

# **TÀI LIỆU ÔN MÔN CÔNG NGHỆ THÔNG TIN TRONG XÉT TUYỂN VIÊN CHỨC NĂM 2021**

## **1. Luật An ninh mạng số: 24/2018/QH14, ngày 12 tháng 6 năm 2018**

### **Điều 4. Nguyên tắc bảo vệ an ninh mạng**

1. Tuân thủ Hiến pháp và pháp luật; bảo đảm lợi ích của Nhà nước, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

2. Đặt dưới sự lãnh đạo của Đảng Cộng sản Việt Nam, sự quản lý thống nhất của Nhà nước; huy động sức mạnh tổng hợp của hệ thống chính trị và toàn dân tộc; phát huy vai trò nòng cốt của lực lượng chuyên trách bảo vệ an ninh mạng.

3. Kết hợp chặt chẽ giữa nhiệm vụ bảo vệ an ninh mạng, bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia với nhiệm vụ phát triển kinh tế - xã hội, bảo đảm quyền con người, quyền công dân, tạo điều kiện cho cơ quan, tổ chức, cá nhân hoạt động trên không gian mạng.

4. Chủ động phòng ngừa, phát hiện, ngăn chặn, đấu tranh, làm thất bại mọi hoạt động sử dụng không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân; sẵn sàng ngăn chặn các nguy cơ đe dọa an ninh mạng.

5. Triển khai hoạt động bảo vệ an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia; áp dụng các biện pháp bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia.

6. Hệ thống thông tin quan trọng về an ninh quốc gia được thẩm định, chứng nhận đủ điều kiện về an ninh mạng trước khi đưa vào vận hành, sử dụng; thường xuyên kiểm tra, giám sát về an ninh mạng trong quá trình sử dụng và kịp thời ứng phó, khắc phục sự cố an ninh mạng.

7. Mọi hành vi vi phạm pháp luật về an ninh mạng phải được xử lý kịp thời, nghiêm minh.

### **Điều 5. Biện pháp bảo vệ an ninh mạng**

1. Biện pháp bảo vệ an ninh mạng bao gồm:

- a) Thẩm định an ninh mạng;
- b) Đánh giá điều kiện an ninh mạng;
- c) Kiểm tra an ninh mạng;
- d) Giám sát an ninh mạng;
- đ) Ứng phó, khắc phục sự cố an ninh mạng;
- e) Đấu tranh bảo vệ an ninh mạng;
- g) Sử dụng mật mã để bảo vệ thông tin mạng;

h) Ngăn chặn, yêu cầu tạm ngừng, ngừng cung cấp thông tin mạng; đình chỉ, tạm đình chỉ các hoạt động thiết lập, cung cấp và sử dụng mạng viễn thông, mạng Internet, sản xuất và sử dụng thiết bị phát, thu phát sóng vô tuyến theo quy định của pháp luật;

i) Yêu cầu xóa bỏ, truy cập xóa bỏ thông tin trái pháp luật hoặc thông tin sai sự thật trên không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân;

k) Thu thập dữ liệu điện tử liên quan đến hoạt động xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân trên không gian mạng;

l) Phong tỏa, hạn chế hoạt động của hệ thống thông tin; đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin, thu hồi tên miền theo quy định của pháp luật;

m) Khởi tố, điều tra, truy tố, xét xử theo quy định của Bộ luật Tố tụng hình sự;

n) Biện pháp khác theo quy định của pháp luật về an ninh quốc gia, pháp luật về xử lý vi phạm hành chính.

2. Chính phủ quy định trình tự, thủ tục áp dụng biện pháp bảo vệ an ninh mạng, trừ biện pháp quy định tại điểm m và điểm n khoản 1 Điều này.

## **Điều 6. Bảo vệ không gian mạng quốc gia**

Nhà nước áp dụng các biện pháp để bảo vệ không gian mạng quốc gia; phòng ngừa, xử lý hành vi xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân trên không gian mạng.

## **Điều 8. Các hành vi bị nghiêm cấm về an ninh mạng**

1. Sử dụng không gian mạng để thực hiện hành vi sau đây:

a) Hành vi quy định tại khoản 1 Điều 18 của Luật này;

b) Tổ chức, hoạt động, câu kết, xúi giục, mua chuộc, lừa gạt, lôi kéo, đào tạo, huấn luyện người chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam;

c) Xuyên tạc lịch sử, phủ nhận thành tựu cách mạng, phá hoại khối đại đoàn kết toàn dân tộc, xúc phạm tôn giáo, phân biệt đối xử về giới, phân biệt chủng tộc;

d) Thông tin sai sự thật gây hoang mang trong Nhân dân, gây thiệt hại cho hoạt động kinh tế - xã hội, gây khó khăn cho hoạt động của cơ quan nhà nước hoặc người thi hành công vụ, xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác;

đ) Hoạt động mại dâm, tệ nạn xã hội, mua bán người; đăng tải thông tin dâm ô, đồi trụy, tội ác; phá hoại thuần phong, mỹ tục của dân tộc, đạo đức xã hội, sức khỏe của cộng đồng;

e) Xúi giục, lôi kéo, kích động người khác phạm tội.

