin liên tục được xây dựng một cách rõ ràng trong quản lý nghiệp vụ liên tục hoặc quy trình quản lý phục hồi sau thảm họa.

Thông tin về quản lý nghiệp vụ liên tục có thể được tìm thấy trong ISO/IEC 27031^[14], ISO 22313^[9] và ISO 22301^[8].

17.1.2 Triển khai đảm bảo an toàn thông tin liên tục

Kiểm soát

Tổ chức phải thiết lập, lập tài liệu, thực hiện và duy trì các quy trình, thủ tục, biện pháp kiểm soát để đảm bảo mức độ yêu cầu về tính liên tục cho an toàn thông tin trong mọi tình huống bất lợi.

Hướng dẫn thi hành

Một tổ chức phải đảm bảo rằng:

- a) có một cấu trúc quản lý thích hợp để chuẩn bị trước, giảm thiểu và ứng phó với một sự cố, trong đó sử dụng các cán bộ được trao thẩm quyền cần thiết, có kinh nghiệm và năng lực;
- b) cán bộ ứng phó sự cố được đề cử phải có tinh thần trách nhiệm, đủ quyền hạn và thẩm quyền quản lý và xử lý một sự cố và duy trì an toàn thông tin;
- c) các kế hoạch được lập tài liệu, các thủ tục ứng phó và phục hồi sau sự cố cần được phát triển và được phê duyệt, có chi tiết cách thức tổ chức sẽ quản lý một sự cố và sẽ duy trì an toàn thông tin của tổ chức đến một mức độ đã xác định trước, dựa trên các mục tiêu quản lý an toàn thông tin liên tục đã được thông qua (xem 17.1.1).

Theo yêu cầu an toàn thông tin liên tục, tổ chức cần thành lập, xây dựng tài liệu, thực hiện và duy trì:

- a) kiểm soát an toàn thông tin trong quy trình nghiệp vụ liên tục hoặc quy trình phục hồi thảm họa, các thủ tục, hệ thống và công cụ hỗ trợ;
- b) các quy trình, thủ tục và thực hiện những thay đổi để duy trì các biện pháp kiểm soát an toàn thông tin hiện hành trong các tình huống bất lợi;

- c) hỗ trợ kiểm soát cho các biện pháp kiểm soát an toàn thông tin không thể được duy trì trong một tình huống bất lợi.

Thông tin khác

Trong ngữ cảnh nghiệp vụ liên tục hoặc phục hồi sau thảm họa, các quy trình và thủ tục cụ thể có thể được xác định. Các thông tin được xử lý trong các quy trình và thủ tục này hoặc trong các hệ thống thông tin chuyên dụng hỗ trợ thông tin cần được bảo vệ. Do đó một tổ chức cần mời các chuyên gia an toàn thông tin khi thiết lập, thực hiện và duy trì nghiệp vụ liên tục hoặc các quy trình và thủ tục phục hồi sau thảm họa.

Các biện pháp kiểm soát an toàn thông tin đã được thực hiện cần tiếp tục hoạt động trong tình huống bất lợi. Nếu các kiểm soát an toàn không thể tiếp tục bảo đảm an toàn thông tin, các kiểm soát khác cần được thiết lập, thực hiện và duy trì để đảm bảo một mức độ chấp nhận được của an toàn thông tin.

17.1.3 Xác minh, soát xét và đánh giá an toàn thông tin liên tục

Kiểm soát

Các tổ chức cần xác minh các kiểm soát an toàn thông tin liên tục đã thiết lập và thực hiện một cách đều đặn để đảm bảo rằng chúng là hợp lệ và có hiệu quả trong những tình huống bất lợi.

Hướng dẫn thi hành

Các thay đổi mang tính tổ chức, kỹ thuật, thủ tục và quy trình, cho dù trong ngữ cảnh vận hành và liên tục, có thể dẫn đến những thay đổi trong các yêu cầu về an toàn thông tin liên tục. Trong trường hợp này, tính liên tục của các quy trình, thủ tục và kiểm soát cho an toàn thông tin cần được soát xét lại nhằm đáp ứng những yêu cầu thay đổi.

