INTERNATIONAL STANDARD

TIÊU CHUẨN QUỐC TẾ

ISO/IEC 27001

Third edition
2022-10

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

AN TOÀN THÔNG TIN, AN NINH MẠNG VÀ BẢO VỆ QUYỀN RIÊNG TƯ - HỆ THỐNG QUẢN LÝ AN TOÀN THÔNG TIN - CÁC YÊU CẦU

Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences

Tài liệu phục vụ Đào tạo nghiên cứu

Bản Dịch nhằm phục vụ Đào tạo và phổ biến Kiến thức, Khi áp dụng Cá nhân, Tổ chức phải tuân thủ nguyên tắc Bản Quyền và mua chính tức Tiêu chuẩn.

Liên hệ Vcard:

Lê xuân Trường

Lời nói đầu

ISO/IEC 27001:2022 (EV) hoàn toàn tương đương với ISO/IEC 27001:2022

Bản dịch tiếng Việt được thực hiện chỉ dùng cho mục đích tham khảo

Tài liệu phục vụ Đào tạo, nghiên cứu

Cộng đồng sử dụng và chia sẻ về Tiêu chuẩn ISO/IEC 27001

Group Zalo:



Introduction

0.1 General

This document has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an information security management system. The adoption of an information security management system is a strategic decision for an organization. The establishment and implementation of an organization's information security management system is influenced by the organization's needs and objectives, security requirements, the organizational processes used and the size and structure of the organization. All of these influencing factors are expected to change over time.

The information security management system preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed.

It is important that the information security management system is part of and integrated with the organization's processes and overall management structure and that information security is considered in the design of processes, information systems, and controls. It is expected that an information security management system implementation will be scaled in accordance with the needs of the organization.

This document can be used by internal and external parties to assess the organization's ability to meet the organization's own information security requirements.

The order in which requirements are presented in this document does not reflect their importance or imply the order in which they are to be implemented. The list items are enumerated for reference purpose only.

ISO/IEC 27000 describes the overview and the vocabulary of information security management systems, referencing the information security management system family of standards (including ISO/IEC 27003[2], ISO/IEC 27004[3] and ISO/IEC 27005[4]), with related terms and definitions.

0.2 Compatibility with other management system standards

This document applies the high-level structure, identical sub-clause titles, identical text, common terms, and core definitions defined in Annex SL of

0. Giới thiệu

0.1 Tổng quan

Tài liệu này được chuẩn bị nhằm cung cấp các yêu cầu cho việc thiết lập, áp dụng, duy trì và cải tiến liên tục Hệ thống quản lý An toàn thông tin (ISMS). Việc áp dụng ISMS là quyết định mang tính chiến lược của một tổ chức. Việc thiết lập và triển khai thực hiện hệ thống quản lý an toàn thông tin của một tổ chức chịu ảnh hưởng bởi các nhu cầu và các mục tiêu của tổ chức, các yêu cầu an toàn, các quá trình được sử dụng và bởi quy mô, cấu trúc của tổ chức. Tất cả các yếu tố ảnh hưởng đó có thể xảy ra sự thay đổi theo thời gian.

Hệ thống quản lý an toàn thông tin duy trì tính bảo mật, tính toàn vẹn và tính sẵn sàng của thông tin bằng cách áp dụng một quá trình quản lý rủi ro và mang lại sự tin cậy cho các bên quan tâm rằng các rủi ro đã được quản lý đầy đủ.

Điều quan trọng là hệ thống quản lý an toàn thông tin phải là một phần, và được tích hợp với các quá trình và cấu trúc quản lý tổng thể của tổ chức, và an toàn thông tin cần được quan tâm trong thiết kế các quá trình, các hệ thống thông tin, và các biện pháp kiểm soát. Chắc rằng việc triển khai một hệ thống quản lý an toàn thông tin sẽ được mở rộng, thu hẹp theo nhu cầu của tổ chức.

Tài liệu này có thể được sử dụng bởi nội bộ hoặc các tổ chức bên ngoài để đánh giá khả năng của tổ chức đáp ứng các yêu cầu an toàn thông tin của tổ chức.

Thứ tự của các yêu cầu được trình bày trong tài liệu này không phản ảnh tầm quan trọng của chúng cũng như không phản ảnh hàm ý về thứ tự mà chúng trình bày. Danh sách các mục là được liệt kê dành cho mục đích tham khảo.

ISO/IEC 27000 mô tả tổng quan và từ vựng của hệ thống quản lý an toàn thông tin, viện dẫn các tiêu chuẩn của bộ tiêu chuẩn về Hệ thống quản lý an toàn thông tin (bao gồm ISO/IEC 27003, ISO/IEC 27004 and ISO/IEC 27005), với các thuật ngữ và định nghĩa liên quan

0.2 Tương thích với các tiêu chuẩn hệ thống quản lý khác

Tài liệu này áp dụng cấu trúc cao cấp, đồng nhất giống nhau tiêu đề các điều khoản phụ, đồng nhất về văn bản, các thuật ngữ chung, và các định nghĩa cốt

Tài liệu phục vụ Đào tạo, nghiên cứu

Bản Dịch nhằm phục vụ Đào tạo và phổ biến Kiến thức, Khi áp dụng Cá nhân, Tổ chức phải tuân thủ nguyên tắc Bản Quyền và mua chính tức Tiêu chuẩn. (contact: Lê Xuân Trường 0868688767 / 0903452826)

ISO/IEC Directives, Part 1, Consolidated ISO Supplement, and therefore maintains compatibility with other management system standards that have adopted the Annex SL.

This common approach defined in the Annex SL will be useful for those organizations that choose to operate a single management system that meets the requirements of two or more management system standards.

lõi được định nghĩa trong Phụ lục SL của Chỉ thị ISO/IEC, Phần 1, Phụ lục hợp nhất ISO, và do đó đảm bảo duy trì khả năng tương thích với các tiêu chuẩn hệ thống quản lý khác đã áp dụng theo Phụ lục SL.

Cách tiếp cận chung được quy định tại Phụ lục SL sẽ hữu ích cho các tổ chức lựu chọn để vận hành một hệ thống quản lý duy nhất đáp ứng các yêu cầu của hai hoặc nhiều tiêu chuẩn hệ thống quản lý.

Tài liệu phục vụ Đào tạo, nghiên cứu

Bản Dịch nhằm phục vụ Đào tạo và phổ biến Kiến thức, Khi áp dụng Cá nhân, Tổ chức phải tuân thủ nguyên tắc Bản Quyền và mua chính tức Tiêu chuẩn. (contact: Lê Xuân Trường 0868688767 / 0903452826)

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

1 Scope

This document specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. This document also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization.

The requirements set out in this document are generic and are intended to be applicable to all organizations, regardless of type, size or nature. Excluding any of the requirements specified in Clauses 4 to 10 is not acceptable when an organization claims conformity to this document.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, Information technology — Security techniques — Information security management systems — Overview and vocabulary

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

An toàn thông tin, an ninh mạng và bảo vệ quyền riêng

1. Phạm vi

Tài liệu này chỉ định rõ các yêu cầu đối với hoạt động thiết lập, áp dụng, duy trì và cải tiến liên tục một Hệ thống quản lý An toàn thông tin trong bối cảnh của tổ chức. Tài liệu này cũng bao gồm các yêu cầu cho hoạt động đánh giá và xử lý các rủi ro an toàn thông tin đáp ứng nhu cầu của tổ chức.

Các yêu cầu trình bày trong tài liệu này mang tính tổng quát và nhằm áp dụng cho tất cả các tổ chức, bất kể loại hình, qui mô, tính chất. Việc loại trừ bất kỳ yêu cầu nào trong điều 4 đến 10 đều không được chấp nhận khi tổ chức tuyên bố phù hợp với tài liệu này.

2. Tài liệu viện dẫn

Các tài liệu dưới đây, được đề cập đến trong văn bản theo cách mà một số hoặc tất cả nội dung của chúng tạo thành các yêu cầu của văn bản này. Với các trích dẫn ghi ngày tháng, chỉ có các trích dẫn được nêu mới áp dụng. Các trích dẫn không ghi ngày tháng, bản mới nhất của tài liệu trích dẫn (bao gồm cả bổ sung) được áp dụng.

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

Tài liệu này sử dụng các thuật ngữ và định nghĩa của ISO/IEC 27000

ISO và IEC duy trì cơ sở dữ liệu thuật ngữ để sử dụng trong hoạt động tiêu chuẩn hóa tại các địa chỉ sau:

- Nền tảng ISO Online: có tại https://www.iso.org/obp

-IEC Electropedia: có tại https://www.electropedia.org/

Tài liệu phục vụ Đào tạo, nghiên cứu

Bản Dịch nhằm phục vụ Đào tạo và phổ biến Kiến thức, Khi áp dụng Cá nhân, Tổ chức phải tuân thủ nguyên tắc Bản Quyền và mua chính tức Tiêu chuẩn. (contact: Lê Xuân Trường 0868688767 / 0903452826)

4 Context of the organization

4.1 Understanding the organization and its context

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.

NOTE Determining these issues refers to establishing the external and internal context of the organization considered in Clause 5.4.1 of ISO 31000:2018[5].

4.2 Understanding the needs and expectations of interested parties

The organization shall determine:

a) interested parties that are relevant to the information security management system;

b) the relevant requirements of these interested parties;

c) which of these requirements will be addressed through the information security management system.

NOTE The requirements of interested parties can include legal and regulatory requirements and contractual obligations.

4.3 Determining the scope of the information security management system

The organization shall determine the boundaries and applicability of the information security management system to establish its scope.

When determining this scope, the organization shall consider:

a) the external and internal issues referred to in 4.1;

b) the requirements referred to in 4.2;

c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.

