TIÊU CHUẨN QUỐC GIA

TCVN ISO/IEC 27002:2011

ISO/IEC 27002:2005

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

Lời nói đầu

TCVN ISO/IEC 27002:2011 hoàn toàn tương đương với ISO/IEC 27002:2005.

TCVN ISO/IEC 27002:2011 do Viện Khoa học Kỹ thuật Bưu điện 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 thiết lập các hướng dẫn và nguyên tắc chung cho hoạt động khởi tạo, triển khai, duy trì và cải tiến công tác quản lý an toàn thông tin trong một tổ chức. Mục tiêu của tiêu chuẩn này là đưa ra hướng dẫn chung nhằm đạt được các mục đích chung đã được chấp nhận trong quản lý an toàn thông tin.

Các mục tiêu và biện pháp quản lý của tiêu chuẩn này được xây dựng nhằm đáp ứng các yêu cầu đã được xác định bởi quá trình đánh giá rủi ro. Tiêu chuẩn này có thể đóng vai trò như một hướng dẫn thực hành trong việc xây dựng các tiêu chuẩn an toàn thông tin cho tổ chức và các quy tắc thực hành quản lý an toàn thông tin hiệu quả và giúp tạo dựng sự tin cậy trong các hoạt động liên tổ chức.

2. Thuật ngữ và định nghĩa

2.1. Tài sản (asset)

Bất cứ thứ gì có giá trị đối với tổ chức.

[ISO/IEC 13335-1:2004]

2.2. Biện pháp quản lý (control)

Các biện pháp quản lý rủi ro bao gồm các chính sách, thủ tục, hướng dẫn, thực hành hoặc các cơ cấu tổ chức, trên phương diện hành chính, kỹ thuật, quản lý hoặc bản chất pháp lý.

CHÚ THÍCH: Biện pháp quản lý cũng được sử dụng đồng nghĩa với biện pháp bảo vệ hay biện pháp đối phó.

2.3. Hướng dẫn (guideline)

Một mô tả trong đó chỉ ra điều cần làm và phương thức tiến hành nhằm đạt được các mục tiêu đã chỉ ra trong các chính sách.

[ISO/IEC 13335-1:2004]

2.4. Phương tiện xử lý thông tin (information processing facilities)

Hệ thống, dịch vụ hay cơ sở hạ tầng xử lý thông tin, hoặc các vị trí vật lý để đặt chúng.

2.5. An toàn thông tin (information security)

Sự duy trì tính bí mật, tính toàn vẹn và tính sẵn sàng của thông tin; ngoài ra còn có thể bao hàm một số tính chất khác như tính xác thực, giải trình trách nhiệm, không thể chối bỏ và tin cậy.

2.6. Sự kiện an toàn thông tin (information security event)

Một sự kiện đã được xác định của một hệ thống, dịch vụ hay trạng thái mạng chỉ ra khả năng vi phạm chính sách an toàn thông tin, sự thất bại của hệ thống bảo vệ, hoặc một tình huống chưa rõ gây ảnh hưởng đến an toàn thông tin.

[ISO/IEC TR 18004:2004]

2.7. Sự cố an toàn thông tin (information security incident)

Một hoặc một chuỗi các sự kiện an toàn thông tin không mong muốn có khả năng làm tổn hại các hoạt động nghiệp vụ và đe dọa an toàn thông tin.

[ISO/IEC TR 18044:2004]

2.8. Chính sách (policy)

Mục đích và định hướng tổng thể được công bố một cách chính thức bởi ban quản lý.

2.9. Rủi ro (risk)

Sự kết hợp giữa khả năng xảy ra một sự kiện và hậu quả.

2.10. Phân tích rủi ro (risk analysis)

Sử dụng thông tin một cách có hệ thống nhằm xác định các nguồn gốc và ước đoán rủi ro.

[ISO/IEC Guide 73:2002]

2.11. Đánh giá rủi ro (risk assessment)

Quá trình tổng thể gồm phân tích rủi ro và ước lượng rủi ro.

[ISO/IEC Guide 73:2002],

2.12. Ước lượng rủi ro (risk evaluation)

Quá trình so sánh rủi ro đã ước đoán với một chỉ tiêu rủi ro đã có nhằm xác định độ nghiêm trọng của rủi ro.

[ISO/IEC Guide 73:2002]

2.13. Quản lý rủi ro (risk management)

Các hoạt động phối hợp nhằm điều khiển và quản lý một tổ chức trước các rủi ro có thể xảy ra

CHÚ THÍCH: Quản lý rủi ro thường gồm đánh giá rủi ro, xử lý rủi ro, chấp nhận rủi ro và thông báo rủi ro.

[ISO/IEC Guide 73:2002]

2.14. Xử lý rủi ro (risk treament)

Quá trình lựa chọn và triển khai các biện pháp hạn chế rủi ro.

[ISO/IEC Guide 73:2002]

2.15. Bên thứ ba (thirt party)

Một cá nhân hay một tổ chức được công nhận là độc lập với các bên tham gia, có liên quan đến vấn đề đang phải giải quyết.

2.16. Mối đe dọa (threat)

Nguyên nhân tiềm ẩn gây ra sự cố không mong muốn, kết quả là có thể gây tổn hại cho một hệ thống hoặc tổ chức.

[ISO/IEC 13335-1:2004]

2.17. Điểm yếu (vulnerability)

Nhược điểm của một tài sản hoặc một nhóm tài sản có khả năng bị lợi dụng bởi một hay nhiều mối đe [ISO/IEC 13335-1:2004]

3. Đánh giá và xử lý rủi ro

3.1. Đánh giá rủi ro an toàn thông tin

Đánh giá rủi ro cần xác định, định lượng và phân loại ưu tiên các rủi ro dựa trên tiêu chí về chấp nhận rủi ro và các mục tiêu phù hợp với tổ chức. Các kết quả cần hướng dẫn và xác định hoạt động quản lý phù hợp và phân loại ưu tiên nhằm phục vụ cho việc quản lý các rủi ro an toàn thông tin và triển khai các biện pháp quản lý đã được chọn nhằm chống lại các rủi ro này. Quá trình đánh giá các rủi ro và chọn lựa các biện pháp quản lý có thể cần được thực hiện nhiều lần nhằm bao quát hết các bộ phận khác nhau của tổ chức hoặc các hệ thống thông tin riêng lẻ.

Đánh giá rủi ro cần bao hàm cách tiếp cận có hệ thống trong việc ước lượng độ lớn của các rủi ro (phân tích rủi ro) và quá trình so sánh các rủi ro đã được ước đoán với tiêu chí rủi ro nhằm xác định độ nghiêm trọng của các rủi ro (ước lượng rủi ro).

Đánh giá rủi ro cần được thực hiện định kỳ nhằm phát hiện những thay đổi về các yêu cầu an toàn và tình huống rủi ro, ví dụ trong các tài sản, các mối đe dọa, các điểm yếu, các tác động, trong ước lượng rủi ro, và khi xảy ra những thay đổi lớn. Những đánh giá rủi ro này cần được thực hiện một cách có phương pháp nhằm đưa ra các kết quả có khả năng so sánh và tái sử dụng.

Để có hiệu quả thì đánh giá rủi ro an toàn thông tin cần có một phạm vi xác định rõ ràng, và nếu thích hợp thì cần bao hàm cả các mối quan hệ với việc đánh giá rủi ro cho các lĩnh vực khác.

Phạm vi của đánh giá rủi ro có thể là trong toàn bộ tổ chức, các bộ phận của tổ chức, một hệ thống thông tin cụ thể nào đó, các thành phần hệ thống nhất định, hoặc các dịch vụ mà ở đó có thể thực hiện đánh giá rủi ro một cách khả thi, thực tế, và hữu dụng. Các ví dụ về các hệ phương pháp đánh giá rủi ro được đề cập trong ISO/IEC TR 13335-3 (Các hướng dẫn quản lý an toàn công nghệ thông tin: Các kỹ thuật quản lý an toàn công nghệ thông tin).

3.2. Xử lý các rủi ro an toàn thông tin

Trước khi xem xét xử lý rủi ro, tổ chức cần quyết định tiêu chí để xác định liệu các rủi ro có được chấp nhận hay không. Ví dụ, các rủi ro có thể được chấp nhận nếu nó được đánh giá là rủi ro ở mức thấp, hay chi phí cho xử lý rủi ro không quá nặng nề đối với tổ chức. Các quyết định như vậy cần được ghi lại.