Các tổ chức cần xác minh quy trình quản lý an toàn thông tin liên tục của mình bằng cách:

- a) thực hành và kiểm tra chức năng của các quy trình an toàn thông tin liên tục, các thủ tục và kiểm soát để đảm bảo rằng chúng phù hợp với các mục tiêu an toàn thông tin liên tục;
- b) thực hành và kiểm tra kiến thức và thói quen hoạt động an toàn thông tin liên tục, các quy trình, thủ tục và kiểm soát để đảm bảo rằng hoạt động của chúng là phù hợp với mục tiêu an toàn thông tin liên tục;
- c) soát xét hiệu lực và hiệu quả của các biện pháp an toàn thông tin liên tục khi hệ thống thông tin, quy trình an toàn thông tin, thủ tục và kiểm soát hoặc quy trình quản lý nghiệp vụ liên tục/quản lý phục hồi thảm họa và các giải pháp thay đổi.

Thông tin khác

Việc xác minh kiểm soát an toàn thông tin liên tục là khác với các kiểm tra an toàn thông tin chung, xác minh cần được thực hiện bên cạnh việc thử nghiệm các thay đổi. Nếu có thể, sẽ là thích hợp hơn để

tích hợp xác minh các kiểm soát an toàn thông tin liên tục với các kiểm tra nghiệp vụ liên tục hoặc kiểm tra phục hồi thảm họa của tổ chức.

17.2 Dự phòng

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

17.2.1 Tính sẵn sàng của phương tiện xử lý thông tin

Kiểm soát

Các phương tiện xử lý thông tin cần được triển khai với dự phòng đủ để đáp ứng các yêu cầu sẵn có.

Hướng dẫn thi hành

Các tổ chức cần xác định các yêu cầu nghiệp vụ cho sự sẵn sàng của các hệ thống thông tin. Trường hợp không thể đảm bảo sự sẵn sàng với kiến trúc hệ thống hiện tại, các thành phần hoặc kiến trúc dự phòng cần được xem xét.

Nếu có thể, các hệ thống thông tin dự phòng nên được kiểm tra để đảm bảo khi có lỗi công việc sẽ chuyển từ thành phần này sang thành phần khác như dự kiến.

Thông tin khác

Việc thực hiện các dự phòng có thể đưa ra các rủi ro liên quan đến tính toàn vẹn hoặc tính bí mật của thông tin và hệ thống thông tin, do vậy cần được xem xét khi thiết kế các hệ thống thông tin.

18 Sự tuân thủ

18.1 Sự tuân thủ 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, các yêu cầu về đảm bảo an toàn thông tin.

18.1.1 Xác định các điều luật áp dụng và yêu cầu hợp đồng

Kiểm soát

Tất cả các yêu cầu về pháp lý, quy định, nghĩa vụ trong hợp đồng đã ký và cách tiếp cận của tổ chức để đáp ứng những yêu cầu này phải được xác định rõ ràng, lập thành tài liệu và được cập nhật thường xuyên đối với mỗi hệ thống thông tin và tổ chức.

Hướng dẫn triển khai

Các biện pháp kiểm soát cụ thể và các trách nhiệm của cá nhân để đáp ứng các yêu cầu này phải được xác định và được lập thành tài liệu.

Các nhà quản lý cần phải xác định tất cả các quy định pháp luật áp dụng đối với tổ chức của họ để đáp ứng các yêu cầu cho loại hình nghiệp vụ của họ. Nếu tổ chức có các hoạt động nghiệp vụ ở các nước khác, các nhà quản lý cần soát xét việc tuân thủ pháp luật của tất cả các nước có liên quan.

18.1.2 Quyền sở hữu trí tuệ

Kiểm soát

Các thủ tục phù hợp cần được triển khai nhằm đảm bảo sự phù hợp với các yêu cầu pháp lý, các quy định và cam kết theo hợp đồng trong việc sử dụng các tài liệu có quyền sở hữu trí tuệ và các sản phẩm phần mềm độc quyền.