4. Bối cảnh của tổ chức

4.1 Hiểu tổ chức và bối cảnh của tổ chức

Tổ chức phải xác định các vấn đề bên ngoài và nội bộ liên quan đến mục đích của tổ chức và ảnh hưởng đến khả năng đạt được (các) kết quả dự kiến của hệ thống quản lý an toàn thông tin của tổ chức.

Chú thích: Xác định các vấn đề liên quan đến việc thiết lập bối cảnh bên ngoài và nội bộ của các tổ chức có thể xem xét tại khoản 5.4.1 của ISO 31000.

4.2 Hiểu nhu cầu và mong đợi của các bên quan tâm

Tổ chức phải xác định:

a) các bên quan tâm có liên quan đến hệ thống quản lý an toàn thông tin; và

b) các yêu cầu liên quan của các bên quan tâm này;

c) yêu cầu nào trong số này sẽ được giải quyết thông qua hệ thống quản lý an toàn thông tin

CHÚ THÍCH: Các yêu cầu của các bên quan tâm **có thể bao gồm các yêu cầu pháp lý và nghĩa vụ hợp đồng**.

4.3 Xác định phạm vi của hệ thống quản lý an toàn thông tin

Tổ chức phải xác định ranh giới và phạm vi áp dụng hệ thống quản lý an toàn thông tin để thiết lập phạm vi của nó.

Khi xác định phạm vi này, tổ chức phải xem xét:

a) các vấn đề bên ngoài và nội bộ được đề cập trong 4.1;

b) các yêu cầu nêu trong 4.2;

c) những cái chung và những phần phụ thuộc giữa các hoạt động được thực hiện bởi tổ chức, và các hoạt động được thực hiện bởi các tổ chức khác.

Tài liệu phục vụ Đào tạo, nghiên cứu

Bản Dịch nhằm phục vụ Đào tạo và phổ biến Kiến thức, Khi áp dụng Cá nhân, Tổ chức phải tuân thủ nguyên tắc Bản Quyền và mua chính tức Tiêu chuẩn. (contact: Lê Xuân Trường 0868688767 / 0903452826)

The scope shall be available as documented information.

4.4 Information security management system

The organization shall establish, implement, maintain and continually improve an information security management system, including the processes needed and their interactions, in accordance with the requirements of this document.

5 Leadership

5.1 Leadership and commitment

Top management shall demonstrate leadership and commitment with respect to the information security management system by:

a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;

b) ensuring the integration of the information security management system requirements into the organization's processes;

c) ensuring that the resources needed for the information security management system are available;

d) communicating the importance of effective information security management and of conforming to the information security management system requirements;

e) ensuring that the information security management system achieves its intended outcome(s);

f) directing and supporting persons to contribute to the effectiveness of the information security management system;

g) promoting continual improvement; and

h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

NOTE Reference to "business" in this document can be interpreted broadly to mean those activities that are core to the purposes of the organization's existence.

Phạm vi sẽ phải sẵn có như một thông tin được lập văn bản

4.4 Hệ thống quản lý an toàn thông tin

Tổ chức phải thiết lập, áp dụng, duy trì và cải tiến liên tục hệ thống quản lý an toàn thông tin, bao gồm các quá trình cần thiết và các tương tác giữa các quá trình, phù hợp với các yêu cầu của tài liệu này.

5. Sự lãnh đạo

5.1 Sự lãnh đạo và sự cam kết

Lãnh đạo cao nhất phải chứng minh sự lãnh đạo và sự cam kết liên quan đến hệ thống quản lý an toàn thông tin thông qua việc:

a) đảm bảo chính sách an toàn thông tin và các mục tiêu an toàn thông tin được thiết lập và tương thích với các định hướng chiến lược của tổ chức;

b) đảm bảo sự tích hợp của các yêu cầu hệ thống quản lý an toàn thông tin vào các quá trình của tổ chức;

c) đảm bảo rằng các nguồn lực cần thiết cho hệ thống quản lý an toàn thông tin được đáp ứng;

d) truyền đạt tầm quan trọng của hiệu lực quản lý an toàn thông tin và sự tuân thủ với các yêu cầu hệ thống quản lý an toàn thông tin;

e) đảm bảo hệ thống quản lý an toàn thông tin đạt được (các) kết quả mong muốn;

f) chỉ đạo và hỗ trợ nhân sự tạo nên sự hiệu lực của hệ thống quản lý an toàn thông tin;

g) thúc đẩy cải tiến liên tục, và

h) hỗ trợ các vai trò quản lý khác có liên quan để chứng minh sự lãnh đạo của ban lãnh đạo tương ứng với vai trò, trách nhiệm của từng vị trí.

CHÚ THÍCH: Việc tham chiếu đến "kinh doanh" trong tài liệu này **có thể được hiểu theo nghĩa rộng có nghĩa là những hoạt động cốt lõi cho mục đích tồn tại của tổ chức**

Tài liệu phục vụ Đào tạo, nghiên cứu

Bản Dịch nhằm phục vụ Đào tạo và phổ biến Kiến thức, Khi áp dụng Cá nhân, Tổ chức phải tuân thủ nguyên tắc Bản Quyền và mua chính tức Tiêu chuẩn. (contact: Lê Xuân Trường 0868688767 / 0903452826)

5.2 Policy

Top management shall establish an information security policy that:

a) is appropriate to the purpose of the organization;

b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives;

c) includes a commitment to satisfy applicable requirements related to information security;

d) includes a commitment to continual improvement of the information security management system. The information security policy shall:

e) be available as documented information;

f) be communicated within the organization;

g) be available to interested parties, as appropriate.

5.3 Organizational roles, responsibilities and authorities

Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated within the organization.

Top management shall assign the responsibility and authority for:

a) ensuring that the information security management system conforms to the requirements of this document;

b) reporting on the performance of the information security management system to top management.

NOTE Top management can also assign responsibilities and authorities for reporting performance of the information security management system within the organization.

6 Planning

6.1 Actions to address risks and opportunities

6.1.1 General

5.2 Chính sách

Lãnh đạo cao nhất phải thiết lập một chính sách an toàn thông tin:

a) phù hợp với mục đích của tổ chức;

b) bao gồm các mục tiêu an toàn thông tin (xem 6.2) hoặc cung cấp khuôn khổ cho việc thiết lập các mục tiêu an toàn thông tin;

c) bao gồm việc cam kết đáp ứng các yêu cầu áp dụng liên quan đến an toàn thông tin; và

d) bao gồm việc cam kết cải tiến liên tục hệ thống quản lý an toàn thông tin. Chính sách an toàn thông tin phải:

e) sẵn có như một thông tin được lập văn bản;

f) được truyền đạt trong tổ chức;

g) sẵn có cho các bên quan tâm, hoặc khi thấy thích hợp.

5.3 Vai trò, trách nhiệm và quyền hạn

Lãnh đạo cao nhất phải đảm bảo rằng các trách nhiệm và quyền hạn cho các vai trò liên quan đến an toàn thông tin được xác định và truyền đạt.

Lãnh đạo cao nhất phải phân công trách nhiệm và quyền hạn cho việc:

a) đảm bảo rằng hệ thống quản lý an toàn thông tin phù hợp với các yêu cầu của tài liệu này, và

b) báo cáo về việc thực hiện hệ thống quản lý an toàn thông tin cho lãnh đạo cao nhất.

CHÚ THÍCH: Lãnh đạo cao nhất cũng có thể phân công các trách nhiệm và quyền hạn đối với việc báo cáo kết quả hoạt động của hệ thống quản lý an toàn thông tin trong tổ chức.

6. Hoạch định

6.1 Hành động để giải quyết rủi ro và các cơ hội cải tiến

6.1.1 Khái quát

Tài liệu phục vụ Đào tạo, nghiên cứu

Bản Dịch nhằm phục vụ Đào tạo và phổ biến Kiến thức, Khi áp dụng Cá nhân, Tổ chức phải tuân thủ nguyên tắc Bản Quyền và mua chính tức Tiêu chuẩn. (contact: Lê Xuân Trường 0868688767 / 0903452826)

When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to:

a) ensure the information security management system can achieve its intended outcome(s);

b) prevent, or reduce, undesired effects;

c) achieve continual improvement.

The organization shall plan:

d) actions to address these risks and opportunities; and

e) how to

1) integrate and implement the actions into its information security management system processes; and

2) evaluate the effectiveness of these actions.

6.1.2 Information security risk assessment

The organization shall define and apply an information security risk assessment process that:

a) establishes and maintains information security risk criteria that include:

1) the risk acceptance criteria; and

2) criteria for performing information security risk assessments;

b) ensures that repeated information security risk assessments produce consistent, valid and comparable results;

c) identifies the information security risks:

1) apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and

2) identify the risk owners;

Khi hoạch định hệ thống quản lý an toàn thông tin, tổ chức phải quan tâm các vấn đề được đề cập trong 4.1 và các yêu cầu nêu trong 4.2 và xác định những rủi ro và các cơ hội cải tiến cần được giải quyết để:

a) đảm bảo hệ thống quản lý an toàn thông tin có thể đạt được (các) kết quả mong muốn;

b) ngăn chặn, hoặc giảm, các tác động không mong muốn, và

c) được cải tiến liên tục.

Tổ chức phải lập kế hoạch:

d) các hành động để giải quyết các rủi ro và các cơ hội này, và

e) làm thế nào để

1) tích hợp và triển khai các hành động này vào các quá trình hệ thống quản lý an toàn thông tin của tổ chức, và

2) đánh giá tính hiệu lực của các hành động này.