Cần đưa ra quyết định xử lý rủi ro đối với các rủi ro đã được xác định sau đánh giá rủi ro. Dưới đây là những lựa chọn nhằm xử lý rủi ro:

a) áp dụng các biện pháp quản lý thích hợp nhằm giảm bớt rủi ro;

b) chấp nhận các rủi ro một cách khách quan và có dụng ý, miễn là chúng thỏa mãn chính sách và tiêu chí chấp nhận rủi ro của tổ chức;

c) tránh rủi ro bằng cách không cho phép các hoạt động sẽ làm phát sinh rủi ro;

d) chuyển các rủi ro liên đới tới các bên khác, ví dụ các nhà bảo hiểm hoặc các nhà cung cấp.

Đối với các rủi ro mà việc quyết định xử lý rủi ro đã xác định phải áp dụng các biện pháp quản lý thích hợp thì những biện pháp quản lý này cần được lựa chọn và thực hiện để đáp ứng các yêu cầu được xác định bởi quá trình đánh giá rủi ro. Các biện pháp quản lý cần đảm bảo rằng các rủi ro được giảm tới một mức chấp nhận, và cần quan tâm tới các vấn đề sau:

a) các yêu cầu và các ràng buộc của pháp luật và các quy định trong nước và quốc tế;

b) các mục tiêu của tổ chức;

c) các yêu cầu và các ràng buộc về vận hành;

d) chi phí triển khai và vận hành liên quan tới các rủi ro sẽ được giảm thiểu, và duy trì tương quan đối với các yêu cầu và các ràng buộc của tổ chức;

e) nhu cầu cân bằng đầu tư trong quá trình triển khai và vận hành các biện pháp quản lý để chống lại thiệt hại có thể xảy ra do các lỗi về an toàn.

Các biện pháp quản lý có thể được chọn từ tiêu chuẩn này hoặc từ bộ các biện pháp quản lý khác, hoặc các biện pháp quản lý mới có thể được thiết kế phù hợp với các yêu cầu nhất định của tổ chức. Cũng cần phải thừa nhận rằng một số biện pháp quản lý có thể không phù hợp đối với mọi môi trường và mọi hệ thống thông tin, và có thể không khả thi đối với tất cả các tổ chức. Một ví dụ là, 9.1.3 mô tả cách phân tách nhiệm vụ nhằm ngăn chặn gian lận và sai sót. Các tổ chức có qui mô nhỏ hơn khó có thể phân tách tất cả các nhiệm vụ và như vậy có thể tìm các cách khác để đạt được mục tiêu quản lý tương tự. Một ví dụ khác là, 9.10 mô tả cách giám sát hệ thống và thu thập chứng cứ. Các biện pháp quản lý được mô tả, ví dụ ghi nhật ký sự kiện, có thể lại mâu thuẫn với các điều luật hiện hành, ví dụ luật bảo vệ sự riêng tư của các khách hàng hoặc tại nơi làm việc.

Các biện pháp quản lý an toàn thông tin cần được quan tâm ở giai đoạn thiết kế và xác định các yêu cầu đối với các dự án và các hệ thống. Lỗi ở giai đoạn này có thể làm phát sinh chi phí và giảm hiệu quả của các giải pháp, và trong trường hợp xấu nhất còn không thể đạt được sự an toàn thông tin một cách thỏa đáng.

Cần lưu ý rằng không tồn tại bộ các biện pháp quản lý giúp đạt được an toàn tuyệt đối, và cần thực hiện hoạt động quản lý bổ trợ nhằm giám sát, ước lượng, và nâng cao khả năng và tính hiệu quả của các biện pháp quản lý an toàn nhằm hướng đến các mục tiêu của tổ chức.

4. Chính sách an toàn thông tin

4.1. Chính sách an toàn thông tin

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

Ban quản lý cần thiết lập định hướng chính sách rõ ràng phù hợp với các mục tiêu nghiệp vụ, hỗ trợ và cam kết về an toàn thông tin thông qua việc ban hành và duy trì một chính sách an toàn thông tin trong toàn bộ tổ chức.

4.1.1. Tài liệu chính sách an toàn thông tin

Biện pháp quản lý

Một tài liệu về chính sách an toàn thông tin cần phải được phê duyệt bởi ban quản lý và được cung cấp, thông báo tới mọi nhân viên cũng như các bên liên quan.

Hướng dẫn triển khai

Tài liệu chính sách an toàn thông tin cần công bố rõ cam kết của ban quản lý và đưa ra phương thức quản lý an toàn thông tin của tổ chức. Văn bản này cần bao gồm các nội dung sau:

a) định nghĩa về an toàn thông tin, các mục tiêu chung, phạm vi và tầm quan trọng của an toàn thông tin như là một cơ chế cho phép chia sẻ thông tin;

b) công bố về mục đích quản lý, hỗ trợ các mục tiêu và nguyên tắc an toàn thông tin phù hợp với chiến lược và các mục tiêu nghiệp vụ;

c) khuôn khổ cho việc thiết lập các mục tiêu quản lý và các biện pháp quản lý, bao gồm cơ cấu đánh giá và quản lý rủi ro;

d) giải thích ngắn gọn các chính sách, nguyên tắc, tiêu chuẩn an toàn, và các yêu cầu tuân thủ có tầm quan trọng đặc biệt đối với tổ chức, bao gồm:

1) tuân thủ các yêu cầu của luật pháp, quy định, và hợp đồng;

2) các yêu cầu về giáo dục, đào tạo và nhận thức về an toàn;

3) quản lý tính liên tục của hoạt động nghiệp vụ;

4) các hậu quả của các vi phạm chính sách an toàn thông tin;

e) định nghĩa các trách nhiệm chung và riêng về quản lý an toàn thông tin, bao gồm cả việc báo cáo các sự cố an toàn thông tin;

f) tham chiếu tới văn bản hỗ trợ chính sách, ví dụ các chính sách và thủ tục an toàn chi tiết hơn cho các hệ thống thông tin cụ thể hoặc các quy tắc an toàn mà người dùng bắt buộc phải tuân theo.

Chính sách an toàn thông tin này cần được tổ chức phổ biến đến người dùng theo một hình thức phù hợp, dễ truy cập và dễ hiểu.

Thông tin khác

Chính sách an toàn thông tin có thể là một phần của một văn bản chính sách chung nào đó. 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. Thông tin chi tiết hơn có thể tham khảo trong ISO/IEC 13335-1:2004.

4.1.2. Soát xét lại chính sách an toàn thông tin

Biện pháp quản lý

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 triển khai

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 soát xét của ban quản lý. Cũng cần có các thủ tục soát xét nhất định của ban quản lý, bao gồm cả lịch trình hoặc chu kỳ soát xét.

Thông tin đầu vào của quá trình soát xét của ban quản lý cần bao gồm thông tin về:

a) phản hồi từ các bên quan tâm;

b) các kết quả soát xét một cách độc lập (xem 5.1.8);

c) trạng thái của các hoạt động phòng ngừa và sửa chữa (xem 5.1.8 và 14.2.1);

d) kết quả của các lần soát xét trước đó của ban quản lý;

e) sự tuân thủ chính sách an toàn thông tin và hiệu suất quy trình;

f) những thay đổi có thể ảnh hưởng đến phương thức quản lý an toàn thông tin của tổ chức, bao gồm những thay đổi về môi trường tổ chức, các tình huống nghiệp vụ, sự sẵn sàng của nguồn tài nguyên, các điều kiện về pháp lý, quy định và hợp đồng, hoặc môi trường kỹ thuật;

g) các xu hướng liên quan đến các mối đe dọa và các điểm yếu;

h) các sự cố an toàn thông tin đã được báo cáo (xem 12.1);

i) các khuyến nghị của các cơ quan liên quan (xem 5.1.6).

Đầu ra của quá trình soát xét của ban quản lý phải là các quyết định và hành động bất kỳ có liên quan đến:

a) việc cải tiến phương thức của tổ chức trong việc quản lý an toàn thông tin và các quy trình quản lý an toàn thông tin;

b) việc nâng cao các mục tiêu quản lý và các biện pháp quản lý;

c) việc cải tiến trong việc phân bổ các nguồn tài nguyên và/hoặc các trách nhiệm.

Cần duy trì hồ sơ về việc soát xét của ban quản lý

Chính sách an toàn thông tin đã được chỉnh sửa cần có sự chấp thuận của ban quản lý.