2. Thực hiện tấn công mạng, khủng bố mạng, gián điệp mạng, tội phạm mạng; gây sự cố, tấn công, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt hoặc phá hoại hệ thống thông tin quan trọng về an ninh quốc gia.

3. Sản xuất, đưa vào sử dụng công cụ, phương tiện, phần mềm hoặc có hành vi cản trở, gây rối loạn hoạt động của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử; phát tán chương trình tin học gây hại cho hoạt động của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử; xâm nhập trái phép vào mạng viễn thông, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử của người khác.

4. Chống lại hoặc cản trở hoạt động của lực lượng bảo vệ an ninh mạng; tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng biện pháp bảo vệ an ninh mạng.

5. Lợi dụng hoặc lạm dụng hoạt động bảo vệ an ninh mạng để xâm phạm chủ quyền, lợi ích, an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân hoặc để trục lợi.

6. Hành vi khác vi phạm quy định của Luật này.

## **Điều 9. Xử lý vi phạm pháp luật về an ninh mạng**

Người nào có hành vi vi phạm quy định của Luật này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật, xử lý vi phạm hành chính hoặc bị truy cứu trách nhiệm hình sự, nếu gây thiệt hại thì phải bồi thường theo quy định của pháp luật.

## **Điều 22. Đấu tranh bảo vệ an ninh mạng**

1. Đấu tranh bảo vệ an ninh mạng là hoạt động có tổ chức do lực lượng chuyên trách bảo vệ an ninh mạng thực hiện trên không gian mạng nhằm bảo vệ an ninh quốc gia và bảo đảm trật tự, an toàn xã hội.

2. Nội dung đấu tranh bảo vệ an ninh mạng bao gồm:

- a) Tổ chức nắm tình hình có liên quan đến hoạt động bảo vệ an ninh quốc gia;
- b) Phòng, chống tấn công và bảo vệ hoạt động ổn định của hệ thống thông tin quan trọng về an ninh quốc gia;
- c) Làm tê liệt hoặc hạn chế hoạt động sử dụng không gian mạng nhằm gây phương hại an ninh quốc gia hoặc gây tổn hại đặc biệt nghiêm trọng trật tự, an toàn xã hội;
- d) Chủ động tấn công vô hiệu hóa mục tiêu trên không gian mạng nhằm bảo vệ an ninh quốc gia và bảo đảm trật tự, an toàn xã hội.

3. Bộ Công an chủ trì, phối hợp với Bộ, ngành có liên quan thực hiện đấu tranh bảo vệ an ninh mạng.

**2. Thông Tư Số: 54/2017/TT-BYT ngày 29 tháng 12 năm 2017 của Bộ Y tế ban hành bộ tiêu chí ứng dụng công nghệ thông tin tại các cơ sở khám bệnh, chữa bệnh**

#### **Điều 4. Nguyên tắc xác định mức ứng dụng công nghệ thông tin**

1. Mức ứng dụng công nghệ thông tin tại cơ sở khám bệnh, chữa bệnh được xác định theo bảng tổng hợp tiêu chí để đánh giá mức ứng dụng công nghệ thông tin tại cơ sở khám bệnh, chữa bệnh quy định tại Phụ lục II Thông tư này.

2. Bảo đảm nguyên tắc khách quan, chính xác và trung thực.

3. Phải đạt tất cả tiêu chí ở mức đánh giá. Nếu có ít nhất 01 tiêu chí không đạt thì xếp ở mức thấp hơn liền kề.

#### **Điều 5. Hướng dẫn việc xác định mức ứng dụng công nghệ thông tin**

1. Căn cứ vào quy định tại Điều 3 và Điều 4 Thông tư này, người đứng đầu cơ sở khám bệnh, chữa bệnh quyết định đầu tư theo thẩm quyền và ban hành quyết định xác định mức ứng dụng công nghệ thông tin tại cơ sở phụ trách. Trong trường hợp cần thiết, người đứng đầu cơ sở khám bệnh, chữa bệnh thành lập Hội đồng chuyên môn hoặc thuê tổ chức độc lập để tư vấn việc xác định mức ứng dụng công nghệ thông tin tại cơ sở phụ trách.

2. Quyết định xác định mức ứng dụng công nghệ thông tin của cơ sở khám bệnh, chữa bệnh phải được gửi báo cáo cơ quan quản lý cấp trên trực tiếp và gửi Cục Công nghệ thông tin - Bộ Y tế.

