

**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
information security management*

HÀ NỘI – 2011

Mục lục

1	Phạm vi áp dụng	11
2	Thuật ngữ và định nghĩa	11
3	Đánh giá và xử lý rủi ro	14
3.1	Đánh giá rủi ro an toàn thông tin	14
3.2	Xử lý các rủi ro an toàn thông tin.....	14
4	Chính sách an toàn thông tin	15
4.1	Chính sách an toàn thông tin.....	15
4.1.1	Tài liệu chính sách an toàn thông tin	16
4.1.2	Soát xét lại chính sách an toàn thông tin	16
5	Tổ chức đảm bảo an toàn thông tin	18
5.1	Tổ chức nội bộ.....	18
5.1.1	Cam kết của ban quản lý về đảm bảo an toàn thông tin.....	18
5.1.2	Phối hợp đảm bảo an toàn thông tin.....	19
5.1.3	Phân định trách nhiệm đảm bảo an toàn thông tin	19
5.1.4	Quy trình cấp phép cho phương tiện xử lý thông tin.....	20
5.1.5	Các thỏa thuận về bảo mật.....	21
5.1.6	Liên lạc với những cơ quan/tổ chức có thẩm quyền.....	22
5.1.7	Liên lạc với các nhóm chuyên gia	22
5.1.8	Soát xét độc lập về an toàn thông tin.....	23
5.2	Các bên tham gia bên ngoài.....	24
5.2.1	Xác định các rủi ro liên quan đến các bên tham gia bên ngoài.....	24
5.2.2	Giải quyết an toàn khi làm việc với khách hàng.....	26
5.2.3	Giải quyết an toàn trong các thỏa thuận với bên thứ ba.....	27
6	Quản lý tài sản	30
6.1	Trách nhiệm đối với tài sản	30
6.1.1	Kiểm kê tài sản.....	30
6.1.2	Quyền sở hữu tài sản	31
6.1.3	Sử dụng hợp lý tài sản.....	32
6.2	Phân loại thông tin.....	33
6.2.1	Hướng dẫn phân loại	33
6.2.2	Gắn nhãn và xử lý thông tin.....	34
7	Đảm bảo an toàn thông tin từ nguồn nhân lực	34
7.1	Trước khi tuyển dụng	34
7.1.1	Các vai trò và trách nhiệm	35
7.1.2	Thẩm tra.....	35
7.1.3	Điều khoản và điều kiện tuyển dụng	36

7.2	Trong thời gian làm việc	37
7.2.1	Trách nhiệm của ban quản lý	38
7.2.2	Nhận thức, giáo dục và đào tạo về an toàn thông tin	38
7.2.3	Xử lý kỷ luật	39
7.3	Chấm dứt hoặc thay đổi công việc	39
7.3.1	Trách nhiệm khi kết thúc hợp đồng	40
7.3.2	Bàn giao tài sản	40
7.3.3	Hủy bỏ quyền truy cập	41
8	Đảm bảo an toàn vật lý và môi trường	42
8.1	Các khu vực an toàn	42
8.1.1	Vành đai an toàn vật lý	42
8.1.2	Kiểm soát cổng truy cập vật lý	43
8.1.3	Bảo vệ các văn phòng, phòng làm việc và vật dụng	44
8.1.4	Bảo vệ chống lại các mối đe dọa từ bên ngoài và từ môi trường	44
8.1.5	Làm việc trong các khu vực an toàn	44
8.1.6	Các khu vực truy cập tự do, phân phối và tập kết hàng	45
8.2	Đảm bảo an toàn trang thiết bị	46
8.2.1	Bố trí và bảo vệ thiết bị	46
8.2.2	Các tiện ích hỗ trợ	47
8.2.3	An toàn cho dây cáp	48
8.2.4	Bảo dưỡng thiết bị	48
8.2.5	An toàn cho thiết bị hoạt động bên ngoài trụ sở của tổ chức	49
8.2.6	An toàn khi loại bỏ hoặc tái sử dụng thiết bị	50
8.2.7	Di dời tài sản	50
9	Quản lý truyền thông và vận hành	51
9.1	Các trách nhiệm và thủ tục vận hành	51
9.1.1	Các thủ tục vận hành được ghi thành văn bản	51
9.1.2	Quản lý thay đổi	52
9.1.3	Phân tách nhiệm vụ	52
9.1.4	Phân tách các chức năng phát triển, kiểm thử và vận hành	53
9.2	Quản lý chuyển giao dịch vụ của bên thứ ba	54
9.2.1	Chuyển giao dịch vụ	54
9.2.2	Giám sát và soát xét các dịch vụ của bên thứ ba	54
9.2.3	Quản lý thay đổi đối với các dịch vụ của bên thứ ba	55
9.3	Lập kế hoạch và chấp nhận hệ thống	56
9.3.1	Quản lý năng lực hệ thống	56
9.3.2	Chấp nhận hệ thống	57
9.4	Bảo vệ chống lại mã độc hại và mã di động	58