5. Tổ chức đảm bảo an toàn thông tin

5.1. Tổ chức nội bộ

Mục tiêu: Nhằm quản lý an toàn thông tin bên trong tổ chức

Cần thiết lập một khuôn khổ quản lý nhằm khởi tạo và quản lý việc triển khai an toàn thông tin trong nội bộ tổ chức.

Ban quản lý cần thông qua chính sách an toàn thông tin, phân định các vai trò an toàn, phối hợp và soát xét việc triển khai thực hiện an toàn thông tin trong toàn bộ tổ chức.

Nếu cần thiết thì cần thiết lập và sẵn sàng có nguồn hỗ trợ chuyên môn về an toàn thông tin từ trong nội bộ của tổ chức. Cũng cần thiết lập những mối liên hệ với các nhóm hoặc các chuyên gia về an toàn thông tin ở bên ngoài nhằm có thể theo kịp các xu hướng công nghiệp, giám sát các tiêu chuẩn và các phương pháp đánh giá và đưa ra các điểm vận dụng phù hợp trong quá trình xử lý các sự cố về an toàn thông tin.

Cũng cần khuyến khích cách tiếp cận an toàn thông tin đa chiều.

5.1.1. Cam kết của ban quản lý về đảm bảo an toàn thông tin

Biện pháp quản lý

Ban quản lý phải chủ động hỗ trợ đảm bảo an toàn thông tin trong tổ chức bằng các định hướng rõ ràng, các cam kết có thể thấy được, các nhiệm vụ rõ ràng, và nhận thức rõ trách nhiệm về đảm bảo an toàn thông tin.

Hướng dẫn triển khai

Ban quản lý cần:

a) đảm bảo rằng các mục tiêu an toàn thông tin đã được xác định rõ, đáp ứng được các yêu cầu của tổ chức, và được đưa vào các quy trình liên quan;

b) trình bày một cách có hệ thống, soát xét và phê chuẩn chính sách an toàn thông tin;

c) soát xét tính hiệu quả của việc triển khai chính sách an toàn thông tin;

d) đưa ra định hướng rõ ràng và sự hỗ trợ rõ ràng của ban quản lý đối với các hoạt động an toàn thông tin;

e) cung cấp các nguồn tài nguyên cần thiết cho an toàn thông tin;

f) phê chuẩn sự phân định các vai trò và trách nhiệm cụ thể về an toàn thông tin trong toàn bộ tổ chức;

g) khởi động các chương trình và kế hoạch nhằm duy trì nhận thức về an toàn thông tin;

h) đảm bảo rằng việc triển khai các biện pháp quản lý an toàn thông tin được phối hợp trong toàn thể nội bộ tổ chức (xem 5.1.2).

Ban quản lý cần xác định rõ các nhu cầu cần có hỗ trợ chuyên môn về an toàn thông tin trong nội bộ hoặc bên ngoài tổ chức, soát xét và phối hợp các kết quả từ những hỗ trợ như vậy trong toàn bộ tổ chức.

Tùy thuộc vào quy mô của tổ chức, các trách nhiệm như vậy cũng có thể được xử lý bởi một diễn đàn quản lý riêng hoặc bởi một ban quản lý đương nhiệm, ví dụ ban giám đốc.

Thông tin khác

Thông tin chi tiết hơn tham khảo trong ISO/IEC 13335-1:2004.

5.1.2. Phối hợp đảm bảo an toàn thông tin

Biện pháp quản lý

Các hoạt động đảm bảo an toàn thông tin cần được phối hợp bởi các đại diện của các bộ phận trong tổ chức với vai trò và nhiệm vụ cụ thể.

Hướng dẫn triển khai

Về cơ bản thì các hoạt động an toàn thông tin cần có sự phối hợp và cộng tác của những người quản lý, người dùng, người quản trị mạng, những nhà thiết kế ứng dụng, những đánh giá viên và nhân viên an toàn, và các kỹ năng chuyên môn trong các lĩnh vực như bảo hiểm, pháp lý, nguồn nhân lực, quản lý rủi ro hoặc IT. Hoạt động này cần:

a) đảm bảo rằng các hoạt động an toàn được thực hiện tuân thủ theo chính sách an toàn thông tin;

b) xác định rõ phương thức xử lý những điểm không tuân thủ;

c) phê chuẩn các hệ phương pháp và các quy trình an toàn thông tin. ví dụ đánh giá rủi ro, phân loại thông tin;

d) xác định những thay đổi lớn về các mối đe dọa và chỉ ra các thông tin và các phương tiện xử lý thông tin bị đe dọa;

e) đánh giá tính phù hợp và phối hợp triển khai các biện pháp quản lý an toàn thông tin;

f) thúc đẩy việc giáo dục, đào tạo và nâng cao nhận thức về an toàn thông tin trên toàn tổ chức một cách hiệu quả;

g) đánh giá thông tin nhận được từ việc giám sát và soát xét các sự cố an toàn thông tin, và khuyến nghị các hoạt động phù hợp đối với các sự cố an toàn thông tin đã được xác định.

Nếu tổ chức không sử dụng riêng một nhóm chức năng chéo, ví dụ do nhóm kiểu này không phù hợp với quy mô của tổ chức, thì các hoạt động được mô tả ở trên cần được đảm trách bởi một ban quản lý thích hợp khác hoặc một người quản lý riêng.

5.1.3. Phân định trách nhiệm đảm bảo an toàn thông tin

Biện pháp quản lý

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

Hướng dẫn triển khai

Việc phân bổ các trách nhiệm về an toàn thông tin cần phù hợp với chính sách an toàn thông tin (xem điều 3). 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 công bố rõ ràng; cụ thể là:

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) trách nhiệm đối với từng tài sản hoặc quy trình an toàn cần được phân định cụ thể và trách nhiệm chi tiết cần được ghi thành văn bản (xem 6.1.2);

c) các mức cấp phép cần được xác định rõ và ghi thành văn bản.

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 quản lý phù hợp.

Tuy nhiên, trách nhiệm trong việc tìm ra và triển khai các biện pháp quản lý 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.

5.1.4. Quy trình cấp phép cho phương tiện xử lý thông tin

Biện pháp quản lý

Một quy trình cấp phép cho phương tiện xử lý thông tin phải được xác định rõ và triển khai.

Hướng dẫn triển khai

Sau đây là các hướng dẫn đối với quy trình cấp phép:

a) những phương tiện mới cần có sự cấp phép sử dụng và mục đích sử dụng từ ban quản lý. Việc cấp phép cũng cần phải được người quản lý có trách nhiệm trong việc duy trì môi trường an toàn của hệ thống thông tin thông qua nhằm đảm bảo rằng tất cả các các chính sách và yêu cầu về an toàn đều được thỏa mãn;

b) khi cần thiết thì cần kiểm tra cả phần cứng và phần mềm nhằm đảm bảo rằng chúng đều tương thích với các thành phần hệ thống khác;

c) việc sử dụng các phương tiện xử lý thông tin thuộc sở hữu cá nhân, ví dụ máy tính xách tay, máy tính tại nhà riêng, hoặc các thiết bị cầm tay, nhằm xử lý thông tin nghiệp vụ có thể làm phát sinh những yếu điểm mới và vì vậy, cần xác định và triển khai các biện pháp quản lý cần thiết.

5.1.5. Các thỏa thuận về bảo mật

Biện pháp quản lý

Các yêu cầu về bảo mật 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 lại.

Hướng dẫn triển khai

Các thỏa thuận bảo mật 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. Khi xác định các yêu cầu đối với các thỏa thuận bảo mật 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 dự kiến của thỏa thuận, bao gồm cả các trường hợp yêu cầu bảo mật không thời hạn;

c) các hoạt động được yêu cầu khi kết thúc thỏa thuận;

d) các trách nhiệm và hành động của các bên 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) việc được phép sử dụng thông tin mật và các quyền của người ký kết sử dụng thông tin;

g) quyền đánh giá 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 hành động dự kiến 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 không tiết lộ hoặc thỏa thuận bảo mật.

Các thỏa thuận bảo mật và không tiết lộ cần tuân thủ tất cả những quy định và điều luật phù hợp (xem thêm 14.1.1);

Các yêu cầu đối với các thỏa thuận bảo mật 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 bảo mật hoặc không tiết lộ sẽ bảo vệ các thông tin của tổ chức và thông báo cho các bên ký kết về trách nhiệm của họ trong việc bảo vệ, sử dụng và tiết lộ thông tin một cách có trách nhiệm và đúng thẩm quyền.