Hướng dẫn thi hành

Các hướng dẫn sau cần được quan tâm để bảo vệ mọi tài liệu có quyền sở hữu trí tuệ:

- a) tiết lộ các quyền sở hữu trí tuệ phải tuân thủ theo chính sách trong đó xác định việc sử dụng hợp pháp các sản phẩm thông tin và phần mềm;
- b) chỉ lấy phần mềm qua các nguồn quen biết và đáng tin cậy, nhằm đảm bảo rằng không vi phạm bản quyền;
- c) duy trì nhận thức về các chính sách bảo vệ các quyền sở hữu trí tuệ, và đưa ra lưu ý về mục đích thực hiện hành động kỷ luật đối với các cá nhân vi phạm chính sách;
- d) duy trì đăng ký các tài sản phù hợp, và xác định tất cả các tài sản cùng các yêu cầu bảo vệ các quyền sở hữu trí tuệ;
- e) duy trì chứng minh và bằng chứng về quyền sở hữu các bản quyền, các đĩa thu gốc, sách hướng dẫn...;
- f) triển khai các biện pháp kiểm soát nhằm đảm bảo rằng không bị vượt quá số lượng người dùng tối đa được phép;
- g) thực hiện các cuộc kiểm tra để đảm bảo rằng chỉ các phần mềm được cấp phép và các sản phẩm có bản quyền mới được cài đặt;
- h) cung cấp một chính sách duy trì các điều kiện bản quyền thích hợp;
- i) cung cấp một chính sách bố trí hoặc chuyển phần mềm cho những người khác;
- j) Sử dụng các công cụ kiểm toán phù hợp;
- k) tuân theo các điều khoản và điều kiện đối với phần mềm và thông tin lấy được từ các mạng công cộng;
- l) không nhân bản, chuyển đổi sang dạng khác hoặc lấy từ các hồ sơ thương mại (phim ảnh, tiếng nói) trừ khi đã được phép;

m) không sao chép toàn bộ hoặc từng phần các sách, báo, báo cáo hoặc các dạng tài liệu khác trừ khi được luật bản quyền cho phép.

Thông tin khác

Các quyền sở hữu trí tuệ bao gồm bản quyền phần mềm hoặc tài liệu, các quyền thiết kế, đăng ký thương mại, bằng sáng chế, và các đăng ký mã nguồn.

Các sản phẩm phần mềm có bản quyền thường được cung cấp theo một thỏa thuận đăng ký nhằm xác định các điều khoản và điều kiện đăng ký, ví dụ, giới hạn sử dụng các sản phẩm chỉ với các máy móc cụ thể hoặc giới hạn sao chép chỉ cho các mục đích tạo ra các bản sao lưu. Mức độ quan trọng và nhận thức về các quyền sở hữu trí tuệ đối với phần mềm do tổ chức phát triển cần được truyền thông tới nhân viên.

Các yêu cầu pháp lý, quy định và giao kèo có thể đặt ra những giới hạn trong việc sao chép các tài liệu có bản quyền. Cụ thể là, chúng có thể yêu cầu chỉ có các tài liệu được phát triển bởi tổ chức, hoặc được đăng ký bản quyền hoặc được cung cấp bởi người phát triển cho tổ chức, mới có thể được sử dụng. Sự vi phạm bản quyền có thể dẫn đến các hoạt động pháp lý, đó có thể là các cuộc kiện cáo có tính chất hình sự.

18.1.3 Bảo vệ các hồ sơ

Kiểm soát

Các hồ sơ quan trọng cần được bảo vệ khỏi sự mất mát, phá hủy, làm sai lệch, truy cập và tiết lộ trái phép, phù hợp với pháp luật, quy định, các nghĩa vụ trong hợp đồng đã ký.

Hướng dẫn thi hành

Khi quyết định bảo vệ các hồ sơ cụ thể của tổ chức, việc phân loại tương ứng của hồ sơ dựa trên sơ đồ phân loại của tổ chức cần được xem xét. Hồ sơ phải được phân loại thành các loại hồ sơ, ví dụ hồ sơ kế toán, hồ sơ cơ sở dữ liệu, nhật ký giao dịch, nhật ký kiểm toán và các thủ tục điều hành, mỗi hồ sơ đều có các thông tin chi tiết về các giai đoạn sử dụng và loại phương tiện lưu trữ, ví dụ giấy, phim, tüt, quang,... Tất cả các khóa mật mã có liên quan và các chương trình liên kết với lưu trữ mật mã hoặc chữ ký số ([xem điều 10](#)) cũng cần được lưu trữ để cho phép giải mã các hồ sơ, đảm bảo cho thời gian lưu trữ hồ sơ đủ lâu dài theo yêu cầu.

Cần xem xét khả năng hư hỏng của thiết bị được sử dụng để lưu trữ các hồ sơ. Các thủ tục lưu trữ và xử lý cần được triển khai theo các hướng dẫn của nhà sản xuất.