6.1.2 Đánh giá rủi ro an toàn thông tin

Tổ chức phải xác định và áp dụng một quá trình đánh giá rủi ro an toàn thông tin trong đó:

a) thiết lập và duy trì các tiêu chí rủi ro an toàn thông tin, bao gồm:

1) tiêu chí chấp nhận rủi ro; và

2) tiêu chí thực hiện các cuộc đánh giá rủi ro an toàn thông tin;

b) đảm bảo rằng các cuộc đánh giá rủi ro an toàn thông tin lặp đi lặp lại tạo ra kết quả nhất quán, hợp lệ và có thể so sánh được;

c) xác định các rủi ro an toàn thông tin:

1) áp dụng quá trình đánh giá rủi ro an toàn thông tin để xác định các rủi ro liên quan tới sự mất mát của tính bảo mật, tính toàn vẹn và tính sẵn sàng của thông tin trong phạm vi của hệ thống ISMS, và

2) xác định các chủ sở hữu rủi ro

Tài liệu phục vụ Đào tạo, nghiên cứu

Bản Dịch nhằm phục vụ Đào tạo và phổ biến Kiến thức, Khi áp dụng Cá nhân, Tổ chức phải tuân thủ nguyên tắc Bản Quyền và mua chính tức Tiêu chuẩn. (contact: Lê Xuân Trường 0868688767 / 0903452826)

d) analyses the information security risks:

1) assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize;

2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and

3) determine the levels of risk;

e) evaluates the information security risks:

1) compare the results of risk analysis with the risk criteria established in 6.1.2 a); and

2) prioritize the analysed risks for risk treatment.

The organization shall retain documented information about the information security risk assessment process.

6.1.3 Information security risk treatment

The organization shall define and apply an information security risk treatment process to:

a) select appropriate information security risk treatment options, taking account of the risk assessment results;

b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen;

NOTE 1 Organizations can design controls as required, or identify them from any source.

c) compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted;

NOTE 2 Annex A contains a list of possible information security controls. Users of this document are directed to Annex A to ensure that no necessary information security controls are overlooked.

NOTE 3 The information security controls listed in Annex A are not exhaustive and additional

d) phân tích các rủi ro an toàn thông tin:

1) đánh giá các hậu quả tiềm tàng sẽ xảy ra nếu các rủi ro được xác định trong 6.1.2 c) 1) trở thành hiện thực;

2) đánh giá khả năng thực tế sự xuất hiện của các rủi ro đã được xác định trong 6.1.2 c) 1); và

3) xác định các mức độ của rủi ro;

e) ước lượng rủi ro an toàn thông tin:

1) so sánh các kết quả phân tích rủi ro với các tiêu chí rủi ro đã được thiết lập trong 6.1.2 a) và

2) phân tích mức độ ưu tiên cho việc xử lý rủi ro.

Tổ chức phải lưu giữ thông tin được lập văn bản về quá trình đánh giá rủi ro an toàn thông tin.

6.1.3 Xử lý rủi ro an toàn thông tin

Tổ chức phải xác định và áp dụng một quá trình xử lý rủi ro an toàn thông tin để:

a) lựa chọn các phương pháp xử lý rủi ro an toàn thông tin thích hợp, có tính đến kết quả đánh giá rủi ro;

b) xác định tất cả các biện pháp kiểm soát cần thiết để thực hiện (các) phương án xử lý rủi ro an toàn thông tin đã lựa chọn;

CHÚ THÍCH 1: Các tổ chức có thể thiết kế các biện pháp kiểm soát theo yêu cầu, hoặc xác định chúng từ bất cứ nguồn nào.

c) so sánh các biện pháp kiểm soát đã xác định trong 6.1.3 b) ở trên với những biện pháp kiểm soát trong Phụ lục A và xác minh rằng không có biện pháp kiểm soát cần thiết nào bị bỏ qua; ;

CHÚ THÍCH 2: Phụ lục A chứa một danh sách các biện pháp kiểm soát an toàn thông tin có thể có. Người sử dụng Tài liệu này được định hướng đến Phụ lục A để đảm bảo rằng không có biện pháp kiểm soát quan trọng nào bị bỏ qua.

CHÚ THÍCH 3: Các biện pháp kiểm soát an toàn thông tin được liệt kê trong Phụ lục A là chưa đầy đủ

Tài liệu phục vụ Đào tạo, nghiên cứu

Bản Dịch nhằm phục vụ Đào tạo và phổ biến Kiến thức, Khi áp dụng Cá nhân, Tổ chức phải tuân thủ nguyên tắc Bản Quyền và mua chính tức Tiêu chuẩn. (contact: Lê Xuân Trường 0868688767 / 0903452826)

information security controls can be included if needed.

d) produce a Statement of Applicability that contains:

— the necessary controls (see 6.1.3 b) and c));

— justification for their inclusion;

— whether the necessary controls are implemented or not; and

— the justification for excluding any of the Annex A controls.

e) formulate an information security risk treatment plan; and

f) obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks.

The organization shall retain documented information about the information security risk treatment process.

NOTE 4 The information security risk assessment and treatment process in this document aligns with the principles and generic guidelines provided in ISO 31000[5].

6.2 Information security objectives and planning to achieve them

The organization shall establish information security objectives at relevant functions and levels.The information security objectives shall:

a) be consistent with the information security policy;

b) be measurable (if practicable);

c) take into account applicable information security requirements, and results from risk assessment and risk treatment;

d) be monitored;

e) be communicated;

f) be updated as appropriate;

g) be available as documented information.

và các biện pháp kiểm soát an toàn thông tin bổ sung có thể được đưa vào nếu cần.

d) đưa ra một bản Tuyên bố áp dụng có chứa:

- các biện pháp kiểm soát cần thiết (xem 6.1.3 a), b) và c));

- bao gồm các giải thích, cho dù chúng được triển khai hay không; và

- lý giải cho việc loại trừ các biện pháp kiểm soát trong Phụ lục A;

e) xây dựng một kế hoạch xử lý rủi ro an toàn thông tin;

f) đạt được sự chấp thuận của các chủ sở hữu rủi ro về kế hoạch xử lý rủi ro an toàn thông tin và sự chấp nhận các rủi ro an toàn thông tin còn lại.

Tổ chức phải có trách nhiệm lưu giữ thông tin được lập văn bản về quá trình xử lý rủi ro an toàn thông tin

CHÚ THÍCH 4: Quá trình đánh giá và xử lý rủi ro an toàn thông tin trong tài liệu này gắn với các nguyên tắc và hướng dẫn chung được cung cấp trong tiêu chuẩn ISO 31000.

6.2 Mục tiêu an toàn thông tin và hoạch định để đạt được mục tiêu

Tổ chức phải thiết lập các mục tiêu an toàn thông tin tại các cấp và bộ phận chức năng thích hợp có liên quan. **Các mục tiêu an toàn thông tin phải:**

a) nhất quán với chính sách an toàn thông tin;

b) có thể đo lường được (nếu có thể);

c) tính đến các yêu cầu bảo mật thông tin hiện hành và các kết quả từ đánh giá rủi ro và xử lý rủi ro;

d) được theo dõi;

e) được truyền đạt;

f) được cập nhật thích hợp.

g) sẵn có dưới dạng thông tin dạng văn bản.

Tài liệu phục vụ Đào tạo nghiên cứu

Bản Dịch nhằm phục vụ Đào tạo và phổ biến Kiến thức, Khi áp dụng Cá nhân, Tổ chức phải tuân thủ nguyên tắc Bản Quyền và mua chính tức Tiêu chuẩn. (contact: Lê Xuân Trường 0868688767 / 0903452826)

The organization shall retain documented information on the information security objectives.

When planning how to achieve its information security objectives, the organization shall determine:

h) what will be done;

i) what resources will be required;

j) who will be responsible;

k) when it will be completed; and

l) how the results will be evaluated.

6.3 Planning of changes

When the organization determines the need for changes to the information security management system, the changes shall be carried out in a planned manner.

7 Support

7.1 Resources

The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.

7.2 Competence

The organization shall:

a) determine the necessary competence of person(s) doing work under its control that affects its information security performance;

b) ensure that these persons are competent on the basis of appropriate education, training, or experience;

c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and

d) retain appropriate documented information as evidence of competence.

NOTE Applicable actions can include, for example: the provision of training to, the mentoring of, or the

Tổ chức phải lưu giữ thông tin được lập văn bản các mục tiêu an toàn thông tin.

Khi lập kế hoạch để đạt được các mục tiêu an toàn thông tin, tổ chức phải xác định:

h) những gì sẽ được thực hiện;

i) những nguồn lực sẽ được yêu cầu;

j) người sẽ chịu trách nhiệm;

k) khi nào sẽ được hoàn thành, và

l) kết quả sẽ được đo lường như thế nào

6.3 Hoạch định các thay đổi

Khi tổ chức xác định sự cần thiết phải thay đổi đối với hệ thống quản lý an toàn thông tin, thì các thay đổi này phải được thực hiện một cách có kế hoạch.

7. Hỗ trợ

7.1 Nguồn lực

Tổ chức phải xác định và cung cấp các nguồn lực cần thiết cho việc thiết lập, áp dụng, duy trì và cải tiến liên tục hệ thống quản lý an toàn thông tin.

7.2 Năng lực

Tổ chức phải:

a) xác định năng lực cần thiết của (những) người đang làm công việc mà dưới sự quản lý của họ có ảnh hưởng đến hoạt động an toàn thông tin;

b) đảm bảo rằng những người đó có đủ năng lực dựa trên cơ sở được giáo dục, đào tạo, hoặc kinh nghiệm;

c) khi thích hợp, tiến hành các hành động để có được các năng lực cần thiết, và đánh giá hiệu lực của các hành động đã thực hiện; và

d) lưu giữ thông tin được lập văn bản thích hợp như bằng chứng về năng lực.

CHÚ THÍCH: Áp dụng các hành động có thể bao gồm, ví dụ: cung cấp các khóa đào tạo, các cố vấn, hoặc phân công lại vai trò của người lao động hiện

Tài liệu phục vụ Đào tạo, nghiên cứu

Bản Dịch nhằm phục vụ Đào tạo và phổ biến Kiến thức, Khi áp dụng Cá nhân, Tổ chức phải tuân thủ nguyên tắc Bản Quyền và mua chính tức Tiêu chuẩn. (contact: Lê Xuân Trường 0868688767 / 0903452826)

re-assignment of current employees; or the hiring or contracting of competent persons.

hành; hoặc tuyển dụng hoặc ký hợp đồng với người đủ năng lực.