Mỗi tổ chức cũng cần sử dụng các hình thức thỏa thuận bảo mật hoặc không tiết lộ khác nhau theo từng tình huống cụ thể.

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

Biện pháp quản lý

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

Hướng dẫn triển khai

Các tổ chức cần có các thủ tục xác định khi nào và ai sẽ liên hệ với các cơ quan có thẩm quyền (ví dụ, cơ quan thi hành luật, cảnh sát phòng cháy chữa cháy, các cơ quan giám sát), và cách thức báo cáo các sự cố an toàn thông tin đã xác định một cách kịp thời nếu có nghi ngờ đã có sự vi phạm luật.

Các tổ chức bị tấn công từ Internet có thể cần các bên thứ ba (ví dụ, một nhà cung cấp dịch vụ Internet hoặc một nhà khai thác viễn thông) tiến hành các hoạt động chống lại nguồn gốc tấn công.

Thông tin khác

Việc duy trì những liên lạc như vậy có thể là một yêu cầu giúp hỗ trợ quản lý các sự cố an, toàn thông tin (xem 12.2) hoặc quá trình lập kế hoạch nghiệp vụ đột xuất và liên tục (xem 13). Các mối liên hệ với các cơ quan luật pháp 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 mà các tổ chức bắt buộc phải tuân theo. Những liên hệ với những cơ quan có thẩm quyền khác bao gồm cả các dịch vụ khẩn cấp, tiện ích, sức khỏe và an toàn, ví dụ các sở cứu hỏa (có liên quan đến sự liên tục về nghiệp vụ), các nhà cung cấp dịch vụ viễn thông (có liên quan đến độ sẵn sàng), các nhà cung cấp nước (có liên quan đến các phương tiện làm mát cho thiết bị).

5.1.7. Liên lạc với các nhóm chuyên gia

Biện pháp quản lý

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

Hướng dẫn triển khai

Cần coi các thành viên trong các diễn đàn hoặc các nhóm chuyên gia như phương tiện nhằm:

a) nâng cao kiến thức về cách thức thực hành 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 và liên quan đến những tấn công và những yếu điểm;

d) tiếp cận đến những lời khuyên của chuyên gia an toàn thông tin;

e) chia sẻ và trao đổi thông tin về các công nghệ, sản phẩm, những mối đe dọa hoặc những yếu điểm mới;

f) cung cấp những đầu mối liên hệ phù hợp khi giải quyết các sự cố về an toàn thông tin (xem thêm 12.2.1).

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 nhạy cảm.

5.1.8. Soát xét độc lập về an toàn thông tin

Biện pháp quản lý

Cách tiếp cận quản lý an toàn thông tin của tổ chức và việc triển khai của tổ chức (chẳng hạn như: các mục tiêu và biện pháp quản lý, các chính sách, các quá trình và thủ tục đảm bảo an toàn thông tin) phải được soát xét định kỳ hoặc khi xuất hiện những thay đổi quan trọng liên quan đến an toàn thông tin.

Hướng dẫn triển khai

Việc soát xét một cách độc lập cần được thực hiện bởi ban quản lý. Việc soát xét như vậy là cần thiết nhằm đảm bảo tính phù hợp, tính vẹn toàn và tính hiệu quả liên tục của phương thức triển khai an toàn thông tin của tổ chức. Việc soát xét cần bao gồm cả việc đánh giá các cơ hội trong việc cải tiến và nhu cầu cần có những thay đổi về phương thức an toàn, bao gồm cả chính sách và các mục tiêu quản lý.

Việc soát xét như vậy cũng cần được thực hiện bởi các cá nhân độc lập trong khu vực soát xét, ví dụ những người có chức năng đánh giá nội bộ, người quản lý độc lập hoặc một tổ chức bên thứ ba chuyên thực hiện những cuộc soát xét như vậy. Các cá nhân thực hiện các cuộc soát xét cần có các kỹ năng và kinh nghiệm phù hợp.

Các kết quả của những lần soát xét độc lập cần được ghi lại và báo cáo đến ban quản lý. Các bản báo cáo này cần được lưu lại.

Nếu một cuộc soát xét độc lập cho thấy rằng phương thức và việc triển khai của tổ chức trong quản lý an toàn thông tin là không phù hợp hoặc không tuân thủ chỉ dẫn về an toàn thông tin đã được công bố trong văn bản chính sách an toàn thông tin (xem 4.1.1) thì ban quản lý cần cân nhắc đến việc sửa đổi.

Thông tin khác

Các khu vực mà những người quản lý cần soát xét định kỳ cũng có thể cần được soát xét độc lập (xem 14.2.1). Các kỹ thuật soát xét có thể bao gồm các cuộc phỏng vấn của ban quản lý, kiểm tra sổ sách ghi chép hoặc soát xét các văn bản về chính sách an toàn. ISO 19011:2002, Hướng dẫn đánh giá các hệ thống quản lý môi trường và/hoặc chất lượng, cũng có thể là một hướng dẫn rất hữu ích cho việc thực hiện soát xét độc lập, trong đó bao gồm việc thiết lập và triển khai một chương trình soát xét. 14.3 sẽ tập trung vào các biện pháp quản lý liên quan đến soát xét độc lập các hệ thống thông tin điều hành và việc sử dụng các công cụ đánh giá hệ thống.

5.2. Các bên tham gia bên ngoài

Mục tiêu: Nhằm duy trì an toàn đối với thông tin và các phương tiện xử lý thông tin của tổ chức được truy cập, xử lý, truyền tới, hoặc quản lý bởi các bên tham gia bên ngoài tổ chức.

Tính an toàn của thông tin và các phương tiện xử lý thông tin của tổ chức không được bị làm thuyên giảm bởi sự xuất hiện của các sản phẩm hoặc dịch vụ của tổ chức bên ngoài.

Cần quản lý tất cả các truy cập tới các phương tiện xử lý thông tin của tổ chức, việc xử lý và truyền thông được thực hiện bởi các tổ chức bên ngoài.

Khi có nhu cầu nghiệp vụ cần làm việc với các tổ chức bên ngoài mà công việc ấy có thể đòi hỏi phải truy cập đến thông tin và các phương tiện xử lý thông tin của tổ chức, hoặc có nhu cầu cần nhận được hoặc cung cấp một sản phẩm và dịch vụ từ hoặc tới một tổ chức bên

ngoài thì cần thực hiện đánh giá rủi ro nhằm xác định các ảnh hưởng liên quan đến an toàn thông tin và các yêu cầu về biện pháp quản lý. Các biện pháp quản lý cũng cần được thỏa thuận và xác định trong một bản thỏa thuận với tổ chức bên ngoài.

5.2.1. Xác định các rủi ro liên quan đến các bên tham gia bên ngoài

Biện pháp quản lý

Các rủi ro đối với thông tin và các phương tiện xử lý thông tin của tổ chức từ các quy trình nghiệp vụ liên quan đến các bên tham gia bên ngoài phải được nhận biết và triển khai biện pháp quản lý thích hợp trước khi cấp quyền truy cập.

Hướng dẫn triển khai

Khi có nhu cầu cho phép tổ chức bên ngoài truy cập đến các phương tiện xử lý thông tin hoặc thông tin của tổ chức thì cần thực hiện đánh giá rủi ro (xem điều 3) nhằm xác định các yêu cầu đối với các biện pháp quản lý cụ thể. Việc xác định các rủi ro liên quan đến truy cập của tổ chức bên ngoài cần xem xét các yếu tố sau:

a) các phương tiện xử lý thông tin mà tổ chức bên ngoài được yêu cầu truy cập;

b) hình thức truy cập mà tổ chức bên ngoài sẽ thực hiện đối với thông tin và các phương tiện xử lý thông tin, ví dụ:

1) truy cập mức vật lý, ví dụ tới các văn phòng, các phòng máy tính, các ngăn tài liệu;

2) truy cập logic, ví dụ đến cơ sở dữ liệu, hệ thống thông tin của tổ chức;

3) kết nối mạng giữa mạng của tổ chức và của tổ chức bên ngoài, ví dụ kết nối cố định, truy cập từ xa;