Trường hợp thiết bị lưu trữ điện tử được lựa chọn thì các thủ tục nhằm đảm bảo khả năng truy cập dữ liệu (cả khả năng đọc phương tiện và định dạng) trong toàn bộ quá trình lưu trữ cũng cần được thiết lập nhằm bảo vệ an toàn trước những mất mát do sự thay đổi công nghệ trong tương lai.

Các hệ thống lưu trữ dữ liệu cần được lựa chọn sao cho dữ liệu được yêu cầu có thể được lấy lại trong định dạng và khung thời gian ở mức chấp nhận được, tùy thuộc vào các yêu cầu phải đáp ứng.

Hệ thống lưu trữ và xử lý cần đảm bảo định danh rõ các hồ sơ và thời gian lưu trữ chúng như đã được xác định bởi các yêu cầu pháp lý, quy định của quốc gia hoặc khu vực. Hệ thống này phải cho phép hủy bỏ các hồ sơ một cách phù hợp sau thời gian lưu trữ đó nếu chúng không cần thiết cho tổ chức nữa.

Để thỏa mãn các mục tiêu bảo vệ hồ sơ, các bước sau đây cần được thực hiện trong nội bộ tổ chức:

- a) đưa ra các hướng dẫn về việc sử dụng, lưu trữ, xử lý và loại bỏ các hồ sơ và thông tin;
- b) kế hoạch lưu trữ cần được phác thảo nhằm xác định các hồ sơ và khoảng thời gian lưu trữ chúng;
- c) một bản kiểm kê các nguồn của các thông tin quan trọng cần được duy trì.

Thông tin khác

Một số hồ sơ có thể cần được lưu giữ an toàn để tuân thủ các yêu cầu pháp lý, quy định hoặc giao kèo, cũng như để hỗ trợ các hoạt động nghiệp vụ cần thiết. Ví dụ các hồ sơ có thể được yêu cầu là bằng chứng cho thấy tổ chức hoạt động tuân theo các quy định hoặc các yêu cầu pháp lý, nhằm đảm bảo chống lại các hành động tiềm ẩn về dân sự hoặc hình sự, hoặc để xác nhận tình trạng tài chính của một tổ chức trước các cổ đông, các bên liên quan và các kiểm toán viên. Khoảng thời gian và nội dung dữ liệu cần lưu trữ thông tin có thể được quy định bởi các điều luật hoặc quy định quốc gia.

Thông tin sâu hơn về việc quản lý các hồ sơ của tổ chức có thể tìm thấy trong ISO 15489-1^[5].

18.1.4 An toàn riêng tư và bảo vệ thông tin cá nhân

Kiểm soát

Việc bảo vệ dữ liệu và tính riêng tư cần được đảm bảo theo yêu cầu pháp lý, quy định khi áp dụng.

Hướng dẫn thi hành

Chính sách về sự riêng tư và bảo vệ dữ liệu của tổ chức cần được phát triển và triển khai. Chính sách này cần được phổ biến cho tất cả các nhân viên tham gia vào việc xử lý thông tin cá nhân.

Việc tuân thủ chính sách này và tất cả các yêu cầu pháp lý và quy định về bảo vệ dữ liệu có liên quan đòi hỏi cơ cấu và biện pháp kiểm soát phù hợp. Thông thường cách tốt nhất để đạt được điều này là chỉ định trách nhiệm cá nhân, ví dụ chỉ định ra một nhân viên bảo vệ dữ liệu, người này phải đưa ra hướng dẫn cho những người quản lý, người dùng, và các nhà cung cấp dịch vụ trên cơ sở các trách nhiệm cá nhân của họ và các thủ tục cần phải tuân theo. Trách nhiệm đối với việc xử lý thông tin cá nhân và đảm bảo nhận thức về các nguyên tắc bảo vệ dữ liệu cần được đề cập phù hợp tuân theo các yêu cầu pháp lý và các quy định. Các biện pháp kỹ thuật và tổ chức phù hợp để bảo vệ thông tin cá nhân cũng cần được triển khai.

Thông tin khác

ISO/IEC 29100^[26] cung cấp một khuôn khổ mức cao cho bảo vệ thông tin cá nhân trong các hệ thống công nghệ thông tin và truyền thông. Một số nước đã đưa ra quy định pháp lý về các biện pháp kiểm soát việc thu thập, xử lý, và chuyển giao dữ liệu cá nhân (nhìn chung, thông tin về những người còn sống có thể được xác định từ các thông tin đó). Tùy thuộc vào các quy định pháp lý riêng của từng quốc gia mà các biện pháp kiểm soát có thể áp đặt các nhiệm vụ lên những cá nhân thu thập, xử lý, và phổ biến thông tin cá nhân, và có thể hạn chế khả năng truyền dữ liệu đó tới nước khác.