7.3 Awareness

7.3 Nhận thức

Persons doing work under the organization's control shall be aware of:

Người làm công việc dưới sự quản lý của tổ chức phải có nhận thức về:

a) the information security policy;

a) chính sách an toàn thông tin;

b) their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and

b) việc đóng góp của họ vào hiệu lực của hệ thống quản lý an toàn thông tin, bao gồm cả các lợi ích của sự cải tiến hoạt động thực hiện an toàn thông tin; và

c) the implications of not conforming with the information security management system requirements.

c) những hệ quả của việc không thực hiện phù hợp với các yêu cầu của hệ thống quản lý an toàn thông tin.

7.4 Communication

7.4 Trao đổi thông tin

The organization shall determine the need for internal and external communications relevant to the information security management system including:

Tổ chức phải xác định nhu cầu trao đổi thông tin nội bộ và bên ngoài có liên quan đến hệ thống quản lý an toàn thông tin bao gồm:

a) on what to communicate;

a) trao đổi thông tin gì;

b) when to communicate;

b) trao đổi thông tin khi nào;

c) with whom to communicate;

c) trao đổi thông tin với ai;

d) how to communicate.

d) cách thức trao đổi thông tin.

7.5 Documented information

7.5 Thông tin được lập văn bản

7.5.1 General

7.5.1 Khái quát

The organization's information security management system shall include:

Hệ thống quản lý an toàn thông tin của tổ chức phải bao gồm:

a) documented information required by this document; and

a) thông tin được lập văn bản theo yêu cầu của tài liệu này, và

b) documented information determined by the organization as being necessary for the effectiveness of the information security management system.

b) thông tin được lập văn bản được xác định bởi tổ chức như là sự cần thiết cho tính hiệu lực của hệ thống quản lý an toàn thông tin.

NOTE The extent of documented information for an information security management system can differ from one organization to another due to:

CHÚ THÍCH: Mức độ thông tin được lập văn bản cho một hệ thống quản lý an toàn thông tin có thể khác nhau giữa các tổ chức phụ thuộc vào:

1) the size of organization and its type of activities, processes, products and services;

1) quy mô của tổ chức và loại hình hoạt động, quy trình, sản phẩm và dịch vụ của tổ chức;

2) the complexity of processes and their interactions; and

2) sự phức tạp và sự tương tác của các quá trình; và

Tài liệu phục vụ Đào tạo nghiên cứu

Bản Dịch nhằm phục vụ Đào tạo và phổ biến Kiến thức, Khi áp dụng Cá nhân, Tổ chức phải tuân thủ nguyên tắc Bản Quyền và mua chính tức Tiêu chuẩn. (contact: Lê Xuân Trường 0868688767 / 0903452826)

3) the competence of persons.

7.5.2 Creating and updating

When creating and updating documented information the organization shall ensure appropriate:

a) identification and description (e.g. a title, date, author, or reference number);

b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and

c) review and approval for suitability and adequacy.

7.5.3 Control of documented information

Documented information required by the information security management system and by this document shall be controlled to ensure:

a) it is available and suitable for use, where and when it is needed; and

b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

For the control of documented information, the organization shall address the following activities, as applicable:

c) distribution, access, retrieval and use;

d) storage and preservation, including the preservation of legibility;

e) control of changes (e.g. version control); and

f) retention and disposition.

Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled.

NOTE Access can imply a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information, etc.

3) năng lực của con người.

7.5.2 Khởi tạo và cập nhật

Khi khởi tạo và cập nhật thông tin được lập văn bản tổ chức phải đảm bảo thích hợp:

a) định danh và mô tả (ví dụ như tiêu đề, ngày tháng, tác giả, hoặc mã số tài liệu);

b) định dạng (ví dụ như ngôn ngữ, phiên bản phần mềm, đồ họa) và phương tiện (ví dụ như giấy, điện tử); và

c) xem xét và phê duyệt cho thích hợp và thỏa đáng.

7.5.3 Quản lý thông tin được lập văn bản

Thông tin được lập văn bản theo yêu cầu của hệ thống quản lý an toàn thông tin và tài liệu này phải được kiểm soát để đảm bảo:

a) sẵn có và phù hợp để sử dụng bất kỳ ở đâu và khi nào cần thiết; và

b) được bảo vệ đầy đủ (ví dụ bảo vệ khỏi mất tính bảo mật, sử dụng không đúng cách, hoặc mất tính toàn vẹn).

Đối với việc kiểm soát thông tin được lập văn bản, tổ chức phải quan tâm đến các hoạt động sau đây, có thể áp dụng:

c) phân phối, truy cập, thu hồi và sử dụng;

d) lưu trữ và bảo quản, bao gồm cả việc duy trì tính rõ ràng;

e) kiểm soát các thay đổi (ví dụ như kiểm soát phiên bản); và

f) duy trì và hủy bỏ.

Thông tin lập văn bản có nguồn gốc bên ngoài mà tổ chức xác định là cần thiết cho việc hoạch định và vận hành hệ thống quản lý an toàn thông tin, phải được nhận biết thích hợp, và được kiểm soát.

CHÚ THÍCH: Thuật ngữ Truy cập bao hàm ý nghĩa một quyết định liên quan đến việc cho phép chỉ xem thông tin được lập văn bản, hoặc sự cho phép và thẩm quyền để xem và thay đổi thông tin được lập văn bản, vv

Tài liệu phục vụ Đào tạo, nghiên cứu

Bản Dịch nhằm phục vụ Đào tạo và phổ biến Kiến thức, Khi áp dụng Cá nhân, Tổ chức phải tuân thủ nguyên tắc Bản Quyền và mua chính tức Tiêu chuẩn. (contact: Lê Xuân Trường 0868688767 / 0903452826)

8 Operation

8.1 Operational planning and control

The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in Clause 6, by:

— establishing criteria for the processes;

— implementing control of the processes in accordance with the criteria.

Documented information shall be available to the extent necessary to have confidence that the processes have been carried out as planned.

The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization shall ensure that externally provided processes, products or services that are relevant to the information security management system are controlled.

8.2 Information security risk assessment

The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2 a).

The organization shall retain documented information of the results of the information security risk assessments.

8.3 Information security risk treatment

The organization shall implement the information security risk treatment plan.

The organization shall retain documented information of the results of the information security risk treatment.

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

The organization shall determine:

8. Điều hành

8.1 Hoạch định và kiểm soát hoạt động

Tổ chức phải lập kế hoạch, thực hiện và kiểm soát các quy trình cần thiết để đáp ứng yêu cầu an toàn thông tin, và triển khai các hoạt động đã xác định trong Điều 6, thông qua:

- thiết lập các tiêu chí cho các quá trình;

- thực hiện kiểm soát các quá trình phù hợp với các tiêu chí.

Thông tin dạng văn bản sẽ sẵn có ở mức độ cần thiết để đảm bảo tin cậy rằng các quá trình đã được tiến hành theo kế hoạch.

Tổ chức phải kiểm soát các thay đổi kế hoạch và xem xét các hậu quả của sự thay đổi ngoài ý muốn, có hành động để giảm thiểu bất kỳ tác dụng phụ nào, khi cần thiết.

Tổ chức phải đảm bảo rằng các quá trình, sản phẩm hoặc dịch vụ được cung cấp bởi bên ngoài có liên quan đến hệ thống quản lý an toàn thông tin được kiểm soát.

8.2 Đánh giá rủi ro an toàn thông tin

Tổ chức phải thực hiện đánh giá rủi ro an toàn thông tin trong khoảng thời gian theo kế hoạch hoặc khi có những thay đổi quan trọng theo dự kiến hoặc đã xảy ra, có tính đến các tiêu chí thiết lập trong 6.1.2 a).

Tổ chức có trách nhiệm lưu giữ thông tin được lập văn bản các kết quả của đánh giá rủi ro an toàn thông tin.

8.3 Xử lý rủi ro an toàn thông tin

Tổ chức phải triển khai kế hoạch xử lý rủi ro an toàn thông tin.

Tổ chức phải lưu giữ thông tin được lập văn bản các kết quả của các quá trình xử lý rủi ro an toàn thông tin.

9. Đánh giá hiệu quả

9.1 Giám sát, đo lường, phân tích và đánh giá

Tổ chức phải xác định:

Tài liệu phục vụ Đào tạo, nghiên cứu

Bản Dịch nhằm phục vụ Đào tạo và phổ biến Kiến thức, Khi áp dụng Cá nhân, Tổ chức phải tuân thủ nguyên tắc Bản Quyền và mua chính tức Tiêu chuẩn. (contact: Lê Xuân Trường 0868688767 / 0903452826)

a) what needs to be monitored and measured, including information security processes and controls;

b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results. The methods selected should produce comparable and reproducible results to be considered valid;

c) when the monitoring and measuring shall be performed;

d) who shall monitor and measure;

e) when the results from monitoring and measurement shall be analysed and evaluated;

f) who shall analyse and evaluate these results.

Documented information shall be available as evidence of the results.

The organization shall evaluate the information security performance and the effectiveness of the information security management system.

9.2 Internal audit

9.2.1 General

The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system:

a) conforms to

1) the organization's own requirements for its information security management system;

2) the requirements of this document;

b) is effectively implemented and maintained.

9.2.2 Internal audit programme

The organization shall plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting.

