TCVN TIÊU CHUẨN QUỐC GIA

TCVN ISO/IEC 27001:2019
ISO/IEC 27001:2013

Xuất bản lần 2

CÔNG NGHỆ THÔNG TIN - CÁC KỸ THUẬT AN TOÀN - HỆ THỐNG QUẢN LÝ AN TOÀN THÔNG TIN - CÁC YÊU CẦU

Information technology - Security techniques - Infomation security management systems - Requirements

HÀ NỘI – 2019

Mục lục

Lời nói đầu

TCVN ISO/IEC 27001:2019 thay thế TCVN ISO/IEC 27001:2009.

TCVN ISO/IEC 27001:2019 hoàn toàn tương đương với ISO/IEC 27001:2013; ISO/IEC 27001:2013/Cor.1:2014, ISO/IEC 27001:2013/Cor.2:2015.

TCVN ISO/IEC 27001:2019 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.

0 Lời giới thiệu

0.1 Tổng quan

Tiêu chuẩn này quy định các yêu cầu đối với hoạt động thiết lập, triển khai, duy trì và cải tiến liên tục hệ thống quản lý an toàn thông tin. Việc chấp nhận một hệ thống quản lý an toàn thông tin là quyết định chiến lược của tổ chức. Việc thiết lập và thực hiện một hệ thống quản lý an toàn thông tin của tổ chức chịu ảnh hưởng bởi nhu cầu và mục tiêu của tổ chức, các yêu cầu về an toàn, các quy trình của tổ chức được sử dụng và bởi quy mô và cấu trúc của tổ chức. Tất cả những yếu tố ảnh hưởng này dự kiến sẽ thay đổi theo thời gian.

Hệ thống quản lý an toàn thông tin đảm bảo tính bảo mật, tính toàn vẹn và tính sẵn sàng của thông tin bằng cách áp dụng quy trình quản lý rủi ro và mang lại niềm tin cho các bên liên quan rằng các rủi ro được quản lý đầy đủ.

Điều quan trọng là hệ thống quản lý an toàn thông tin là một phần và được tích hợp các quy trình của tổ chức và với cấu trúc quản lý tổng thể và an toàn thông tin được xem xét trong thiết kế các quy trình, các hệ thống thông tin và các kiểm soát. Dự kiến rằng việc triển khai một hệ thống quản lý an toàn thông tin sẽ có quy mô phù hợp với nhu cầu của tổ chức.

Tiêu chuẩn này có thể được sử dụng bởi các phòng ban nội bộ và bên ngoài để đánh giá khả năng của tổ chức trong việc đáp ứng các yêu cầu an toàn thông tin của chính tổ chức.

Thứ tự yêu cầu được trình bày trong tiêu chuẩn này không phản ánh tầm quan trọng của chúng hay hàm ý thứ tự mà chúng sẽ được thực hiện. Các danh mục được liệt kê chỉ nhằm mục đích tham khảo.

ISO/IEC 27000 mô tả tổng quan và từ vựng của các hệ thống quản lý an toàn thông tin, tham khảo bộ tiêu chuẩn hệ thống quản lý an toàn thông tin (bao gồm ISO/IEC 27003, ISO/IEC 27004 và 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

Tiêu chuẩn này áp dụng cấu trúc cấp cao, cùng tiêu đề điều con, đoạn văn, thuật ngữ chung và định nghĩa cốt lõi được xác định trong Phụ lục SL của Các chỉ dẫn ISO/IEC, Phần 1, Phần Bổ sung ISO hợp nhất, và do đó duy trì sự tương thích với các tiêu chuẩn hệ thống quản lý khác đã áp dụng Phụ lục SL.

Cách tiếp cận phổ biến được xác định trong Phụ lục SL này sẽ hữu ích cho những tổ chức lựa chọn vận hành một hệ thống quản lý duy nhất đáp ứng yêu cầu của hai hoặc nhiều tiêu chuẩn hệ thống quản lý.

Công nghệ thông tin - Các kỹ thuật an toàn - Hệ thống quản lý an toàn thông tin - Các yêu cầu

Information technology - Security techniques - Information security management systems - Requirements

1 Phạm vi áp dụng

Tiêu chuẩn này quy định các yêu cầu đối với hoạt động thiết lập, triển khai, duy trì và cải tiến liên tục hệ thống quản lý an toàn thông tin trong bối cảnh của một tổ chức. Tiêu chuẩn này cũng bao gồm các yêu cầu cho việc đánh giá và xử lý rủi ro an toàn thông tin phù hợp với yêu cầu của tổ chức. Các yêu cầu đặt ra trong tiêu chuẩn này mang tính chất tổng quan và nhằm áp dụng cho tất cả các tổ chức, không phân biệt loại hình, quy mô hay bản chất. Điều 4 đến Điều 10 của tiêu chuẩn là bắt buộc nếu một tổ chức công bố phù hợp với tiêu chuẩn này.

2 Tài liệu viện dẫn

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

TCVN 11238:2015 (ISO/IEC 27000:2014), *Công nghệ thông tin - Các kỹ thuật an toàn - Hệ thống quản lý an toàn thông tin - Tổng quan và từ vựng (Information technology - Security techniques - Information security management systems - Overview and vocabulary).*

3 Thuật ngữ và định nghĩa

Tiêu chuẩn này sử dụng các thuật ngữ và định nghĩa nêu trong TCVN 11238:2015 (ISO/IEC 27000:2014).

4 Bối cảnh của tổ chức

4.1 Hiểu tổ chức và bối cảnh của tổ chức

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

CHÚ THÍCH: Việc xác định những vấn đề liên quan tới thiết lập phạm vi nội bộ và bên ngoài của tổ chức được nêu tại Điều 5.3 của TCVN ISO 31000:2011 (ISO 31000:2009) [5].

4.2 Hiểu được nhu cầu và mong đợi của các bên liên quan

Tổ chức phải xác định:

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