9.4.1	Quản lý chống lại mã độc hại.....	58
9.4.2	Kiểm soát các mã di động.....	59
9.5	Sao lưu.....	60
9.5.1	Sao lưu thông tin.....	60
9.6	Quản lý an toàn mạng.....	61
9.6.1	Kiểm soát mạng.....	61
9.6.2	An toàn cho các dịch vụ mạng.....	62
9.7	Xử lý phương tiện.....	63
9.7.1	Quản lý các phương tiện có thể di dời.....	63
9.7.2	Loại bỏ phương tiện.....	64
9.7.3	Các thủ tục xử lý thông tin.....	64
9.7.4	An toàn cho các tài liệu hệ thống.....	65
9.8	Trao đổi thông tin.....	66
9.8.1	Các chính sách và thủ tục trao đổi thông tin.....	66
9.8.2	Các thỏa thuận trao đổi.....	68
9.8.3	Vận chuyển phương tiện vật lý.....	69
9.8.4	Thông điệp điện tử.....	70
9.8.5	Các hệ thống thông tin nghiệp vụ.....	70
9.9	Các dịch vụ thương mại điện tử.....	71
9.9.1	Thương mại điện tử.....	71
9.9.2	Các giao dịch trực tuyến.....	72
9.9.3	Thông tin công khai.....	73
9.10	Giám sát.....	74
9.10.1	Ghi nhật ký đánh giá.....	74
9.10.2	Giám sát sử dụng hệ thống.....	75
9.10.3	Bảo vệ các thông tin nhật ký.....	77
9.10.4	Nhật ký của người điều hành và người quản trị.....	77
9.10.5	Ghi nhật ký lỗi.....	78
9.10.6	Đồng bộ thời gian.....	78
10	Quản lý truy cập.....	79
10.1	Yêu cầu nghiệp vụ đối với quản lý truy cập.....	79
10.1.1	Chính sách quản lý truy cập.....	79
10.2	Quản lý truy cập người dùng.....	80
10.2.1	Đăng ký người dùng.....	80
10.2.2	Quản lý đặc quyền.....	81
10.2.3	Quản lý mật khẩu người dùng.....	82
10.2.4	Soát xét các quyền truy cập của người dùng.....	83
10.3	Các trách nhiệm của người dùng.....	84

10.3.1	Sử dụng mật khẩu.....	84
10.3.2	Thiết bị người dùng khi không sử dụng	85
10.3.3	Chính sách màn hình sạch và bàn làm việc sạch.....	85
10.4	Quản lý truy cập mạng	86
10.4.1	Chính sách sử dụng các dịch vụ mạng.....	87
10.4.2	Xác thực người dùng cho các kết nối bên ngoài	87
10.4.3	Định danh thiết bị trong các mạng	88
10.4.4	Chuẩn đoán từ xa và bảo vệ cổng cấu hình	89
10.4.5	Phân tách trên mạng.....	89
10.4.6	Quản lý kết nối mạng	90
10.4.7	Quản lý định tuyến mạng	91
10.5	Quản lý truy cập hệ điều hành.....	91
10.5.1	Các thủ tục đăng nhập an toàn	91
10.5.2	Định danh và xác thực người dùng.....	93
10.5.3	Hệ thống quản lý mật khẩu	93
10.5.4	Sử dụng các tiện ích hệ thống	94
10.5.5	Thời gian giới hạn của phiên làm việc	95
10.5.6	Giới hạn thời gian kết nối.....	95
10.6	Điều khiển truy cập thông tin và ứng dụng	96
10.6.1	Hạn chế truy cập thông tin.	96
10.6.2	Cách ly hệ thống nhạy cảm.....	97
10.7	Tính toán di động và làm việc từ xa	97
10.7.1	Tính toán và truyền thông qua thiết bị di động.....	98
10.7.2	Làm việc từ xa.....	99
11	Tiếp nhận, phát triển và duy trì các hệ thống thông tin.....	100
11.1	Yêu cầu đảm bảo an toàn cho các hệ thống thông tin	100
11.1.1	Phân tích và đặc tả các yêu cầu về an toàn	101
11.2	Xử lý đúng trong các ứng dụng	102
11.2.1	Kiểm tra tính hợp lệ của dữ liệu đầu vào	102
11.2.2	Kiểm soát việc xử lý nội bộ	103
11.2.3	Tính toàn vẹn thông điệp	104
11.2.4	Kiểm tra tính hợp lệ của dữ liệu đầu ra.....	104
11.3	Quản lý mã hóa	105
11.3.1	Chính sách sử dụng các biện pháp quản lý mã hóa.....	105
11.3.2	Quản lý khóa	106
11.4	An toàn cho các tệp tin hệ thống	108
11.4.1	Quản lý các phần mềm điều hành	108
11.4.2	Bảo vệ dữ liệu kiểm tra hệ thống	110