3. Người đứng đầu cơ sở khám bệnh, chữa bệnh chịu trách nhiệm trước pháp luật và cơ quan quản lý cấp trên về việc xác định mức ứng dụng công nghệ thông tin tại cơ sở phụ trách; có trách nhiệm xác định lại mức ứng dụng công nghệ thông tin nếu cơ quan quản lý y tế cấp trên kiểm tra phát hiện mức ứng dụng công nghệ thông tin tại cơ sở khám bệnh, chữa bệnh chưa phù hợp với văn bản báo cáo.

### **3. Luật Công nghệ thông tin số: 67/2006/QH11 ngày 29 tháng 6 năm 2006**

#### **Điều 5 Chính sách của Nhà nước về ứng dụng và phát triển công nghệ thông tin**

1. Ưu tiên ứng dụng và phát triển công nghệ thông tin trong chiến lược phát triển kinh tế - xã hội và sự nghiệp công nghiệp hóa, hiện đại hóa đất nước.

2. Tạo điều kiện để tổ chức, cá nhân hoạt động ứng dụng và phát triển công nghệ thông tin đáp ứng yêu cầu phát triển kinh tế - xã hội, đối ngoại, quốc phòng, an ninh; thúc đẩy công nghiệp công nghệ thông tin phát triển thành ngành kinh tế trọng điểm, đáp ứng nhu cầu thị trường nội địa và xuất khẩu.

3. Khuyến khích đầu tư cho lĩnh vực công nghệ thông tin.

4. Ưu tiên dành một khoản ngân sách nhà nước để ứng dụng công nghệ thông tin trong một số lĩnh vực thiết yếu, tạo lập nền công nghiệp công nghệ thông tin và phát triển nguồn nhân lực công nghệ thông tin.

5. Tạo điều kiện thuận lợi để phát triển cơ sở hạ tầng thông tin quốc gia.

6. Có chính sách ưu đãi để tổ chức, cá nhân có hoạt động ứng dụng và phát triển công nghệ thông tin đối với nông nghiệp; nông thôn, vùng sâu, vùng xa, biên giới, hải đảo; người dân tộc thiểu số, người tàn tật, người có hoàn cảnh khó khăn.

7. Bảo đảm quyền và lợi ích hợp pháp của tổ chức, cá nhân ứng dụng và phát triển công nghệ thông tin.

8. Tăng cường giao lưu và hợp tác quốc tế; khuyến khích hợp tác với tổ chức, cá nhân Việt Nam ở nước ngoài trong lĩnh vực công nghệ thông tin.

## **Điều 6. Nội dung quản lý nhà nước về công nghệ thông tin**

1. Xây dựng, tổ chức thực hiện chiến lược, quy hoạch, kế hoạch, chính sách ứng dụng và phát triển công nghệ thông tin.

2. Xây dựng, ban hành, tuyên truyền, phổ biến, tổ chức thực hiện văn bản quy phạm pháp luật, tiêu chuẩn quốc gia, quy chuẩn kỹ thuật trong lĩnh vực công nghệ thông tin.

3. Quản lý an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin.

4. Tổ chức quản lý và sử dụng tài nguyên thông tin, cơ sở dữ liệu quốc gia.

5. Quản lý và tạo điều kiện thúc đẩy công tác hợp tác quốc tế về công nghệ thông tin.

6. Quản lý, đào tạo, bồi dưỡng và phát triển nguồn nhân lực công nghệ thông tin.

7. Xây dựng cơ chế, chính sách và các quy định liên quan đến sản phẩm, dịch vụ công ích trong lĩnh vực công nghệ thông tin.

8. Xây dựng cơ chế, chính sách và các quy định về việc huy động nguồn lực công nghệ thông tin phục vụ quốc phòng, an ninh và các trường hợp khẩn cấp quy định tại Điều 14 của Luật này.

9. Quản lý thống kê về công nghệ thông tin.

10. Thanh tra, kiểm tra, giải quyết khiếu nại, tố cáo và xử lý vi phạm trong lĩnh vực công nghệ thông tin.

## **Điều 7. Trách nhiệm quản lý nhà nước về công nghệ thông tin**

1. Chính phủ thống nhất quản lý nhà nước về công nghệ thông tin.

2. Bộ Bru chính, Viễn thông chịu trách nhiệm trước Chính phủ trong việc chủ trì, phối hợp với bộ, cơ quan ngang bộ có liên quan thực hiện quản lý nhà nước về công nghệ thông tin.

3. Bộ, cơ quan ngang bộ trong phạm vi nhiệm vụ, quyền hạn của mình có trách nhiệm chủ trì, phối hợp với Bộ Bru chính, Viễn thông thực hiện quản lý nhà nước về công nghệ thông tin theo phân công của Chính phủ.

4. Ủy ban nhân dân tỉnh, thành phố trực thuộc trung ương trong phạm vi nhiệm vụ, quyền hạn của mình thực hiện quản lý nhà nước về công nghệ thông tin tại địa phương.

5. Việc tổ chức thực hiện ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước do Chính phủ quy định.