

**TCVN**

**TIÊU CHUẨN QUỐC GIA**

**TCVN 13265:2021**  
**ISO/IEC 27009:2016**

Xuất bản lần 1

**CÔNG NGHỆ THÔNG TIN – CÁC KỸ THUẬT AN TOÀN-  
ÁP DỤNG TCVN ISO/IEC 27001 CHO LĨNH VỰC CỤ THỂ-  
CÁC YÊU CẦU**

*Information technology – Security techniques – Sector- specific application  
of TCVN ISO/IEC 27001 - Requirements*

HÀ NỘI - 2021

## Mục lục

Lời nói đầu .....	4
1 Phạm vi áp dụng .....	5
2 Tài liệu viện dẫn .....	5
3 Thuật ngữ và định nghĩa .....	5
4 Tổng quan về tiêu chuẩn .....	6
4.1 Tổng quan .....	6
4.2 Cấu trúc của tiêu chuẩn .....	7
4.3 Mở rộng các yêu cầu của TCVN ISO/IEC 27001 hoặc các biện pháp kiểm soát của TCVN ISO/IEC 27002 .....	7
5 Các yêu cầu bổ sung, hiệu chỉnh hoặc giải thích TCVN ISO/IEC 27001 .....	7
5.1 Tổng quan .....	7
5.2 Yêu cầu bổ sung .....	8
5.3 Yêu cầu hiệu chỉnh .....	8
5.4 Yêu cầu giải thích .....	8
6 Hướng dẫn bổ sung hoặc sửa đổi TCVN ISO/IEC 27002 .....	8
6.1 Tổng quan .....	8
6.2 Hướng dẫn bổ sung .....	9
6.3 Hướng dẫn sửa đổi .....	9
Phụ lục A (Quy định) Mẫu để xây dựng các tiêu chuẩn cho lĩnh vực cụ thể liên quan đến TCVN ISO/IEC 27001:2019 hoặc TCVN ISO/IEC 27002:2020 .....	10

## **Lời nói đầu**

TCVN 13265:2021 hoàn toàn tương đương ISO/IEC 27009:2016.

TCVN 13265:2021 do Trung tâm ứng cứu khẩn cấp không gian mạng Việt Nam (thuộc Cục An toàn thông tin) 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 - Áp dụng TCVN ISO/IEC 27001 cho lĩnh vực cụ thể - Các yêu cầu

*Information technology - Security techniques - Sector-specific application of TCVN ISO/IEC 27001 - Requirements*

## 1 Phạm vi áp dụng

Tiêu chuẩn này xác định các yêu cầu đối với việc sử dụng TCVN ISO/IEC 27001 trong các lĩnh vực cụ thể (ngành, lĩnh vực ứng dụng hoặc khu vực thị trường). Tiêu chuẩn này hướng dẫn cách thức thêm vào các yêu cầu của TCVN ISO/IEC 27001, cách thức hiệu chỉnh các yêu cầu của TCVN ISO/IEC 27001 và cách thức thêm vào các biện pháp kiểm soát hoặc tập các biện pháp kiểm soát bổ sung cho các biện pháp kiểm soát tại Phụ lục A của TCVN ISO/IEC 27001:2019.

Tiêu chuẩn này đảm bảo các yêu cầu bổ sung hoặc hiệu chỉnh không mâu thuẫn với các yêu cầu trong TCVN ISO/IEC 27001.

Tiêu chuẩn này được áp dụng cho việc xây dựng các tiêu chuẩn cho lĩnh vực cụ thể liên quan đến TCVN ISO/IEC 27001.

## 2 Tài liệu viện dẫn

Các tài liệu viện dẫn sau rất cần thiết cho việc 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 (nếu có).

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.

TCVN ISO/IEC 27001:2019 (ISO/IEC 27001:2013), Công nghệ thông tin - Các kỹ thuật an toàn - Hệ thống quản lý an toàn thông tin - Các yêu cầu.

TCVN ISO/IEC 27002:2020 (ISO/IEC 27002:2013), Công nghệ thông tin - Các kỹ thuật an toàn - Quy tắc 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 nêu trong TCVN 11238 và các thuật ngữ, định nghĩa sau:

### 3.1

#### Giải thích (interpretation)

Diễn giải (dưới dạng yêu cầu hoặc hướng dẫn) yêu cầu của TCVN ISO/IEC 27001 cho lĩnh vực cụ thể mà không làm mất hiệu lực bất kỳ yêu cầu nào của TCVN ISO/IEC 27001.

### 3.2

#### Hiệu chỉnh (refinement)