4) truy cập được thực hiện tại chỗ hay từ xa;

c) giá trị và độ nhạy cảm của thông tin liên quan, và sự quan trọng của nó đối với các hoạt động nghiệp vụ;

d) các biện pháp quản lý cần thiết nhằm bảo vệ những thông tin mà các tổ chức bên ngoài không được quyền truy cập;

e) nhân viên thuộc tổ chức bên ngoài tham gia vào việc xử lý thông tin của tổ chức;

f) có thể cần xác định cách thức truy cập mà tổ chức hoặc cá nhân được cấp phép, cần kiểm tra giấy phép, và xác định khoảng thời gian cần xác minh lại việc cấp phép;

g) các phương tiện và các biện pháp kiểm soát khác nhau được tổ chức bên ngoài sử dụng khi lưu trữ, xử lý, truyền thông, chia sẻ và trao đổi thông tin;

h) ảnh hưởng của việc truy cập chưa sẵn sàng đối với tổ chức bên ngoài khi có yêu cầu, và việc nhập vào hoặc nhận thông tin không chính xác hoặc sai lệch của tổ chức bên ngoài;

i) các thủ tục và biện pháp xử lý sự cố an toàn thông tin và các thiệt hại tiềm ẩn, các điều kiện và điều khoản truy cập của tổ chức bên ngoài trong trường hợp có xảy ra sự cố an toàn thông tin;

j) Các yêu cầu pháp lý và quy tắc và các nghĩa vụ thỏa thuận liên quan đến tổ chức bên ngoài;

Không được cho phép các tổ chức bên ngoài truy cập tới thông tin của tổ chức trừ khi đã triển khai các biện pháp quản lý phù hợp, và nếu khả thi thì cần ký một bản hợp đồng xác định thời hạn và các điều kiện kết nối hoặc truy cập. Nhìn chung, tất cả các yêu cầu về an toàn khi làm việc với các tổ chức bên ngoài hoặc các biện pháp quản lý bên trong cần được đề cập trong một bản thỏa thuận với tổ chức bên ngoài (xem thêm trong 5.2.2 và 5.2.3).

Cũng cần đảm bảo rằng tổ chức bên ngoài nhận thức được các nghĩa vụ của họ, và chấp thuận các trách nhiệm và nghĩa vụ pháp lý khi truy cập, xử lý, truyền thông, hoặc quản lý thông tin và các phương tiện xử lý thông tin của tổ chức.

Thông tin khác

Thông tin có thể bị rủi ro do các tổ chức thứ ba quản lý an toàn thông tin không phù hợp. Các biện pháp quản lý cần được xác định và sử dụng nhằm quản lý việc truy cập của tổ chức bên ngoài tới các phương tiện xử lý thông tin. Ví dụ, nếu có yêu cầu đặc biệt về tính bí mật của thông tin thì có thể sử dụng các thỏa thuận không tiết lộ thông tin.

Các tổ chức có thể phải đối mặt với những rủi ro liên quan đến việc xử lý, quản lý và truyền thông liên tổ chức nếu áp dụng thuê khoán ngoài ở mức độ cao, hoặc có sự tham gia của nhiều tổ chức.

Các biện pháp quản lý trong 5.2.2 và 5.2.3 bao hàm các biện pháp khi làm việc với nhiều loại tổ chức thứ ba, ví dụ bao gồm:

a) các nhà cung cấp dịch vụ, như ISP, các nhà cung cấp mạng, các dịch vụ điện thoại, các dịch vụ hỗ trợ và bảo trì;

b) các dịch vụ an toàn được quản lý;

c) các khách hàng;

d) thuê khoán các thiết bị và/hoặc các dịch vụ điều hành, ví dụ các hệ thống IT, các dịch vụ thu thập dữ liệu, các trung tâm khai thác cuộc gọi;

e) các nhà tư vấn về quản lý và nghiệp vụ và các đánh giá viên;

f) các nhà cung cấp và phát triển, ví dụ các hệ thống IT và các sản phẩm phần mềm;

g) các dịch vụ vệ sinh, rác thải và các dịch vụ hỗ trợ được thuê khoán khác;

h) lao động tạm thời, sử dụng sinh viên, và các vị trí ngắn hạn khác;

Những thỏa thuận này có thể giúp làm giảm các rủi ro liên quan tới các tổ chức bên ngoài.

5.2.2. Giải quyết an toàn khi làm việc với khách hàng

Biện pháp quản lý

Tất cả các yêu cầu về an toàn phải được giải quyết trước khi cho phép khách hàng truy cập tới thông tin hoặc tài sản của tổ chức.

Hướng dẫn triển khai

Cần quan tâm đến các vấn đề sau nhằm giải quyết an toàn thông tin trước khi cho phép khách hàng truy cập đến bất kỳ tài sản nào của tổ chức (tùy thuộc vào loại và quy mô của truy cập, không phải áp dụng toàn bộ):

a) bảo vệ tài sản, bao gồm:

1) các quy trình bảo vệ các tài sản của tổ chức, bao gồm thông tin và phần mềm, và quản lý các yếu điểm đã biết trước;

2) các thủ tục xác định tổn hại đến tài sản, ví dụ dữ liệu có bị mất hoặc bị làm thay đổi không;

3) tính toàn vẹn;

4) hạn chế việc sao chép và tiết lộ thông tin;

b) mô tả sản phẩm hoặc dịch vụ được cung cấp;

c) các lý do, yêu cầu khác nhau, và các lợi ích trong việc truy cập của khách hàng;

d) chính sách quản lý truy cập, bao gồm:

1) các phương pháp truy cập được cho phép, biện pháp quản lý và sử dụng các thông tin cá nhân như ID và mật khẩu của người dùng;

2) một quy trình cấp phép truy cập và đặc quyền cho người dùng;

3) một thông báo rằng tất cả các truy cập chưa được cấp phép hợp lệ đều bị cấm;

4) một quy trình thu hồi quyền truy cập hoặc ngắt kết nối giữa các hệ thống;

e) các bước thực hiện báo cáo, thông báo, và điều tra về những sai lệch của thông tin (ví dụ các thông tin chi tiết về cá nhân), các sự cố an toàn thông tin và các lỗ hổng bảo mật;

f) mô tả về từng dịch vụ sẽ được cung cấp;

g) mức kỳ vọng của dịch vụ và các mức không chấp nhận được của dịch vụ;

h) quyền giám sát, thu hồi, và thực hiện hoạt động bất kỳ liên quan đến các tài sản của tổ chức;

i) các nghĩa vụ tương ứng của tổ chức và khách hàng;

j) các trách nhiệm liên quan đến các vấn đề luật pháp và phương thức nhằm đảm bảo rằng các yêu cầu về luật pháp đều được đáp ứng, ví dụ cưỡng chế bảo vệ dữ liệu, đặc biệt là phải tính đến các hệ thống luật pháp quốc gia khác nếu thỏa thuận có sự phối hợp với các khách hàng ở các quốc gia khác (xem thêm trong 14.1);

k) các quyền sở hữu trí tuệ (IPR) và vấn đề bản quyền (xem 14.1.2) và việc bảo vệ các kết quả công việc có sự cộng tác (xem thêm 5.1.5).

Thông tin khác

Các yêu cầu về an toàn thông tin liên quan đến các khách hàng truy cập vào tài sản của tổ chức có thể rất khác nhau tùy theo các phương tiện xử lý thông tin và thông tin đang bị truy cập. Các yêu cầu về an toàn này có thể được đề cập trong các thỏa thuận với khách hàng, các thỏa thuận này bao gồm tất cả các rủi ro và các yêu cầu an toàn đã xác định (xem 5.2.1).

Các thỏa thuận với các tổ chức bên ngoài cũng có thể bao gồm các bên khác. Các thỏa thuận chấp nhận việc truy cập của tổ chức bên ngoài cần bao gồm cả việc cho phép chỉ định các tổ chức có đủ tư cách khác, các điều kiện truy cập và sự tham gia của họ

5.2.3. Giải quyết an toàn trong các thỏa thuận với bên thứ ba

Biện pháp quản lý

Các thỏa thuận với bên thứ ba liên quan đến truy cập, xử lý, truyền thông, quản lý thông tin và các phương tiện xử lý thông tin của tổ chức, hoặc các sản phẩm, dịch vụ phụ trợ của các phương tiện xử lý thông tin phải bao hàm tất cả các yêu cầu an toàn có liên quan.

Hướng dẫn triển khai

Thỏa thuận cần đảm bảo rằng không có sự hiểu nhầm giữa tổ chức và bên thứ ba.

