**Tiêu chuẩn ISO 27001 Hệ thống quản lý an toàn thông tin**

Bộ Tiêu chuẩn ISO 27000 là hệ thống tiêu chuẩn về hệ thống bảo mật & quản lý an ninh thông tin. Thông tin rất quan trọng của mỗi tổ chức và ISO 27001; đưa ra các phưong pháp đánh giá việc theo dõi; bảo vệ và quản lý hệ thống thông tin, dữ liệu. Việc mất thông tin trong bất cứ trường hợp nào; dù ít hay nhiều cũng gây ra thiệt hại cho tổ chức. Thậm chí có thể khiến tổ chức sụp đổ.

## **Khái niệm TCVN ISO 27001**

ISO 27001 là hệ thống tiêu chuẩn của Anh về hệ thống quản lý an ninh thông tin. Tiêu chuẩn ISO 27001 giúp quản lý an ninh thông tin một cách hiệu quả nhất. Thông tin ở đây bao gồm những dữ liệu được lưu lại dưới dạng điện tử; hoặc dữ liệu đã được in ra – dữ liệu mềm và dữ liệu cứng.

Thông qua việc áp dụng ISO 27001. Các tổ chức sẽ xác định được loại thông tin và xác định các mối nguy, rủi ro có thể xảy ra. Sau đó thiết lập hệ thống, thiết lập sự kiểm soát cũng như các quy trình để giảm thiểu các rủi ro đó.  ISO 27001 phù hợp với mọi quy mô của tổ chức; các công ty – doanh nghiệp và nó được áp dụng ở mọi lĩnh vực kinh tế khác nhau.

## **Cấu trúc tiêu chuẩn ISO 27001**

### 07 điều khoản chính của  ISO 27001

Từ phần 4 đến phần 10 của **tiêu chuẩn ISO 27001;** đưa ra yêu cầu bắt buộc về các công việc cần thực hiện trong việc; thiết lập, vận hành, giám sát và nâng cấp Hệ thống quản lý an ninh thông tin của các tổ chức. Bất kỳ vi phạm nào khác biệt so với các quy định nằm trong 07 điều khoản này đều được coi là không tuân thủ theo:

### **Điều khoản 4 – Phạm vi tổ chức:**

Điều khoản này đưa ra các yêu cầu cụ thể để tổ chức căn cứ trên quy mô; lĩnh vực hoạt động và yêu cầu, kỳ vọng của các bên liên quan thiết lập phạm vi Hệ thống quản lý an ninh thông tin phù hợp.

### **Điều khoản 5 – Lãnh đạo:**

Điều khoản này quy định các vấn đề về trách nhiệm; của Ban lãnh đạo mỗi tổ chức trong Hệ thống an ninh thông tin. Bao gồm các yêu cầu về sự cam kết, quyết tâm của Ban lãnh đạo trong việc xây dựng, duy trì hệ thống thông tin; các yêu cầu về việc cung cấp nguồn lực, tài chính để vận hành hệ thống thông tin.

### **Điều khoản 6 – Lập kế hoạch:**

Doanh nghiệp, tổ chức cần định nghĩa và áp dụng các quy trình đánh giá rủi ro; đưa ra các quy trình xử lý. Điều khoản này đưa ra các yêu cầu; về việc thiết lập mục tiêu an toàn thông tin và kế hoạch để đạt được mục tiêu đó.

### **Điều khoản 7 – Hỗ trợ:**

Yêu cầu đối với việc tổ chức đào tạo; nâng cao nhận thức cho toàn thể cán bộ; nhân viên của tổ chức về lĩnh vực an toàn thông tin và ISMS, số hóa thông tin.

### **Điều khoản 8 – Vận hành hệ thống:**

Doanh nghiệp, tổ chức cần có kế hoạch vận hành và quản lý để đạt được các mục tiêu. Đồng thời cần định kỳ thực hiện đánh giá rủi ro an toàn thông tin và có kế hoạch xử lý.

### **Điều khoản 9 – Đánh giá hiệu năng hệ thống:**

Quy định trách nhiệm của Ban lãnh đạo trong việc định kỳ xem xét; đánh giá Hệ thống quản lý an ninh thông tin của tổ chức. Phần này đưa ra yêu cầu đối với mỗi kỳ xem xét hệ thống; đảm bảo đánh giá được toàn bộ hoạt động của hệ thống; đo lường hiệu quả và có kế hoạch khắc phục; nâng cấp hệ thống cho phù hợp.