When establishing the internal audit programme(s), the organization shall consider the importance of the processes concerned and the results of previous audits.

a) những gì cần phải được giám sát và đo lường, bao gồm các quá trình và các biện pháp kiểm soát an toàn thông tin;

b) các phương pháp giám sát, đo lường, phân tích và đánh giá, nếu có, để đảm bảo kết quả hợp lệ; Các phương pháp được lựa chọn cần tạo ra kết quả có thể so sánh được và có thể tái sử dụng, được coi là hợp lệ.

c) khi nào hoạt động giám sát và đo lường được thực hiện;

d) ai phải thực hiện giám sát và đo lường;

e) khi nào các kết quả từ giám sát và đo lường được phân tích và đánh giá; và

f) ai phải phân tích và đánh giá các kết quả này.

Thông tin dạng văn bản phải sẵn có làm bằng chứng về kết quả giám sát và đo lường.

Tổ chức phải đánh giá việc thực hiện an toàn thông tin và tính hiệu lực của hệ thống quản lý an toàn thông tin.

9.2 Đánh giá nội bộ

9.2.1 Khái quát

Tổ chức phải tiến hành các hoạt động đánh giá nội bộ định kỳ theo kế hoạch để cung cấp thông tin xem hệ thống ISMS có:

a) phù hợp với

1) Các yêu cầu của chính tổ chức đối với hệ thống quản lý an toàn thông tin của mình,

2) các yêu cầu của tài liệu này;

b) được thực hiện và duy trì có hiệu lực.

9.2.2 Chương trình đánh giá nội bộ

Tổ chức phải lập kế hoạch, thiết lập, triển khai và duy trì một hoặc nhiều chương trình đánh giá, bao gồm tần suất, phương pháp, trách nhiệm, yêu cầu lập kế hoạch và báo cáo.

Khi lập một hoặc nhiều chương trình đánh giá nội bộ, tổ chức phải xem xét tầm quan trọng của các quy trình liên quan và kết quả của các cuộ đánh giá trước đó.

Tài liệu phục vụ Đào tạo, nghiên cứu

Bản Dịch nhằm phục vụ Đào tạo và phổ biến Kiến thức, Khi áp dụng Cá nhân, Tổ chức phải tuân thủ nguyên tắc Bản Quyền và mua chính tức Tiêu chuẩn. (contact: Lê Xuân Trường 0868688767 / 0903452826)

The organization shall:

a) define the audit criteria and scope for each audit;

b) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;

c) ensure that the results of the audits are reported to relevant management;

Documented information shall be available as evidence of the implementation of the audit programme(s) and the audit results.

9.3 Management review

9.3.1 General

Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

9.3.2 Management review inputs

The management review shall include consideration of:

a) the status of actions from previous management reviews;

b) changes in external and internal issues that are relevant to the information security management system;

c) changes in needs and expectations of interested parties that are relevant to the information security management system;

d) feedback on the information security performance, including trends in:

1) nonconformities and corrective actions;

2) monitoring and measurement results;

3) audit results;

4) fulfilment of information security objectives;

e) feedback from interested parties;

Tổ chức phải:

a) xác định tiêu chí đánh giá và phạm vi cho mỗi cuộc đánh giá;

b) lựa chọn các đánh giá viên và thực hiện các cuộc đánh giá đảm bảo tính khách quan và công bằng của quy trình đánh giá;

c) đảm bảo rằng kết quả của các cuộc đánh giá được báo cáo đến cấp quản lý có liên quan;

Thông tin được lập văn bản phải có sẵn làm bằng chứng về việc thực hiện (các) chương trình đánh giá và các kết quả đánh giá.

9.3 Xem xét của lãnh đạo

9.3.1 Khái quát

Lãnh đạo cao nhất phải xem xét định kỳ theo kế hoạch hệ thống ISMS của tổ chức để đảm bảo nó luôn phù hợp, thoả đáng và có hiệu lực.

9.3.2 Đầu vào xem xét của lãnh đạo

Việc xem xét của lãnh đạo phải bao gồm sự xem xét:

a) tình trạng của các hành động từ lần xem xét lãnh đạo trước đó;

b) các thay đổi trong các vấn đề bên ngoài và nội bộ có liên quan đến hệ thống quản lý an toàn thông tin;

c) những thay đổi về nhu cầu và mong đợi của các bên quan tâm có liên quan đến hệ thống quản lý an toàn thông tin;

d) phản hồi về việc thực hiện an toàn thông tin, bao gồm:

1) các sự không phù hợp và các hành động khắc phục;

2) các kết quả giám sát và đo lường;

3) các kết quả đánh giá; và

4) sự đáp ứng các mục tiêu an toàn thông tin;

e) thông tin phản hồi từ các bên quan tâm;

Tài liệu phục vụ Đào tạo nghiên cứu

Bản Dịch nhằm phục vụ Đào tạo và phổ biến Kiến thức, Khi áp dụng Cá nhân, Tổ chức phải tuân thủ nguyên tắc Bản Quyền và mua chính tức Tiêu chuẩn. (contact: Lê Xuân Trường 0868688767 / 0903452826)

f) results of risk assessment and status of risk treatment plan;

g) opportunities for continual improvement.

9.3.3 Management review results

The results of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system.

Documented information shall be available as evidence of the results of management reviews.

10 Improvement

10.1 Continual improvement

The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.

10.2 Nonconformity and corrective action

When a nonconformity occurs, the organization shall:

a) react to the nonconformity, and as applicable:

1) take action to control and correct it;

2) deal with the consequences;

b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by:

1) reviewing the nonconformity;

2) determining the causes of the nonconformity; and

3) determining if similar nonconformities exist, or could potentially occur;

c) implement any action needed;

d) review the effectiveness of any corrective action taken; and

e) make changes to the information security management system, if necessary.

f) kết quả đánh giá rủi ro và tình trạng của kế hoạch xử lý rủi ro; và

g) các cơ hội cải tiến liên tục

9.3.3 Kết quả xem xét của lãnh đạo

Kết quả xem xét của lãnh đạo phải bao gồm những quyết định liên quan đến các cơ hội cải tiến liên tục và bất cứ nhu cầu cần thiết nào cho các thay đổi đối với hệ thống quản lý an toàn thông tin.

Thông tin được lập văn bản phải sẵn có làm bằng chứng về kết quả của các cuộc xem xét của lãnh đạo.

10. Cải tiến

10.1 Cải tiến liên tục

Tổ chức phải liên tục cải tiến nâng cao tính thích hợp, đầy đủ và hiệu lực của hệ thống quản lý an toàn thông tin.

10.2 Sự không phù hợp và hành động khắc phục

Khi xảy ra sự không phù hợp, tổ chức phải:

a) phản ứng với sự không phù hợp, và có thể áp dụng:

1) Thực hiện hành động để kiểm soát và khắc phục sự không phù hợp đó;

2) Giải quyết các hậu quả;

b) Đánh giá sự cần thiết phải hành động để loại bỏ nguyên nhân của sự không phù hợp, để nó không tái diễn hoặc xảy ra ở nơi khác, bằng cách:

1) xem xét sự không phù hợp;

2) xác định nguyên nhân gây ra sự không phù hợp; và

3) xác định nếu có sự không phù hợp tương tự tồn tại, hoặc có khả năng có thể xảy ra hay không;

c) thực hiện bất kỳ hành động cần thiết nào;

d) xem xét hiệu lực của bất kỳ hành động khắc phục đã thực hiện; và

e) thay đổi hệ thống quản lý an toàn thông tin, nếu cần thiết.

Tài liệu phục vụ Đào tạo, nghiên cứu

Bản Dịch nhằm phục vụ Đào tạo và phổ biến Kiến thức, Khi áp dụng Cá nhân, Tổ chức phải tuân thủ nguyên tắc Bản Quyền và mua chính tức Tiêu chuẩn. (contact: Lê Xuân Trường 0868688767 / 0903452826)

Corrective actions shall be appropriate to the effects of the nonconformities encountered. Documented information shall be available as evidence of:

f) the nature of the nonconformities and any subsequent actions taken,

g) the results of any corrective action.

Các hành động khắc phục phải phù hợp với tác động của sự không phù hợp gặp phải. Thông tin được lập văn bản phải sẵn có làm bằng chứng về:

f) bản chất của sự không phù hợp và bất kỳ hành động tiếp theo nào được thực hiện, và

g) kết quả của các hành động khắc phục.

Tài liệu phục vụ Đào tạo, nghiên cứu

Bản Dịch nhằm phục vụ Đào tạo và phổ biến Kiến thức, Khi áp dụng Cá nhân, Tổ chức phải tuân thủ nguyên tắc Bản Quyền và mua chính tức Tiêu chuẩn. (contact: Lê Xuân Trường 0868688767 / 0903452826)

Annex A (normative) **Information security controls reference**	**Phụ lục A** (quy định) **Các biện pháp kiểm soát an toàn thông tin tham khảo**
The information security controls listed in Table A.1 are directly derived from and aligned with those listed in ISO/IEC 27002:2022[1], Clauses 5 to 8, and shall be used in context with 6.1.3.	Các biện pháp kiểm soát an toàn thông tin được liệt kê trong bảng A.1 bắt nguồn trực tiếp và có liên kết với các mục từ mục 5 đến 8 được liệt kê trong ISO/IEC27002:2022 và phải được sử dụng trong bối cảnh của điều khoản 6.1.3.
Table A.1 — Information security controls	**Bảng A.1- Các biện pháp kiểm soát an toàn thông tin**

A.5. Các biện pháp kiểm soát về tổ chức - (Organizational controls)

5.1 Chính sách an toàn thông tin

Kiểm soát:

Chính sách an toàn thông tin và các chính sách chuyên đề liên quan phải được xây dựng, phê duyệt bởi lãnh đạo, công bố, truyền thông đến và được xác nhận bởi các nhân sự liên quan và các bên quan tâm, đồng thời được xem xét định kỳ hoặc khi có thay đổi lớn.

5.2 Vai trò và trách nhiệm an toàn thông tin

Kiểm soát:

Phải xác định và phân công rõ ràng các vai trò, trách nhiệm liên quan đến an toàn thông tin phù hợp với nhu cầu của tổ chức.