18.1.5 Quy định về quản lý mật mã

Kiểm soát

Quản lý mật mã cần được áp dụng phù hợp với các thỏa thuận, luật pháp và các quy định liên quan.

Hướng dẫn thi hành

Những vấn đề sau cần được quan tâm nhằm tuân thủ các thỏa thuận, luật pháp và quy định liên quan:

- a) các hạn chế về việc nhập khẩu và/hoặc xuất khẩu phần mềm và phần cứng máy tính để thực hiện các chức năng mật mã;
- b) các hạn chế về việc nhập khẩu và/hoặc xuất khẩu phần mềm và phần cứng máy tính được thiết kế để bổ sung các chức năng mật mã.
- c) các hạn chế về việc sử dụng mật mã;
- d) các phương pháp bắt buộc hoặc tùy chọn về truy cập bởi các cơ quan quản lý quốc gia tới thông tin được mật mã bởi phần cứng hoặc phần mềm để có được bí mật của nội dung.

Cần có tư vấn pháp lý để đảm bảo sự tuân thủ các luật lệ và quy định của quốc gia. Trước khi thông tin đã mật mã hoặc các biện pháp kiểm soát mật mã được chuyển sang quốc gia khác thì cũng cần có sự tư vấn pháp lý.

18.2 Soát xét về an toàn thông tin

18.2.1 Soát xét độc lập về an toàn thông tin

Kiểm soát

Cách tiếp cận của tổ chức để quản lý an toàn thông tin và việc thực hiện nó (tức là các mục tiêu kiểm soát, các biện pháp kiểm soát, các chính sách, các quy trình và thủ tục an toàn thông tin) cần được soát xét lại một cách độc lập tại các khoảng thời gian được lên kế hoạch hoặc khi có thay đổi đáng kể xảy ra.

Hướng dẫn thi hành

Cấp quản lý cần khởi động việc đánh giá độc lập. Một đánh giá độc lập là cần thiết để đảm bảo sự tương thích liên tục, đầy đủ và hiệu quả của phương pháp tiếp cận của tổ chức để quản lý an toàn thông tin. Việc soát xét phải bao gồm việc đánh giá các cơ hội cải tiến và nhu cầu để thay đổi cách tiếp cận đối với an toàn, bao gồm các chính sách và các mục tiêu kiểm soát.

Các rà soát như vậy cần được thực hiện bởi các cá nhân độc lập với các khu vực được soát xét, ví dụ: các chức năng kiểm toán nội bộ, hoặc một nhà quản lý độc lập hoặc một tổ chức bên ngoài chuyên đánh giá như vậy. Cá nhân tiến hành các đánh giá này cần phải có những kỹ năng và kinh nghiệm thích hợp.

Các kết quả của việc soát xét độc lập cần được ghi lại và báo cáo cho cấp quản lý, là những người khởi xướng việc đánh giá. Những hồ sơ này phải được duy trì.

Nếu kết quả soát xét độc lập xác định rằng phương pháp của tổ chức và thực hiện việc quản lý an toàn thông tin không đầy đủ, ví dụ mục tiêu và yêu cầu tài liệu không được đáp ứng hay không phù hợp với định hướng an toàn thông tin nêu trong chính sách an toàn thông tin ([xem 5.1.1](#)), cấp quản lý cần xem xét các hành động khắc phục.

Thông tin khác

ISO/IEC 27007^[12], "Hướng dẫn đánh giá các hệ thống quản lý an toàn thông tin" và ISO/IEC TR 27008^[13], "Hướng dẫn chuyên gia đánh giá các biện pháp kiểm soát an toàn thông tin" cũng cung cấp hướng dẫn cho việc thực hiện đánh giá (kiểm toán) độc lập.

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

Kiểm soát

Các nhà quản lý cần thường xuyên soát xét sự tuân thủ của việc xử lý thông tin và thủ tục trong khu vực trách nhiệm của mình với các chính sách an toàn thích hợp, các tiêu chuẩn và yêu cầu an toàn khác.