Các điều khoản sau cần được xem xét đưa vào bản thỏa thuận nhằm thỏa mãn các yêu cầu an toàn đã xác định (xem 5.2.1):

a) chính sách an toàn thông tin;

b) các biện pháp quản lý nhằm đảm bảo tài sản được bảo vệ, bao gồm:

1) các thủ tục bảo vệ tài sản của tổ chức, bao gồm thông tin, phần mềm và phần cứng;

2) các cơ chế và biện pháp quản lý vật lý được yêu cầu;

3) các biện pháp quản lý nhằm đảm bảo việc bảo vệ chống lại phần mềm độc hại;

4) các thủ tục xác định xem có tổn hại nào đến tài sản hay không, ví dụ mất mát hoặc chỉnh sửa thông tin, phần mềm và phần cứng;

5) các biện pháp quản lý nhằm đảm bảo khôi phục hoặc cấu trúc tại thông tin và tài sản khi kết thúc hoặc tại một thời điểm thỏa thuận trong toàn bộ giai đoạn hiệu lực của thỏa thuận;

6) tính bí mật, tính toàn vẹn, tính sẵn sàng, và thuộc tính liên quan bất kỳ của các tài sản;

7) các hạn chế về sao chép và tiết lộ thông tin, và áp dụng các thỏa thuận về bảo mật (xem 5.1.5);

c) đào tạo người dùng và người quản lý về các phương pháp, thủ tục và an toàn thông tin;

d) đảm bảo rằng người dùng hiểu về các vai trò và trách nhiệm của mình về an toàn thông tin;

e) các quy định về điều chuyển nhân sự khi có yêu cầu;

f) các trách nhiệm về lắp đặt và bảo dưỡng phần cứng và phần mềm;

g) cấu trúc báo cáo rõ ràng và các định dạng báo cáo đã thỏa thuận;

h) quy trình rõ ràng về quản lý các thay đổi;

i) chính sách giám sát truy cập, bao gồm:

1) các lý do, yêu cầu và lợi ích khác nhau chứng minh nhu cầu cần truy cập của tổ chức thứ ba;

2) các phương pháp truy cập được phép, quản lý và sử dụng các thông tin cá nhân như ID và mật khẩu của người dùng;

3) một quy trình cấp phép truy cập và đặc quyền đối với người dùng;

4) một yêu cầu duy trì danh sách các cá nhân được cấp phép sử dụng dịch vụ, và quyền và đặc quyền truy cập của họ;

5) một thông báo rằng tất cả các truy cập chưa được cấp phép một cách hợp lệ đều bị cấm;

6) một quy trình thu hồi quyền truy cập hoặc ngắt kết nối giữa các hệ thống;

j) các thủ tục báo cáo, thông báo và điều tra về các sự cố an toàn thông tin và các lỗ hổng an toàn, cũng như những vi phạm các yêu cầu đã công bố trong bản thỏa thuận;

k) mô tả về sản phẩm hoặc dịch vụ được cung cấp, và mô tả về thông tin đã sẵn sàng cùng với phân cấp an toàn của thông tin (xem 6.2.1);

l) mức kỳ vọng của dịch vụ và các mức không chấp nhận được của dịch vụ;

m) định nghĩa về chỉ tiêu hiệu suất, việc giám sát và báo cáo chúng;

n) quyền giám sát, và thu hồi, khai thác liên quan đến các tài sản của tổ chức;

o) quyền được đánh giá các trách nhiệm đã xác định trong thỏa thuận, quyền được thuê tổ chức thứ ba thực hiện các công việc đánh giá, và quyền được công bố các quyền do luật pháp quy định của nhân viên đánh giá;

p) thiết lập quy trình nâng dần cấp xử lý để xử lý sự cố;

q) các yêu cầu về tính liên tục của dịch vụ, bao gồm các chỉ tiêu về độ sẵn sàng và độ tin cậy, phù hợp với các thứ tự ưu tiên về nghiệp vụ;

r) các nghĩa vụ pháp lý tương ứng của các tổ chức theo thỏa thuận;

s) các trách nhiệm đối với các vấn đề pháp lý và phương thức nhằm đảm bảo rằng các yêu cầu pháp lý đều được thỏa mãn, ví dụ cưỡng chế bảo vệ dữ liệu, đặc biệt quan tâm đến các hệ thống luật pháp quốc gia khác nếu thỏa thuận có sự hợp tác với các tổ chức của các quốc gia khác (xem thêm 14.1);

t) các quyền sở hữu trí tuệ (IPR) và đăng ký bản quyền (xem 14.1.2) và bảo vệ công việc có sự phối hợp cộng tác (xem thêm 5.1.5);

u) nếu việc hợp tác với tổ chức thứ ba có thêm các nhà thầu phụ thì cần triển khai các biện pháp quản lý an toàn đối với các nhà thầu phụ này;

v) các điều kiện thương lượng lại/hủy bỏ các thỏa thuận:

1) cần thực hiện một kế hoạch đột xuất trong trường hợp cả hai phía đều mong muốn kết thúc mối quan hệ trước thời điểm kết thúc thỏa thuận như đã định;

2) thương lượng lại các thỏa thuận nếu các yêu cầu về an toàn của tổ chức thay đổi;

3) lập tài liệu danh sách các tài sản, các giấy phép, các thỏa thuận hoặc quyền liên quan đến chúng.

Các thông tin khác

Các thỏa thuận có thể rất khác nhau tùy theo các loại các tổ chức khác nhau và giữa các loại bên thứ ba khác nhau. Do vậy, cần cẩn trọng việc đưa ra các rủi ro và các yêu cầu về an toàn (xem thêm 5.2.1) trong các thỏa thuận. Khi cần thiết thì có thể mở rộng các biện pháp quản lý và các thủ tục cần thiết trong kế hoạch quản lý an toàn.

Nếu tổ chức thuê bên thứ ba quản lý an toàn thông tin, thì các thỏa thuận cần nhấn mạnh cách thức mà bên thứ ba cần nhằm đảm bảo đạt được độ an toàn thỏa đáng như đã xác định bởi công tác đánh giá rủi ro, và cách thức xác định và xử lý những thay đổi của các rủi ro.

Một vài trong số các khía cạnh khác nhau giữa thuê khoán và các hình thức cung cấp dịch vụ khác của bên thứ ba bao gồm vấn đề về nghĩa vụ pháp lý, việc lập kế hoạch về giai đoạn chuyển đổi và sự đổ vỡ tiềm ẩn của các hoạt động giai đoạn này, các công việc chuẩn bị cho việc lập kế hoạch đột xuất, thu thập và quản lý thông tin về các sự cố an toàn thông tin. Do vậy, vấn đề quan trọng là tổ chức phải lập kế hoạch và quản lý giai đoạn chuyển sang thuê khoán và có những xử lý phù hợp nhằm quản lý những thay đổi và thương lượng lại/kết thúc các thỏa thuận.

Các thủ tục duy trì xử lý thông tin trong trường hợp bên thứ ba không có khả năng cung cấp dịch vụ cũng cần được xem xét trong thỏa thuận nhằm ngăn chặn trì hoãn dàn xếp các dịch vụ thay thế.

Các thỏa thuận với bên thứ ba có thể có sự tham gia của các bên khác. Các thỏa thuận chấp nhận cho bên thứ ba truy cập cần cho phép chỉ định các bên có đủ tư cách khác và các điều kiện truy cập và tham gia của họ.

Nhìn chung các thỏa thuận chủ yếu đều được triển khai bởi tổ chức. Có thể có một số trường hợp mà bên thứ ba triển khai và áp đặt thỏa thuận đối với tổ chức. Tổ chức cần đảm bảo rằng an toàn thông tin của bản thân tổ chức sẽ không bị tác động một cách không cần thiết bởi các yêu cầu của tổ chức thứ ba được quy định trong các thỏa thuận áp đặt.

6. Quản lý tài sản

6.1. Trách nhiệm đối với tài sản

Mục tiêu: Nhằm hoàn thành và duy trì các biện pháp bảo vệ thích hợp đối với tài sản của tổ chức.

Tất cả các tài sản đều cần được kê khai và giao cho một người sở hữu.

Những người sở hữu tài sản cần được xác định đối với tất cả các tài sản và được giao trách nhiệm trong việc duy trì các biện pháp quản lý phù hợp. Nếu thích hợp thì người sở hữu tài sản có thể ủy quyền cho người khác triển khai các biện pháp quản lý nhất định nào đó nhưng người sở hữu vẫn phải duy trì trách nhiệm trong việc bảo vệ tài sản.

6.1.1. Kiểm kê tài sản

Biện pháp quản lý

Mọi tài sản cần được xác định rõ ràng, cần thực hiện và duy trì kiểm kê đối với tất cả các tài sản quan trọng.