5.3 Phân tách nhiệm vụ

Kiểm soát:

Các nhiệm vụ và quyền hạn xung đột phải được phân tách rõ ràng để giảm thiểu rủi ro lạm dụng quyền lực hoặc sai sót.

5.4 Trách nhiệm của lãnh đạo

Kiểm soát:

Lãnh đạo phải yêu cầu mọi nhân viên tuân thủ các chính sách và quy trình an toàn thông tin đã ban hành.

5.5 Thiết lập và duy trì liên lạc với các cơ quan chức năng

Kiểm soát:

Phải thiết lập và duy trì liên hệ với các cơ quan chức năng có liên quan.

Bản Dịch nhằm phục vụ Đào tạo và phổ biến Kiến thức, Khi áp dụng Cá nhân, Tổ chức phải tuân thủ nguyên tắc Bản Quyền và mua chính tức Tiêu chuẩn. (contact: Lê Xuân Trường 0868688767 / 0903452826)

Tài liệu phục vụ Đào tạo, nghiên cứu

5.6 Liên hệ với các nhóm chuyên gia

Kiểm soát:

Phải thiết lập và duy trì liên hệ với các nhóm chuyên môn, diễn đàn hoặc hiệp hội an ninh.

5.7 Cập nhật thông tin tình báo về các mối đe dọa

Kiểm soát:

Phải thu thập và phân tích thông tin liên quan đến các mối đe dọa an toàn thông tin để tạo lập cơ sở dữ liệu tình báo mối đe dọa.

5.8 An toàn thông tin trong quản lý dự án

Kiểm soát:

An toàn thông tin phải được tích hợp vào các hoạt động quản lý dự án.

5.9 Kiểm kê thông tin và tài sản liên quan khác

Kiểm soát:

Phải phát triển và duy trì một danh mục tài sản thông tin và tài sản liên quan, bao gồm cả việc xác định chủ sở hữu tài sản.

5.10 Việc sử dụng thông tin và các tài sản liên quan khác được chấp nhận (Quy định sử dụng tài sản)

Kiểm soát:

Phải xây dựng quy định và quy trình sử dụng tài sản thông tin một cách phù hợp và được áp dụng thống nhất.

Các quy tắc về việc sử dụng và các thủ tục được chấp nhận để xử lý thông tin và các tài sản liên quan khác phải được xác định, ghi chép và triển khai.

5.11 Hoàn trả tài sản

Kiểm soát:

Nhân sự và các bên liên quan khác khi thích hợp phải trả lại tất cả tài sản của tổ chức mà họ đang sở hữu khi thay đổi hoặc chấm dứt việc làm, hợp đồng hoặc nhiệm vụ của họ.

5.12 Phân loại thông tin

Kiểm soát:

Thông tin sẽ được phân loại theo nhu cầu bảo mật thông tin của tổ chức dựa trên tính bảo mật, tính toàn vẹn, tính khả dụng và các yêu cầu của các bên có liên quan.

Tài liệu phục vụ Đào tạo, nghiên cứu

Bản Dịch nhằm phục vụ Đào tạo và phổ biến Kiến thức, Khi áp dụng Cá nhân, Tổ chức phải tuân thủ nguyên tắc Bản Quyền và mua chính tức Tiêu chuẩn. (contact: Lê Xuân Trường 0868688767 / 0903452826)

5.13 Nhãn thông tin

Kiểm soát:

Phải xây dựng và áp dụng một bộ quy trình dán nhãn thông tin phù hợp với hệ thống phân loại thông tin đã thiết lập.

5.14 Chuyển giao thông tin

Kiểm soát:

Phải có các quy tắc, quy trình hoặc thỏa thuận về việc chuyển giao thông tin cho các bên trong và ngoài tổ chức, đảm bảo an toàn thông tin khi di chuyển.

5.15 Kiểm soát truy cập

Kiểm soát:

Phải xây dựng và áp dụng các quy tắc kiểm soát truy cập vật lý và truy cập hệ thống thông tin dựa trên yêu cầu kinh doanh và an toàn thông tin.

5.16 Quản lý danh tính

Kiểm soát:

Chu kỳ sống của danh tính người dùng (tạo lập, thay đổi, vô hiệu hóa) phải được quản lý chặt chẽ.

5.17 Quản lý thông tin xác thực

Kiểm soát:

Phải kiểm soát việc cấp phát và quản lý thông tin xác thực (ví dụ: mật khẩu, thẻ truy cập), bao gồm hướng dẫn người dùng sử dụng và bảo vệ thông tin xác thực.

5.18 Quyền truy cập

Kiểm soát:

Phải cung cấp, rà soát, điều chỉnh hoặc thu hồi quyền truy cập vào thông tin và tài sản liên quan, phù hợp với chính sách kiểm soát truy cập của tổ chức.

5.19 An toàn thông tin trong quan hệ nhà cung cấp

Kiểm soát:

Phải xây dựng quy trình quản lý rủi ro an toàn thông tin liên quan đến sản phẩm hoặc dịch vụ từ nhà cung cấp.

Tài liệu phục vụ Đào tạo, nghiên cứu

Bản Dịch nhằm phục vụ Đào tạo và phổ biến Kiến thức, Khi áp dụng Cá nhân, Tổ chức phải tuân thủ nguyên tắc Bản Quyền và mua chính tức Tiêu chuẩn. (contact: Lê Xuân Trường 0868688767 / 0903452826)

5.20 Đưa yêu cầu an toàn thông tin vào thỏa thuận với nhà cung cấp

Kiểm soát:

Các yêu cầu về an toàn thông tin phải được thiết lập và đưa vào hợp đồng với nhà cung cấp, tùy theo loại hình dịch vụ.

5.21 Quản lý an toàn thông tin trong chuỗi cung ứng CNTT

Kiểm soát:

Phải có quy trình và biện pháp quản lý rủi ro an toàn thông tin trong chuỗi cung ứng sản phẩm, dịch vụ CNTT.

5.22 Giám sát, xem xét và quản lý thay đổi các dịch vụ của nhà cung cấp

Kiểm soát:

Tổ chức cần thường xuyên giám sát, rà soát và quản lý các thay đổi về dịch vụ hoặc hoạt động an toàn thông tin của nhà cung cấp.

5.23 An toàn thông tin khi sử dụng các dịch vụ đám mây

Kiểm soát:

Phải xây dựng quy trình về việc lựa chọn, sử dụng, quản lý và chấm dứt sử dụng dịch vụ điện toán đám mây, phù hợp với yêu cầu an toàn thông tin.

5.24 Lập kế hoạch và chuẩn bị ứng phó sự cố an toàn thông tin

Kiểm soát:

Phải xác định, thiết lập và truyền thông quy trình quản lý sự cố an toàn thông tin, bao gồm vai trò, trách nhiệm rõ ràng.

5.25 Đánh giá và quyết định các sự kiện an toàn thông tin

Kiểm soát:

Tổ chức phải đánh giá các sự kiện an toàn thông tin và quyết định xem có phân loại các sự kiện này là sự cố an toàn thông tin hay không.

5.26 Ứng phó với sự cố an toàn thông tin

Kiểm soát:

Các sự cố an toàn thông tin phải được phản ứng và xử lý theo quy trình đã được tổ chức lập và phê duyệt.

Tài liệu phục vụ Đào tạo, nghiên cứu

Bản Dịch nhằm phục vụ Đào tạo và phổ biến Kiến thức, Khi áp dụng Cá nhân, Tổ chức phải tuân thủ nguyên tắc Bản Quyền và mua chính tức Tiêu chuẩn. (contact: Lê Xuân Trường 0868688767 / 0903452826)

5.27 Rút kinh nghiệm từ các sự cố an toàn thông tin

Kiểm soát:

Tổ chức cần tận dụng kiến thức thu được từ các sự cố an toàn thông tin để củng cố và cải thiện các biện pháp kiểm soát an toàn thông tin.

5.28 Thu thập bằng chứng

Kiểm soát:

Phải xây dựng và thực hiện quy trình để nhận diện, thu thập, tiếp nhận và lưu trữ bằng chứng liên quan đến sự kiện an toàn thông tin.

5.29 An toàn thông tin trong thời gian gián đoạn

Kiểm soát:

Tổ chức phải lập kế hoạch đảm bảo mức độ an toàn thông tin phù hợp trong trường hợp xảy ra gián đoạn hoạt động.

5.30 Sự sẵn sàng của CNTT cho hoạt động kinh doanh liên tục

Kiểm soát:

Tổ chức phải lập kế hoạch, triển khai, duy trì và kiểm tra khả năng sẵn sàng của hệ thống CNTT nhằm đáp ứng các mục tiêu và yêu cầu về liên tục kinh doanh.

5.31 Các yêu cầu pháp lý, luật định, quy định và hợp đồng

Kiểm soát:

Phải xác định, lập tài liệu và cập nhật các yêu cầu pháp luật, quy định và hợp đồng có liên quan đến an toàn thông tin.

5.32 Quyền sở hữu trí tuệ

Kiểm soát:

Tổ chức cần triển khai các biện pháp phù hợp để bảo vệ quyền sở hữu trí tuệ.

5.33 Bảo vệ hồ sơ

Kiểm soát:

Hồ sơ cần được bảo vệ khỏi nguy cơ mất mát, hủy hoại, làm giả, truy cập trái phép hoặc tiết lộ không được phép.

Tài liệu phục vụ Đào tạo, nghiên cứu

Bản Dịch nhằm phục vụ Đào tạo và phổ biến Kiến thức, Khi áp dụng Cá nhân, Tổ chức phải tuân thủ nguyên tắc Bản Quyền và mua chính tức Tiêu chuẩn. (contact: Lê Xuân Trường 0868688767 / 0903452826)

5.34 Bảo vệ dữ liệu cá nhân (PII) và quyền riêng tư

Kiểm soát:

Tổ chức cần nhận diện và đáp ứng yêu cầu pháp luật, quy định và hợp đồng liên quan đến việc bảo vệ quyền riêng tư và dữ liệu cá nhân nhận dạng được (PII).