Hướng dẫn triển khai

Các nhà quản lý cần phải xác định làm thế nào để soát xét rằng các yêu cầu an toàn thông tin quy định trong các chính sách, chuẩn và các quy định hiện hành khác được đáp ứng. Đo lường tự động và các công cụ báo cáo cần phải được soát xét thường xuyên, hiệu quả.

Nếu thấy bất kỳ sự không tuân thủ nào qua kết quả đánh giá, các nhà quản lý cần:

- a) xác định nguyên nhân của sự không tuân thủ;
- b) đánh giá sự cần thiết phải có những hành động để đạt được sự tuân thủ;
- c) thực hiện các hành động khắc phục phù hợp;

d) soát xét các hành động khắc phục thực tế để xác minh tính hiệu quả của nó và xác định những thiếu sót hoặc những lỗ hổng.

Kết quả soát xét và hành động khắc phục được thực hiện bởi các nhà quản lý cần được ghi nhận và lưu lại hồ sơ. Các nhà quản lý phải báo cáo kết quả cho những người thực hiện soát xét độc lập (xem [18.2.1](#)) khi soát xét độc lập diễn ra trong khu vực trách nhiệm của họ.

Thông tin khác

Giám sát hoạt động của các hệ thống sử dụng được bao gồm trong [12.4](#).

18.2.3 Soát xét tuân thủ kỹ thuật

Kiểm soát

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

Hướng dẫn triển khai

Tuân thủ kỹ thuật cần được soát xét tốt hơn với sự hỗ trợ của các công cụ tự động, tạo ra các báo cáo kỹ thuật mà sau này sẽ được giải thích bởi một chuyên gia kỹ thuật. Một cách khác, soát xét nhân công (được hỗ trợ bởi các công cụ phần mềm thích hợp, nếu cần thiết) bởi một kỹ sư hệ thống có kinh nghiệm có thể được thực hiện.

Nếu thực hiện các cuộc kiểm tra thâm nhập hoặc các cuộc đánh giá lỗ hổng thì cần thận trọng vì các hoạt động như vậy có thể gây tổn hại đến sự an toàn của hệ thống. Những cuộc kiểm tra này cần được lên kế hoạch, được lập thành tài liệu và có thể lặp lại.

Mọi cuộc kiểm tra tuân thủ kỹ thuật đều chỉ được thực hiện bởi những người nhân viên có trình độ, có thẩm quyền, hoặc dưới sự giám sát của những nhân viên như vậy.

Thông tin khác

Soát xét tuân thủ kỹ thuật liên quan đến kiểm tra các hệ thống điều hành để đảm bảo rằng các biện pháp kiểm soát phần cứng và phần mềm đều được thực hiện đúng. Loại kiểm tra tuân thủ này đòi hỏi phải được thực hiện bởi những chuyên gia kỹ thuật thành thạo.

Soát xét tuân thủ cũng bao gồm, ví dụ, các cuộc kiểm tra xâm nhập và các cuộc đánh giá lỗ hổng, các cuộc kiểm tra này có thể được thực hiện bởi những chuyên gia độc lập đã được ký hợp đồng thực hiện mục đích này. Cách đó có thể rất hữu ích trong việc phát hiện các lỗ hổng của hệ thống và kiểm tra xem các biện pháp kiểm soát có hiệu quả trong việc ngăn chặn truy cập trái phép do những lỗ hổng này không.

Việc kiểm tra sự xâm nhập và đánh giá các lỗ hổng sẽ cung cấp đánh giá chung về hệ thống trong một trạng thái nhất định vào một thời điểm nhất định. Sự đánh giá này được giới hạn cho các phần của hệ thống thực sự đã được kiểm tra trong mọi nỗ lực xâm nhập. Việc kiểm tra xâm nhập và đánh giá lỗ hổng không thể thay thế việc đánh giá rủi ro.

ISO/IEC TR 27008^[13] cung cấp hướng dẫn cụ thể cho soát xét tuân thủ kỹ thuật.