### **Điều khoản 10 – Cải tiến hệ thống:**

Giữ vững nguyên tắc Kế hoạch – Thực hiện – Kiểm tra – Hành  động. Điều khoản 10 trong tiêu chuẩn ISO 27001; cũng đưa ra các yêu cầu đảm bảo Hệ thống quản lý an ninh thông tin không ngừng được cải tiến trong quá trình hoạt động. Điều khoản này bao gồm các quy định trong việc áp dụng các chính sách mới; các hoạt động khắc phục, phòng ngừa điểm yếu đã xảy ra. Và để đảm bảo hiệu quả của Hệ thống quản lý an ninh thông tin.

### Phụ lục A – Các mục tiêu và biện pháp kiểm soát

Phụ lục A – Các mục tiêu và biện pháp kiểm soát trong **tiêu chuẩn ISO 27001;** đưa ra 14 lĩnh vực kiểm soát nhằm cụ thể hóa các vấn đề mà tổ chức cần xem xét; thực hiện khi xây dựng và duy trì Hệ thống quản lý an ninh thông tin. Các lĩnh vực đưa ra xem xét bao gồm từ chính sách của lãnh đạo tổ chức; tới việc đảm bảo an toàn thông tin trong quản lý; tài sản, nhân sự, các nguyên tắc căn bản để đảm bảo an toàn thông tin trong việc; vận hành, phát triển, duy trì các hệ thống công nghệ thông tin….

Mỗi lĩnh vực khác nhau thì việc kiểm soát lại được cụ thể hóa với các mục tiêu kiểm soát; và các biện pháp cụ thể để đạt được mục tiêu đó. Các biện pháp kiểm soát được lựa chọn; loại bỏ hoặc bổ sung thêm để phù hợp với lĩnh vực hoạt động của mỗi tổ chức.



## **Lợi ích triển khai hệ thống quản lý an ninh thông tin theo tiêu chuẩn ISO 27001**

Hiện nay, ISO 27001 hệ thống quản lý an ninh thông tin; trở nên rất hiệu quả đối với các công ty, tổ chức. Và có thể đáp ứng nhu cầu tương lai của các tổ chức này. Vì công nghệ và các quy định luật pháp thay đổi liên tục. Nên công ty, doanh nghiệp, tổ chức của bạn rất cần một đối tác chứng nhận có thể cung cấp về sự thay đổi của công nghệ; và quy định pháp luật để xây dựng kế hoạch sao cho phù hợp nhất.

Sau đây là những lợi ích khi triển khai hệ thống quản lý an ninh thông tin theo **tiêu chuẩn ISO 27001**:

– Đảm bảo an toàn thông tin của tổ chức đối tác và khách hàng; giúp cho hoạt động của tổ chức luôn thông suốt và an toàn.

– Giúp hoạt động đảm bảo an toàn thông tin luôn được duy trì và cải tiến. Các biện pháp kỹ thuật và chính sách tuân thủ được xem xét, đánh giá hiệu quả và cập nhật định kỳ.

– Giúp nhân viên việc đảm bảo an toàn thông tin trong hoạt động nghiệp vụ thường ngày; Các sự cố an toàn thông tin do người dùng gây ra; sẽ được hạn chế tối đa khi nhân viên được đào tạo; nâng cao nhận thức về an toàn thông tin.

– Đảm bảo hoạt động nghiệp vụ của tổ chức không bị gián đoạn bởi các sự cố liên quan đến an toàn thông tin.

– Nâng cao uy tín của tổ chức, tăng sức cạnh tranh; tạo lòng tin với đối tác, khách hàng; thúc đẩy quá trình toàn cầu hóa và tăng cơ hội hợp tác quốc tế.

## **Quy trình triển khai tiêu chuẩn ISO 27001**

VIỆN TIÊU CHUẨN CHẤT LƯỢNG là một trong những đơn vị chuyên tư vấn. Triển khai Hệ thống ISMS cho các công ty, doanh nghiệp, tổ chức. Chúng tôi đề xuất các tổ chức xây dựng ISMS theo các bước dưới đây để đáp ứng các yêu cầu của tiêu chuẩn ISO 27001:

– Bước 1: Khảo sát và lập kế hoạch.

– Bước 2: Xác định phương pháp quản lý rủi ro an toàn thông tin.

– Bước 3: Xây dựng hệ thống đảm bảo an toàn thông tin tại đơn vị.

– Bước 4: Triển khai áp dụng: các biện pháp đã lựa chọn, đáp ứng chính sách, quy định, quy trình xây dựng và yêu cầu của tiêu chuẩn ISO 27001.

– Bước 5: Đánh giá nội bộ: khắc phục các điểm không phù hợp với yêu cầu của tiêu chuẩn.

Sau khi thực hiện xong bước 5. Công ty/doanh nghiệp/tổ chức có thể mời các đơn vị độc lập để đánh giá; và cấp Chứng nhận phù hợp với tiêu chuẩn Hệ thống quản lý an toàn thông tin ISO 27001 đã xây dựng.