5.35 Đánh giá độc lập về an toàn thông tin

Kiểm soát:

Việc quản lý và vận hành an toàn thông tin, bao gồm con người, quy trình và công nghệ, phải được đánh giá độc lập theo kế hoạch hoặc khi có thay đổi lớn.

5.36 Tuân thủ chính sách, quy tắc và tiêu chuẩn an toàn thông tin

Kiểm soát:

Tổ chức cần định kỳ rà soát việc tuân thủ các chính sách, quy định, quy trình và tiêu chuẩn an toàn thông tin.

5.37 Quy trình vận hành được lập thành văn bản

Kiểm soát:

Các quy trình vận hành cho cơ sở xử lý thông tin phải được lập thành văn bản và cung cấp cho những nhân sự cần thiết.

A.6. Các biện pháp kiểm soát về con người (People Controls)

6.1 Sàng lọc (Screening)

Kiểm soát:

Phải tiến hành kiểm tra lý lịch đối với tất cả ứng viên trước khi họ chính thức trở thành nhân viên, và tiếp tục thực hiện định kỳ (nếu phù hợp), dựa trên yêu cầu công việc, mức độ nhạy cảm của thông tin họ có quyền truy cập, cũng như các yêu cầu pháp luật, quy định và đạo đức áp dụng.

6.2 Điều khoản và điều kiện làm việc

Kiểm soát:

Các thỏa thuận lao động (ví dụ: hợp đồng lao động) phải nêu rõ trách nhiệm của nhân viên và của tổ chức đối với việc bảo đảm an toàn thông tin.

Tài liệu phục vụ Đào tạo, nghiên cứu

Bản Dịch nhằm phục vụ Đào tạo và phổ biến Kiến thức, Khi áp dụng Cá nhân, Tổ chức phải tuân thủ nguyên tắc Bản Quyền và mua chính tức Tiêu chuẩn. (contact: Lê Xuân Trường 0868688767 / 0903452826)

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

Kiểm soát:

Nhân sự của tổ chức và các bên liên quan có liên quan phải được đào tạo, cập nhật thường xuyên về nhận thức, chính sách, và quy trình an toàn thông tin phù hợp với chức năng công việc của họ.

6.4 Quy trình xử lý kỷ luật

Kiểm soát:

Phải xây dựng và truyền thông một quy trình xử lý kỷ luật nhằm xử lý các trường hợp nhân viên hoặc bên liên quan vi phạm chính sách an toàn thông tin.

6.5 Trách nhiệm sau khi thôi việc hoặc thay đổi công việc

Kiểm soát:

Các trách nhiệm và nghĩa vụ về an toàn thông tin còn hiệu lực sau khi kết thúc hoặc thay đổi hợp đồng lao động phải được xác định rõ ràng, thực thi và truyền thông tới những đối tượng liên quan.

6.6 Thỏa thuận bảo mật hoặc cam kết không tiết lộ thông tin

Kiểm soát:

Phải xác định, lập tài liệu, rà soát định kỳ và yêu cầu nhân sự cũng như các bên liên quan ký thỏa thuận bảo mật hoặc cam kết không tiết lộ thông tin, phù hợp với yêu cầu bảo vệ thông tin của tổ chức.

6.7 Làm việc từ xa (Remote Working)

Kiểm soát:

Các biện pháp an toàn thông tin phải được triển khai đối với nhân sự làm việc từ xa nhằm bảo vệ thông tin được truy cập, xử lý hoặc lưu trữ bên ngoài của tổ chức.

6.8 Báo cáo sự kiện an toàn thông tin

Kiểm soát:

Tổ chức phải cung cấp cơ chế cho phép nhân viên và các bên liên quan báo cáo kịp thời những sự kiện hoặc nghi ngờ sự kiện liên quan đến an toàn thông tin thông qua các kênh thích hợp.

A.7 Physical controls – Các biện pháp kiểm soát về vật lý

7.1 Các vành đai an ninh vật lý (Physical Security Perimeters)

Kiểm soát:

Tài liệu phục vụ Đào tạo, nghiên cứu

Phải xác định và sử dụng các ranh giới an ninh để bảo vệ các khu vực chứa thông tin và các tài sản liên quan. Các ranh giới này cần được thiết kế để ngăn chặn truy cập trái phép.

7.2 Cổng ra vào vật lý (Physical Entry)

Kiểm soát:

Các khu vực an toàn phải được bảo vệ bằng các biện pháp kiểm soát ra vào phù hợp, đảm bảo chỉ những người được phép mới có quyền truy cập.

7.3 Bảo vệ văn phòng, phòng và cơ sở vật chất (Securing Offices, Rooms and Facilities)

Kiểm soát:

Các văn phòng, phòng và cơ sở xử lý thông tin phải được thiết kế và triển khai các biện pháp bảo vệ vật lý thích hợp.

7.4 Giám sát an ninh vật lý (Physical Security Monitoring)

Kiểm soát:

Phải thực hiện giám sát liên tục các khu vực để phát hiện và ngăn chặn việc truy cập vật lý trái phép.

7.5 Bảo vệ chống lại các mối đe dọa vật lý và môi trường (Protecting Against Physical and Environmental Threats)

Kiểm soát:

Phải thiết kế và triển khai các biện pháp để bảo vệ cơ sở vật chất khỏi các mối đe dọa vật lý và môi trường, bao gồm thiên tai, hỏa hoạn, lũ lụt và các hành vi phá hoại.

7.6 Làm việc trong khu vực an toàn (Working in Secure Areas)

Kiểm soát:

Phải áp dụng các biện pháp an toàn phù hợp cho những người làm việc trong các khu vực an toàn, bao gồm kiểm soát hành vi và sử dụng thiết bị.

7.7 Quy tắc bàn làm việc sạch và màn hình sạch (Clear Desk and Clear Screen)

Kiểm soát:

Phải xác lập và thực thi quy tắc "bàn làm việc sạch" đối với tài liệu giấy và thiết bị lưu trữ di động, và "màn hình sạch" đối với các thiết bị xử lý thông tin, nhằm giảm nguy cơ truy cập trái phép.

7.8 Bố trí và bảo vệ thiết bị (Equipment Siting and Protection)

Kiểm soát:

Bản Dịch nhằm phục vụ Đào tạo và phổ biến Kiến thức, Khi áp dụng Cá nhân, Tổ chức phải tuân thủ nguyên tắc Bản Quyền và mua chính tức Tiêu chuẩn. (contact: Lê Xuân Trường 0868688767 / 0903452826)

Tài liệu phục vụ Đào tạo, nghiên cứu

Thiết bị phải được bố trí ở những vị trí an toàn, được bảo vệ nhằm giảm thiểu nguy cơ thiệt hại, truy cập trái phép hoặc gây gián đoạn hoạt động.

7.9 An toàn tài sản bên ngoài trụ sở (Security of Assets Off-Premises)

Kiểm soát:

Các tài sản được mang ra ngoài cơ sở tổ chức phải được bảo vệ thích hợp để đảm bảo an toàn thông tin.

7.10 Phương tiện lưu trữ (Storage Media)

Kiểm soát:

Phương tiện lưu trữ phải được quản lý trong toàn bộ vòng đời của chúng (từ tiếp nhận, sử dụng, vận chuyển cho đến tiêu hủy) phù hợp với chính sách phân loại và xử lý thông tin của tổ chức.

7.11 Các tiện ích hỗ trợ (Supporting Utilities)

Kiểm soát:

Các qua trình xử lý thông tin phải được bảo vệ trước sự cố về nguồn điện hoặc các dịch vụ tiện ích khác gây gián đoạn hoạt động.

7.12 An toàn cáp truyền dẫn (Cabling Security)

Kiểm soát:

Cáp điện, cáp dữ liệu hoặc các cáp hỗ trợ dịch vụ thông tin phải được bảo vệ khỏi nguy cơ nghe trộm, can thiệp hoặc hư hỏng.

7.13 Bảo trì thiết bị (Equipment Maintenance)

Kiểm soát:

Thiết bị phải được bảo trì đúng cách nhằm đảm bảo tính sẵn sàng, toàn vẹn và bảo mật của thông tin.

7.14 Xử lý hoặc tái sử dụng thiết bị an toàn (Secure Disposal or Reuse of Equipment)

Kiểm soát:

Trước khi Xử lý/tiêu hủy hoặc tái sử dụng thiết bị chứa phương tiện lưu trữ, phải được xác minh đảm bảo mọi dữ liệu nhạy cảm và phần mềm được cấp phép đã bị xóa hoặc ghi đè an toàn.

A.8. Các biện pháp kiểm soát về kỹ thuật (Technological Controls)

8.1 Thiết bị đầu cuối người dùng (User End Point Devices)

Tài liệu phục vụ Đào tạo, nghiên cứu

Kiểm soát:

Thông tin lưu trữ, xử lý hoặc truy cập thông qua thiết bị đầu cuối của người dùng phải được bảo vệ bằng các biện pháp an toàn phù hợp.

8.2 Quyền truy cập đặc quyền (Privileged Access Rights)

Kiểm soát:

Việc cấp và sử dụng quyền truy cập đặc quyền (ví dụ: quản trị hệ thống) phải được hạn chế và quản lý chặt chẽ.

8.3 Hạn chế truy cập thông tin (Information Access Restriction)

Kiểm soát:

Truy cập vào thông tin và tài sản liên quan phải được hạn chế theo các chính sách kiểm soát truy cập đã thiết lập.

8.4 Truy cập mã nguồn (Access to Source Code)

Kiểm soát:

Việc đọc và ghi mã nguồn, công cụ phát triển và thư viện phần mềm phải được quản lý thích hợp nhằm bảo vệ tài sản trí tuệ và ngăn chặn nguy cơ bị thay đổi trái phép.