11.4.3	Quản lý truy cập đến mã nguồn chương trình	110
11.5	Bảo đảm an toàn trong các quy trình hỗ trợ và phát triển	111
11.5.1	Các thủ tục quản lý thay đổi.....	111
11.5.2	Soát xét kỹ thuật các ứng dụng sau thay đổi của hệ điều hành	112
11.5.3	Hạn chế thay đổi các gói phần mềm.....	113
11.5.4	Sự rò rỉ thông tin	113
11.5.5	Phát triển phần mềm thuê khoán	114
11.6	Quản lý các điểm yếu kỹ thuật	115
11.6.1	Quản lý các điểm yếu về kỹ thuật	115
12	Quản lý các sự cố an toàn thông tin.....	117
12.1	Báo cáo về các sự kiện an toàn thông tin và các điểm yếu.....	117
12.1.1	Báo cáo các sự kiện an toàn thông tin.....	117
12.1.2	Báo cáo các điểm yếu về an toàn thông tin	118
12.2	Quản lý các sự cố an toàn thông tin và cải tiến.....	119
12.2.1	Các trách nhiệm và thủ tục	119
12.2.2	Rút bài học kinh nghiệm từ các sự cố an toàn thông tin.....	121
12.2.3	Thu thập chứng cứ.....	121
13	Quản lý sự liên tục của hoạt động nghiệp vụ.....	122
13.1	Các khía cạnh an toàn thông tin trong quản lý sự liên tục của hoạt động nghiệp vụ	122
13.1.1	Tính đến an toàn thông tin trong các quy trình quản lý sự liên tục của hoạt động nghiệp vụ	123
13.1.2	Đánh giá rủi ro và sự liên tục trong hoạt động của tổ chức	124
13.1.3	Xây dựng và triển khai các kế hoạch về tính liên tục, trong đó bao gồm vấn đề đảm bảo an toàn thông tin	124
13.1.4	Khung hoạch định sự liên tục trong hoạt động nghiệp vụ.....	126
13.1.5	Kiểm tra, duy trì và đánh giá lại các kế hoạch đảm bảo sự liên tục trong hoạt động nghiệp vụ	127
14	Sự tuân thủ.....	128
14.1	Sự tuân thủ các quy định pháp lý	128
14.1.1	Xác định các điều luật hiện đang áp dụng được.....	128
14.1.2	Quyền sở hữu trí tuệ (IPR)	129
14.1.3	Bảo vệ các hồ sơ của tổ chức	130
14.1.4	Bảo vệ dữ liệu và sự riêng tư của thông tin cá nhân	131
14.1.5	Ngăn ngừa việc lạm dụng phương tiện xử lý thông tin.....	132
14.1.6	Quy định về quản lý mã hóa	133
14.2	Sự tuân thủ các chính sách và tiêu chuẩn an toàn, và tương thích kỹ thuật.....	133
14.2.1	Sự tuân thủ các tiêu chuẩn và chính sách an toàn.....	133
14.2.2	Kiểm tra sự tương thích kỹ thuật	134

14.3	Xem xét việc đánh giá các hệ thống thông tin.....	135
14.3.1	Các biện pháp quản lý đánh giá các hệ thống thông tin	135
14.3.2	Bảo vệ các công cụ đánh giá hệ thống thông tin	136
Thư mục tài liệu tham khảo		137

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]