TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN ISO/IEC 27001:2009
ISO/IEC 27001:2005

Xuất bản lần 1

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

Information technology – Information security management system - Requirements

HÀ NỘI – 2009

Mục lục

Lời nói đầu

TCVN ISO/IEC 27001:2009 hoàn toàn tương đương với ISO/IEC 27001:2005.

TCVN ISO/IEC 27001:2009 do Trung tâm Ứng cứu khẩn cấp Máy tính Việt Nam 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 - Hệ thống quản lý an toàn thông tin – Các yêu cầu

Information technology – Information security management system - Requirements

1 Phạm vi áp dụng

Tiêu chuẩn này áp dụng rộng rãi cho nhiều loại hình tổ chức (ví dụ: các tổ chức thương mại, cơ quan nhà nước, tổ chức phi lợi nhuận). Tiêu chuẩn này chỉ rõ yêu cầu đối với hoạt động thiết lập; triển khai; điều hành; giám sát; soát xét; duy trì và cải tiến một hệ thống quản lý an toàn thông tin (ISMS) để đảm bảo an toàn thông tin trước những rủi ro có thể xảy ra với các hoạt động của tổ chức. Tiêu chuẩn này cũng chỉ rõ các yêu cầu khi triển khai các biện pháp quản lý an toàn đã được chọn lọc phù hợp với nhu cầu của tổ chức hoặc bộ phận của tổ chức.

Hệ thống ISMS được thiết kế các biện pháp đảm bảo an toàn thông tin phù hợp và đầy đủ để bảo vệ các tài sản thông tin và đem lại sự tin tưởng của các bên liên quan như đối tác, khách hàng…

Các yêu cầu trình bày trong tiêu chuẩn này mang tính tổng quát và nhằm ứng dụng rộng rãi cho nhiều loại hình tổ chức khác nhau. Điều 4, 5, 6, 7 và 8 của tiêu chuẩn là bắt buộc nếu tổ chức công bố phù hợp với tiêu chuẩn này; các loại trừ đối với các biện pháp quản lý, nếu cần thiết để thoả mãn các tiêu chí chấp nhận rủi ro, cần có lý do chính đáng và có bằng chứng chứng minh các rủi ro liên đới đã được chấp nhận bởi người có trách nhiệm.

2 Tài liệu viện dẫn

ISO/IEC 17799:2005, Information technology – Security techniques – Code of practice for information security management *(Công nghệ thông tin – Các kỹ thuật an toàn – Quy phạm thực hành quản lý an toàn thông tin).*

3 Thuật ngữ và định nghĩa

Tiêu chuẩn này sử dụng các thuật ngữ và định nghĩa sau:

3.1

Tài sản (asset)

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

3.2