8.5 Xác thực an toàn (Secure Authentication)

Kiểm soát:

Phải triển khai các công nghệ và quy trình xác thực an toàn dựa trên các yêu cầu kiểm soát truy cập.

8.6 Quản lý dung lượng (Capacity Management)

Kiểm soát:

Việc sử dụng tài nguyên CNTT phải được giám sát và điều chỉnh phù hợp với nhu cầu hiện tại và dự kiến nhằm tránh gián đoạn dịch vụ.

8.7 Bảo vệ chống phần mềm độc hại (Protection Against Malware)

Kiểm soát:

Các biện pháp phòng chống phần mềm độc hại phải được triển khai và hỗ trợ bởi hoạt động nâng cao nhận thức cho người dùng.

8.8 Quản lý các lỗ hổng kỹ thuật (Management of Technical Vulnerabilities)

Tài liệu phục vụ Đào tạo, nghiên cứu

Bản Dịch nhằm phục vụ Đào tạo và phổ biến Kiến thức, Khi áp dụng Cá nhân, Tổ chức phải tuân thủ nguyên tắc Bản Quyền và mua chính tức Tiêu chuẩn. (contact: Lê Xuân Trường 0868688767 / 0903452826)

Kiểm soát:

Phải thu thập thông tin về lỗ hổng kỹ thuật, đánh giá mức độ phơi nhiễm của tổ chức và thực hiện các biện pháp giảm thiểu phù hợp.

8.9 Quản lý cấu hình (Configuration Management)

Kiểm soát:

Các cấu hình, bao gồm cấu hình bảo mật của phần cứng, phần mềm, dịch vụ và mạng, phải được xác lập, lập tài liệu, triển khai, giám sát và rà soát định kỳ.

8.10 Xóa thông tin (Information Deletion)

Kiểm soát:

Thông tin lưu trữ trên hệ thống, thiết bị hoặc phương tiện lưu trữ khác phải được xóa khi không còn cần thiết, theo phương pháp an toàn.

8.11 Che giấu dữ liệu (Data Masking)

Kiểm soát:

Phải áp dụng các kỹ thuật che giấu dữ liệu phù hợp với chính sách truy cập thông tin và yêu cầu kinh doanh, đồng thời tuân thủ các quy định pháp luật hiện hành.

8.12 Ngăn ngừa rò rỉ dữ liệu (Data Leakage Prevention)

Kiểm soát:

Các biện pháp phòng chống rò rỉ dữ liệu phải được áp dụng cho hệ thống, mạng và các thiết bị xử lý, lưu trữ hoặc truyền tải thông tin nhạy cảm.

8.13 Sao lưu thông tin (Information Backup)

Kiểm soát:

Phải duy trì và thường xuyên kiểm tra các bản sao lưu thông tin, phần mềm và hệ thống theo chính sách sao lưu đã thỏa thuận.

8.14 Dự phòng các phương tiện xử lý thông tin (Redundancy of Information Processing Facilities)

Kiểm soát:

Các phương tiện xử lý thông tin phải được thiết kế có dự phòng đủ để đáp ứng các yêu cầu về tính sẵn sàng.

8.15 Ghi nhật ký (Logging)

Tài liệu phục vụ Đào tạo, nghiên cứu

Bản Dịch nhằm phục vụ Đào tạo và phổ biến Kiến thức, Khi áp dụng Cá nhân, Tổ chức phải tuân thủ nguyên tắc Bản Quyền và mua chính tức Tiêu chuẩn. (contact: Lê Xuân Trường 0868688767 / 0903452826)

Kiểm soát:

Phải ghi nhận, lưu trữ, bảo vệ và phân tích các nhật ký liên quan đến hoạt động, ngoại lệ, sự cố và các sự kiện an toàn thông tin khác.

8.16 Các hoạt động giám sát (Monitoring Activities)

Kiểm soát:

Phải giám sát các mạng, hệ thống và ứng dụng để phát hiện các hành vi bất thường và thực hiện hành động phù hợp.

8.17 Đồng bộ hóa thời gian hệ thống (Clock Synchronization)

Kiểm soát:

Các hệ thống xử lý thông tin phải được đồng bộ hóa thời gian với các nguồn thời gian đã được phê duyệt.

8.18 Sử dụng các chương trình tiện ích đặc quyền (Use of Privileged Utility Programs)

Kiểm soát:

Việc sử dụng các chương trình tiện ích có thể vượt qua kiểm soát hệ thống hoặc ứng dụng phải được hạn chế và kiểm soát chặt chẽ.

8.19 Cài đặt phần mềm trên hệ thống vận hành (Installation of Software on Operational Systems)

Kiểm soát:

Phải có quy trình và biện pháp đảm bảo việc cài đặt phần mềm trên hệ thống vận hành được thực hiện an toàn.

8.20 An toàn mạng (Network Security)

Kiểm soát:

Mạng và các thiết bị mạng phải được bảo mật, quản lý và kiểm soát nhằm bảo vệ thông tin lưu trữ, xử lý và truyền tải trong hệ thống và ứng dụng.

8.21 An toàn dịch vụ mạng (Security of Network Services)

Kiểm soát:

Các cơ chế an toàn, mức dịch vụ và yêu cầu đối với dịch vụ mạng phải được xác định, thực hiện và giám sát thường xuyên.

8.22 Phân tách mạng (Segregation of Networks)

Tài liệu phục vụ Đào tạo, nghiên cứu

Kiểm soát:

Các nhóm dịch vụ thông tin, người dùng và hệ thống thông tin phải được phân tách trong mạng tổ chức nhằm giảm thiểu rủi ro truy cập trái phép.

8.23 Lọc web (Web Filtering)

Kiểm soát:

Phải quản lý việc truy cập vào các trang web bên ngoài nhằm giảm thiểu nguy cơ tiếp xúc với nội dung độc hại hoặc không phù hợp.

8.24 Sử dụng mật mã (Use of Cryptography)

Kiểm soát:

Phải xác định và áp dụng các quy tắc sử dụng mật mã một cách hiệu quả, bao gồm cả quản lý khóa mã hóa, để bảo vệ thông tin.

8.25 Vòng đời phát triển phần mềm an toàn (Secure Development Life Cycle)

Kiểm soát:

Phải xây dựng và áp dụng các quy tắc cho quá trình phát triển phần mềm và hệ thống theo cách an toàn.

8.26 Yêu cầu an toàn thông tin đối với ứng dụng (Application Security Requirements)

Kiểm soát:

Các yêu cầu về an toàn thông tin phải được xác định, phê duyệt và đưa vào quy trình phát triển hoặc mua sắm ứng dụng.

8.27 Nguyên tắc kiến trúc và kỹ thuật hệ thống an toàn (Secure System Architecture and Engineering Principles)

Kiểm soát:

Phải xây dựng, lập tài liệu, duy trì và áp dụng các nguyên tắc kỹ thuật để phát triển các hệ thống thông tin an toàn.

8.28 Lập trình an toàn (Secure Coding)

Kiểm soát:

Phải áp dụng các nguyên tắc lập trình an toàn trong quá trình phát triển phần mềm nhằm giảm thiểu các lỗ hổng an ninh.

Tài liệu phục vụ Đào tạo, nghiên cứu

Bản Dịch nhằm phục vụ Đào tạo và phổ biến Kiến thức, Khi áp dụng Cá nhân, Tổ chức phải tuân thủ nguyên tắc Bản Quyền và mua chính tức Tiêu chuẩn. (contact: Lê Xuân Trường 0868688767 / 0903452826)

8.29 Kiểm thử an toàn trong phát triển và nghiệm thu (Security Testing in Development and Acceptance)

Kiểm soát:

Phải xác định và thực hiện các quy trình kiểm thử an toàn trong suốt vòng đời phát triển hệ thống.

8.30 Phát triển thuê ngoài (Outsourced Development)

Kiểm soát:

Tổ chức phải giám sát, chỉ đạo và đánh giá các hoạt động phát triển hệ thống được thuê ngoài nhằm đảm bảo các yêu cầu an toàn thông tin được đáp ứng.

8.31 Phân tách môi trường phát triển, kiểm thử và vận hành (Separation of Development, Test and Production Environments)

Kiểm soát:

Phải tách biệt và bảo vệ các môi trường phát triển, kiểm thử và vận hành nhằm giảm thiểu nguy cơ ảnh hưởng lẫn nhau hoặc truy cập trái phép.

8.32 Quản lý thay đổi (Change Management)

Kiểm soát:

Các thay đổi đối với phương tiện xử lý thông tin và hệ thống phải tuân theo quy trình quản lý thay đổi chính thức để đảm bảo sự kiểm soát và giảm thiểu rủi ro.

8.33 Thông tin kiểm thử (Test Information)

Kiểm soát:

Thông tin được sử dụng trong quá trình kiểm thử phải được lựa chọn cẩn thận, bảo vệ và quản lý phù hợp.

8.34 Bảo vệ hệ thống thông tin trong quá trình kiểm thử đánh giá (Protection of Information Systems During Audit Testing)

Kiểm soát:

Việc kiểm thử và các hoạt động đánh giá hệ thống vận hành phải được lập kế hoạch và thống nhất trước với quản lý thích hợp để đảm bảo không gây ảnh hưởng tiêu cực đến hệ thống.

Đánh giá các cuộc kiểm thử và các hoạt động đảm bảo khác liên quan đến việc đánh giá hệ thống vận hành sẽ được lập kế hoạch và thống nhất giữa bên đánh giá và nhà quản lý một cách phù hợp.

Tài liệu phục vụ Đào tạo, nghiên cứu

Bản Dịch nhằm phục vụ Đào tạo và phổ biến Kiến thức, Khi áp dụng Cá nhân, Tổ chức phải tuân thủ nguyên tắc Bản Quyền và mua chính tức Tiêu chuẩn. (contact: Lê Xuân Trường 0868688767 / 0903452826)