Hướng dẫn triển khai

Tổ chức cần xác định tất cả các tài sản và tầm quan trọng của các tài sản này cần được ghi vào văn bản. Biên bản kiểm kê tài sản cần chứa tất cả các thông tin cần thiết nhằm phục vụ việc khôi phục thông tin trong trường hợp có thảm họa, bao gồm loại tài sản, định dạng, vị trí, thông tin dự phòng, thông tin đăng ký, và giá trị nghiệp vụ. Biên bản kiểm kê không được sao chép các biên bản kiểm kê khác những thông tin không cần thiết, nhưng cần đảm bảo nội dung thống nhất.

Hơn nữa, quyền sở hữu (xem 6.1.2) và phân loại thông tin (xem 6.2) đối với các tài sản cần

được thỏa thuận và ghi thành văn bản. Các mức độ bảo vệ tương ứng với tầm quan trọng của các tài sản cũng cần được xác định dựa trên tầm quan trọng của các tài sản, giá trị nghiệp vụ và phân loại an toàn của tài sản đó (xem ISO/IEC TR 13335-3 để có thông tin chi tiết hơn về cách thức định giá các tài sản nhằm thể hiện được tầm quan trọng của chúng).

Thông tin khác

Có rất nhiều loại tài sản, bao gồm:

a) thông tin: cơ sở dữ liệu và các tệp dữ liệu, các hợp đồng và thỏa thuận, văn bản về hệ thống, thông tin tìm kiếm, hướng dẫn sử dụng, tài liệu tập huấn, các thủ tục khai thác hoặc hỗ trợ, các kế hoạch nghiệp vụ liên tục, các truy vết, và thông tin thu thập được;

b) các tài sản phần mềm: phần mềm ứng dụng, phần mềm hệ thống, các công cụ phát triển, và các tiện ích;

c) các tài sản vật chất: thiết bị máy tính, thiết bị truyền thông, thiết bị di động và các thiết bị khác;

d) các dịch vụ: các dịch vụ truyền thông và tính toán, các tiện ích chung, ví dụ sưởi, chiếu sáng, năng lượng, và điều hòa nhiệt độ;

e) con người, và các văn bằng chứng chỉ, các kỹ năng và kinh nghiệm của họ;

f) tài sản vô hình, như danh tiếng và hình ảnh của tổ chức.

Các cuộc 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). Quy trình kiểm kê tài sản là một điều kiện tiên quyết vô cùng quan trọng trong quản lý rủi ro (xem thêm điều 3).

6.1.2. Quyền sở hữu tài sản

Biện pháp quản lý

Mọi thông tin và tài sản gắn với phương tiện xử lý thông tin phải được quản lý, kiểm soát bởi một bộ phận do tổ chức chỉ định.

Hướng dẫn triển khai

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

a) đảm bảo rằng thông tin và các tài sản liên quan đến các phương tiện xử lý thông tin được phân loại phù hợp;

b) xác định và định kỳ soát xét lại các giới hạn và phân loại truy cập, cân nhắc các chính sách quản lý truy cập có thể áp dụng.

Quyền sở hữu có thể được chỉ định cho:

a) một quy trình nghiệp vụ;

b) các hoạt động nhất định;

c) một ứng dụng; hoặc

d) một tập các dữ liệu xác định;

Thông tin khác

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.

6.1.3. Sử dụng hợp lý tài sản

Biện pháp quản lý

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

Hướng dẫn triển khai

Tất cả nhân viên, người của nhà thầu và bên thứ ba cần tuân theo các quy tắc sử dụng được phép các thông tin và tài sản liên quan đến các phương tiện xử lý thông tin, bao gồm:

a) các quy tắc sử dụng internet và thư điện tử (xem 9.8);

b) các hướng dẫn sử dụng các thiết bị di động, đặc biệt là sử dụng ở bên ngoài trụ sở của tổ chức (xem 10.7.1);

Các quy tắc hoặc hướng dẫn cụ thể cần được ban quản lý liên quan đề xuất. Những nhân viên, các nhà thầu 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 các giới hạn đang áp dụng trong việc sử dụng thông tin và tài sản của tổ chức liên quan đến các phương tiện xử lý thông tin và các nguồn tài nguyên. Họ cần có trách nhiệm trong việc sử dụng mọi nguồn tài nguyên xử lý thông tin và mọi hình thức sử dụng tài nguyên xử lý thông tin theo trách nhiệm của họ.

6.2. Phân loại thông tin

Mục tiêu: Nhằm đảm bảo thông tin sẽ có mức độ bảo vệ thích hợp.

Thông tin cần được phân loại nhằm chỉ ra nhu cầu, độ ưu tiên, và mức độ bảo vệ dự kiến khi xử lý thông tin.

Thông tin có các mức độ nhạy cảm và độ quan trọng thay đổi. Một số danh mục thông tin có thể cần mức bảo vệ cao hơn hoặc cần được xử lý đặc biệt, cần sử dụng cơ chế phân loại thông tin nhằm xác định tập các mức bảo vệ phù hợp và trao đổi về nhu cầu cần có các biện pháp xử lý đặc biệt.

6.2.1. Hướng dẫn phân loại

Biện pháp quản lý

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

Hướng dẫn triển khai

Việc phân loại và các biện pháp quản lý bảo vệ liên quan cần xem xét đến nhu cầu nghiệp vụ trong việc chia sẻ hoặc hạn chế thông tin và các ảnh hưởng nghiệp vụ liên quan đến các nhu cầu này.

Các hướng dẫn phân loại cần đưa ra các quy ước cho việc phân loại ban đầu và việc phân loại lại theo thời gian phù hợp với chính sách quản lý truy cập đã định trước nào đó (xem 10.1.1).

Cần xác định trách nhiệm của người sở hữu tài sản (xem 6.1.2) trong việc xác định phân loại tài sản, định kỳ soát xét lại phân loại, và đảm bảo rằng phân loại này đã cập nhật và ở mức độ phù hợp. Việc phân loại cần xem xét đến hậu quả kết hợp như đề cập trong 9.7.2.

Cũng cần quan tâm đến số các cấp độ phân loại và lợi ích thu được khi sử dụng chúng. Các cơ chế phân loại quá phức tạp cũng có thể trở thành cồng kềnh và không có hiệu quả về mặt kinh tế hoặc lại không khả thi. Cần cẩn trọng trong việc biên dịch các nhãn phân loại trong các văn bản giữa các tổ chức, các nhãn có tên giống nhau hoặc tương tự nhau có thể có các định nghĩa khác nhau.

Thông tin khác

Mức bảo vệ có thể được quyết định bởi việc phân tích tính bí mật, tính toàn vẹn, tính sẵn sàng và các yêu cầu bất kỳ khác đối với thông tin.

Thông tin thường không còn nhạy cảm hoặc quan trọng nữa sau một khoảng thời gian nhất định,

ví dụ, khi thông tin đã được công bố. Các khía cạnh này cũng cần được quan tâm, vì việc phân loại quá phức tạp cũng có thể dẫn đến việc triển khai các biện pháp quản lý không cần thiết và làm phát sinh thêm chi phí.

Việc cân nhắc các văn bản với các yêu cầu an toàn tương tự nhau khi quyết định các mức phân loại cũng có thể giúp làm đơn giản hóa công tác phân loại.

Nhìn chung, việc phân loại thông tin là một con đường nhanh nhất trong việc xác định phương thức xử lý và bảo vệ thông tin.

6.2.2. Gắn nhãn và xử lý thông tin

Biện pháp quản lý

Các thủ tục cần thiết cho việc gán 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 triển khai

Các thủ tục dán nhãn thông tin cần được xây dựng cho tất cả các tài sản thông tin ở cả dạng vật lý và điện tử.

Đầu ra của các hệ thống chứa các thông tin đã được phân loại là nhạy cảm hoặc quan trọng cần mang một nhãn phân loại phù hợp (ở đầu ra). Việc dán nhãn cần thể hiện phân loại theo các quy tắc đã thiết lập trong 6.2.1. Các danh mục cần quan tâm bao gồm các báo cáo in sẵn, các màn hình hiển thị, phương tiện lưu giữ (ví dụ băng, đĩa, CD), các thông điệp điện tử, và các phần mềm truyền tệp.

Đối với từng mức phân loại, cũng cần xác định các thủ tục xử lý bao gồm xử lý an toàn, lưu trữ, truyền, phân loại lại, và hủy bỏ. Cũng cần có các thủ tục về thắt chặt giám sát và ghi lại bất kỳ sự kiện nào liên quan đến an toàn.

