TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN ISO/IEC 27002:2011
ISO/IEC 27002:2005

Xuất bản lần 1

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 infomation security management

HÀ NỘI – 2011

Mục lục

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 infomation 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]