Thư mục tài liệu tham khảo

- [1] ISO/IEC Directives, Part 2
- [2] TCVN 7817-1 (ISO/IEC 11770-1), Công nghệ thông tin - Kỹ thuật mật mã - Quản lý khóa - Phần 1: Khung tổng quát
- [3] TCVN 7817-2 (ISO/IEC 11770-2), Công nghệ thông tin - Kỹ thuật an ninh - Quản lý khóa - Phần 2: Cơ chế sử dụng kỹ thuật đối xứng
- [4] TCVN 7817-3 (ISO/IEC 11770-3), Công nghệ thông tin - Kỹ thuật mật mã - Quản lý khóa - Phần 3: Các cơ chế sử dụng kỹ thuật không đối xứng
- [5] TCVN 7420-1 (ISO 15489-1), Thông tin và tư liệu - Quản lý hồ sơ - Phần 1: Yêu cầu chung
- [6] TCVN 8695-1 (ISO/IEC 20000-1), Công nghệ thông tin - Quản lý dịch vụ - Phần 1: Các yêu cầu
- [7] TCVN 8695-2 (ISO/IEC 20000-2), Công nghệ thông tin - Quản lý dịch vụ - Phần 2: Quy tắc thực hành
- [8] TCVN ISO 22301, An ninh xã hội - Hệ thống quản lý kinh doanh liên tục - Các yêu cầu
- [9] ISO 22313, Societal security - Business continuity management systems - Guidance
- [10] TCVN ISO/IEC 27001 (ISO/IEC 27001), Công nghệ thông tin - Các kỹ thuật an toàn - Hệ thống quản lý an toàn thông tin - Các yêu cầu
- [11] TCVN 10295 (ISO/IEC 27005), Công nghệ thông tin - Các kỹ thuật an toàn - Quản lý rủi ro an toàn thông tin
- [12] TCVN 11779 (ISO/IEC 27007), Công nghệ thông tin - Các kỹ thuật an toàn - Hướng dẫn đánh giá hệ thống quản lý an toàn thông tin
- [13] TCVN 27008 (ISO/IEC TR 27008), Công nghệ thông tin - Các kỹ thuật an toàn - Hướng dẫn chuyên gia đánh giá về kiểm soát an toàn thông tin
- [14] TCVN ISO/IEC 27031 (ISO/IEC 27031), Công nghệ thông tin - Các kỹ thuật an toàn - Hướng dẫn đảm bảo sự sẵn sàng về công nghệ thông tin và truyền thông cho tính liên tục của hoạt động
- [15] TCVN 9801-1 (ISO/IEC 27033-1), Công nghệ thông tin - Kỹ thuật an ninh - An ninh mạng - Phần 1: Tổng quan và khái niệm
- [16] TCVN 9801-2 (ISO/IEC 27033-2), Công nghệ thông tin - Các kỹ thuật an toàn - An toàn mạng - Phần 2: Hướng dẫn thiết kế và triển khai an toàn mạng
- [17] TCVN 9801-3 (ISO/IEC 27033-3), Công nghệ thông tin - Các kỹ thuật an toàn - An toàn mạng - Phần 3: Các kịch bản kết nối mạng tham chiếu - Nguy cơ, kỹ thuật thiết kế và các vấn đề kiểm soát

TCVN ISO/IEC 27002:2020

- [18] ISO/IEC 27033-4, Information technology - Security techniques - Network security - Part 4: Securing communications between networks using security gateways
 - [19] ISO/IEC 27033-5, Information technology - Security techniques - Network security - Part 5: Securing communications across networks using Virtual Private Network (VPNs)
 - [20] TCVN 11239 (ISO/IEC 27035), Công nghệ thông tin - Các kỹ thuật an toàn - Quản lý sự cố an toàn thông tin
 - [21] ISO/IEC 27036-1, Information technology - Security techniques - Information security for supplier relationships - Part 1: Overview and concepts
 - [22] ISO/IEC 27036-2, Information technology - Security techniques - Information security for supplier relationships - Part 2: Common requirements
 - [23] ISO/IEC 27036-3, Information technology - Security techniques - Information security for supplier relationships - Part 3: Guidelines for ICT supply chain security
 - [24] TCVN ISO/IEC 27037 (ISO/IEC 27037) - Công nghệ thông tin - Các kỹ thuật an toàn - Hướng dẫn xác định, tập hợp, thu nhận và bảo quản các bằng chứng số
 - [25] ISO/IEC 29100, Information technology - Security techniques - Privacy framework
 - [26] ISO/IEC 29101, Information technology - Security techniques - Privacy architecture framework
 - [27] TCVN ISO 31000 (ISO 31000), Quản lý rủi ro - Nguyên tắc và hướng dẫn.
-