Các thỏa thuận với các tổ chức khác về chia sẻ thông tin cần chứa các thủ tục xác định phân loại của thông tin đó và biên dịch các nhãn phân loại giữa các tổ chức.

Thông tin khác

Việc dán nhãn và xử lý thông tin đã phân loại một cách an toàn là một yêu cầu then chốt đối với các chia sẻ thông tin. Các nhãn vật lý là một dạng nhãn thông thường. Tuy nhiên, một số tài sản thông tin, nhãn các tài liệu ở dạng điện tử, thì không thể dán nhãn dưới dạng vật lý và khi đó cần thực hiện dán nhãn điện tử. Ví dụ, nhãn thông tin có thể xuất hiện trên màn hình hoặc được hiển thị bằng máy tính. Nếu việc dán nhãn không khả thi thì các phương tiện phân loại thông tin khác có thể được áp dụng, ví dụ thông qua các thủ tục hoặc các mô tả về dữ liệu.

7. Đảm bảo an toàn thông tin từ nguồn nhân lực

7.1. Trước khi tuyển dụng

Mục tiêu: Đảm bảo rằng các nhân viên, người của nhà thầu và bên thứ ba hiểu rõ trách nhiệm của mình và phù hợp với vai trò được giao, đồng thời giảm thiểu các rủi ro do đánh cắp, gian lận và lạm dụng chức năng, quyền hạn.

Các trách nhiệm về an toàn cần được nhấn mạnh trước khi sử dụng lao động theo những đặc điểm công việc tương xứng, và theo các điều khoản và điều kiện về sử dụng lao động.

Tất cả những ứng viên, người của các nhà thầu và bên thứ ba đều cần được kiểm tra đầy đủ, nhất là đối với những công việc có tính chất nhạy cảm.

Các nhân viên, người của các nhà thầu và bên thứ ba của các phương tiện xử lý thông tin cần ký vào một bản thỏa thuận về vai trò và trách nhiệm đảm bảo an toàn thông tin của họ.

7.1.1. Các vai trò và trách nhiệm

Biện pháp quản lý

Các vai trò và trách nhiệm đảm bảo an toàn thông tin của các nhân viên, người của nhà thầu và

bên thứ ba phải được xác định và ghi thành văn bản phù hợp với chính sách an toàn thông tin của tổ chức.

Hướng dẫn triển khai

Các vai trò và trách nhiệm về an toàn cần gồm các yêu cầu về:

a) triển khai và hành động phù hợp với các chính sách an toàn thông tin của tổ chức (xem 4.1);

b) bảo vệ tài sản trước sự truy nhập, đánh cắp, chỉnh sửa, phá hoại hoặc can thiệp bất hợp pháp;

c) thực hiện các hoạt động và xử lý an toàn bảo mật cụ thể;

d) báo cáo các sự kiện an toàn, những sự kiện tiềm ẩn hoặc những rủi ro an toàn khác đến tổ chức.

Các vai trò và trách nhiệm cần được xác định rõ và thông báo một cách rõ ràng đến các ứng viên trong suốt quá trình trước khi sử dụng lao động.

Thông tin khác

Những mô tả về công việc có thể được sử dụng để ghi lại các vai trò và trách nhiệm về an toàn thông tin. Các vai trò và trách nhiệm về an toàn của các cá nhân chưa được cam kết trong quá trình sử dụng nhân lực của tổ chức, ví dụ đã được cam kết qua một tổ chức thứ ba, cũng cần được xác định rõ và thông báo đến toàn bộ nhân viên.

7.1.2. Thẩm tra

Biện pháp quản lý

Việc xác minh lai lịch của mọi ứng viên tuyển dụng, người của nhà thầu và bên thứ ba 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 triển khai

Các cuộc xác minh lai lịch cần quan tâm đến tính riêng tư, việc bảo vệ dữ liệu cá nhân và/hoặc luật sử dụng lao động, và nếu được phép cần bao gồm những vấn đề sau:

a) sự sẵn sàng 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 (hộ chiếu hoặc giấy tờ tương tự);

e) các kiểm tra chi tiết hơn, ví dụ các kiểm tra về tài chính hoặc các kiểm tra về hồ sơ tội phạm;

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 bảo mật cao, thì tổ chức cũng cần xem xét thực hiện các cuộc kiểm tra chi tiết hơn.

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

Quá trình thẩm tra cũng cần được thực hiện với các nhà thầu, và những người dùng thuộc bên thứ ba. Nếu các nhà thầu này được cung cấp qua một công ty môi giới thì hợp đồng với công ty này cần xác định rõ trách nhiệm của công ty trong việc thẩm tra và các thủ tục khai báo mà họ cần tuân thủ nếu việc thẩm tra không hoàn tất hoặc nếu các kết quả thẩm tra gây ra hồ nghi hoặc lo ngại. Tương tự như vậy, thỏa thuận với bên thứ ba (xem thêm 5.2.3) cũng cần xác định rõ tất cả các trách nhiệm và các thủ tục thông báo về việc thẩm tra.

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 xứng.

Tuỳ theo quy định của luật pháp phù hợp mà các ứng viên cần phải được thông báo trước về các hoạt động thẩm tra này.

7.1.3. Điều khoản và điều kiện tuyển dụng

Biện pháp Quản lý

Như một phần của các ràng buộc trong hợp đồng, các nhân viên, người của nhà thầu và bên thứ ba phải đồng ý và ký vào các điều khoản và điều kiện của hợp đồng tuyển dụng. Việc này làm rõ trách nhiệm của người được tuyển dụng và tổ chức đối với an toàn thông tin.

Hướng dẫn triển khai

Các điều khoản và điều kiện tuyển dụng cần thể hiện cả chính sách an toàn của tổ chức bên cạnh việc công bố rằng :

a) tất cả các nhân viên, người của nhà thầu và bên thứ ba- những người được phép truy cập đến thông tin nhạy cảm, cần ký vào một thỏa thuận bảo mật hoặc không tiết lộ trước khi được cấp phép truy cập đến các phương tiện xử lý thông tin;

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 chế về bảo vệ dữ liệu (xem thêm 14.1.1 và 13.1.2);

c) các trách nhiệm đối với việc phân loại thông tin và quản lý tài sản thuộc tổ chức liên quan đến các dịch vụ và hệ thống thông tin được xử lý bởi các những nhân viên, người của nhà thầu hoặc bên thứ ba (xem thêm 6.2.1 và 9.7.3);

d) các trách nhiệm của người nhân viên, người của nhà thầu hoặc bên thứ ba trong việc xử lý thông tin nhận được từ các công ty khác hoặc các tổ chức bên ngoài;

e) các trách nhiệm của tổ chức trong việc xử lý thông tin cá nhân, bao gồm thông tin cá nhân có được sau hoặc trong quá trình sử dụng lao động của tổ chức (xem thêm 14.1.4);

f) các trách nhiệm sử dụng tài sản bên ngoài trụ sở của tổ chức và bên ngoài thời gian làm việc bình thường, ví dụ trong trường hợp làm việc tại nhà (xem thêm 8.2.5 và 10.7.1);

g) 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 thêm 7.3).

Tổ chức cần đảm bảo rằng các nhân viên, người của nhà thầu và bên thứ ba 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 với 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 thêm 7.3).

Thông tin khác

Có thể sử dụng một bản hướng dẫn trong đó đưa ra các trách nhiệm của các nhân viên, người của nhà thầu và bên thứ ba liên quan đến tính bảo mật, bảo vệ dữ liệu, nội quy, việc sử dụng phù hợp thiết bị và tài sản của tổ chức, cũng như cách thực hiện dự kiến. Nhà thầu hoặc những người dùng thuộc bên thứ ba có thể liên kết với một tổ chức bên ngoài, tổ chức này có thể được yêu cầu tham gia vào các thương thảo hợp đồng với sự đại diện của một cá nhân ký kết.

7.2. Trong thời gian làm việc

Mục tiêu: đảm bảo rằng mọi nhân viên của tổ chức, người của nhà thầu và bên thứ ba nhận thức được các mối nguy cơ và các vấn đề liên quan đến an toàn thông tin, trách nhiệm và nghĩa vụ pháp lý của họ, và được trang bị các kiến thức, điều kiện cần thiết nhằm hỗ trợ chính sách an toàn thông tin của tổ chức trong quá trình làm việc, và giảm thiểu các rủi ro do con người gây ra.

Cần được xác định các trách nhiệm của ban quản lý nhằm đảm bảo đạt được sự an toàn