

Số: 24/2016/QĐ-UBND

Kon Tum, ngày 17 tháng 6 năm 2016

**QUYẾT ĐỊNH**

**V/v Ban hành Quy chế đảm bảo an toàn, an ninh thông tin  
trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước  
trên địa bàn tỉnh Kon Tum**

**ỦY BAN NHÂN DÂN TỈNH KON TUM**

Luật tổ chức chính quyền địa phương ngày 19/6/2015;

Căn cứ Luật Ban hành văn bản quy phạm pháp luật của Hội đồng nhân dân, Ủy ban nhân dân ngày 03/12/2004;

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ về Ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước; Nghị định số 72/2013/NĐ-CP ngày 15/7/2013 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng; Quyết định số 898/QĐ-TTg ngày 27/5/2016 của Thủ tướng Chính phủ phê duyệt phương hướng nhiệm vụ bảo đảm an toàn thông tin mạng giai đoạn 2016-2020;

Căn cứ Thông tư số 23/2011/TT-BTTTT ngày 11/8/2011 của Bộ Thông tin và Truyền thông quy định về việc quản lý, vận hành, sử dụng và bảo đảm an toàn thông tin trên mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước; Thông tư số 27/2011/TT-BTTTT ngày 04/10/2011 của Bộ Thông tin và Truyền thông quy định về điều phối các hoạt động ứng cứu sự cố mạng Internet Việt Nam;

Xét đề nghị của Giám đốc Sở Thông tin và Truyền thông tại Tờ trình số 377/TTr-STTTT ngày 19/5/2016,

**QUYẾT ĐỊNH:**

**Điều 1.** Ban hành kèm theo Quyết định này Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Kon Tum.

**Điều 2.** Quyết định này có hiệu lực thi hành sau 10 ngày, kể từ ngày ký ban hành.

**Điều 3.** Chánh Văn phòng Ủy ban nhân dân tỉnh; Giám đốc Sở Thông tin và Truyền thông; Thủ trưởng các sở, ban, ngành cấp tỉnh; Chủ tịch Ủy ban nhân dân các huyện, thành phố; các doanh nghiệp viễn thông, công nghệ thông tin

trên địa bàn tỉnh và Thủ trưởng các đơn vị có liên quan chịu trách nhiệm thi hành Quyết định này./.

**Nơi nhận:**

- Như Điều 3;
- Văn phòng Chính phủ;
- Bộ Thông tin và Truyền thông;
- Cục kiểm tra văn bản (Bộ Tư pháp);
- Thường trực Tỉnh ủy;
- Thường trực HĐND tỉnh;
- Đoàn Đại biểu Quốc hội tỉnh;
- UBNDTTQVN tỉnh;
- CT, các PCT UBND tỉnh;
- Chi cục Văn thư- Lưu trữ tỉnh Kon Tum;
- Báo Kon Tum, Đài PTTH Kon Tum; Công TTĐT tỉnh;
- Lưu: VT, KGVX2.

**TM. ỦY BAN NHÂN DÂN  
CHỦ TỊCH**



**Đào Xuân Quý**

**QUY CHẾ**

**Về đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn Tỉnh Kon Tum**  
(Ban hành kèm theo Quyết định số 24./2016/QĐ-UBND  
ngày 17 tháng 6 năm 2016 của Ủy ban nhân dân tỉnh Kon Tum)

**Chương I  
QUY ĐỊNH CHUNG**

**Điều 1. Phạm vi điều chỉnh**

1. Quy chế này quy định về công tác đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin (CNTT) của các cơ quan nhà nước trên địa bàn tỉnh Kon Tum.

2. Đối với lực lượng vũ trang ngoài việc thực hiện các quy định tại Quy chế này, các quy định khác của pháp luật có liên quan còn phải thực hiện theo quy định của ngành trong đảm bảo an ninh thông tin, bảo mật trên môi trường mạng.

**Điều 2. Đối tượng áp dụng**

1. Quy chế này áp dụng đối với các cơ quan, đơn vị trên địa bàn tỉnh Kon Tum, bao gồm:

- a) Ủy ban nhân dân tỉnh và các cơ quan chuyên môn trực thuộc;
- b) Ủy ban nhân dân các huyện, thành phố và các phòng, ban chuyên môn trực thuộc;
- c) Ủy ban nhân dân các xã, phường, thị trấn;
- d) Các đơn vị sự nghiệp công lập; các doanh nghiệp nhà nước trên địa bàn tỉnh;
- đ) Các tổ chức, cá nhân có liên quan khi tham gia sử dụng hệ thống thông tin của cơ quan nhà nước, để giao tiếp, cung cấp và trao đổi thông tin số với cơ quan nhà nước.

2. Cán bộ, công chức, viên chức và người lao động đang làm việc tại các đơn vị quy định tại Khoản 1 Điều này.”.

**Điều 3. Mục đích, nguyên tắc đảm bảo an toàn, an ninh thông tin**

1. Việc áp dụng Quy chế này nhằm giảm thiểu được các nguy cơ gây mất an toàn thông tin và đảm bảo an ninh thông tin trong quá trình ứng dụng CNTT trong hoạt động của các cơ quan.

2. Các hoạt động ứng dụng CNTT phải tuân theo nguyên tắc đảm bảo an toàn thông tin được quy định tại Điều 41, Nghị định 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ về ứng dụng CNTT trong hoạt động của cơ quan nhà nước.

#### **Điều 4. Giải thích từ ngữ**

Trong quy chế này các từ ngữ dưới đây được hiểu như sau:

1. An toàn thông tin số: là thuật ngữ dùng để chỉ việc bảo vệ thông tin số và các hệ thống thông tin chống lại các nguy cơ tự nhiên, các hành động truy cập, sử dụng, phát tán, phá hoại, sửa đổi và phá hủy bất hợp pháp nhằm bảo đảm cho các hệ thống thông tin thực hiện đúng chức năng, phục vụ đúng đối tượng một cách sẵn sàng, chính xác và tin cậy. Nội dung của an toàn thông tin mạng bao gồm bảo vệ an toàn mạng và hạ tầng thông tin, an toàn máy tính, dữ liệu và ứng dụng và dịch vụ CNTT.

2. Hệ thống thông tin: là một tập hợp và kết hợp các phần cứng, phần mềm, các hệ thống mạng truyền thông được xây dựng và sử dụng để thu thập, tạo, tái tạo, phân phối và chia sẻ các dữ liệu, thông tin, tri thức nhằm phục vụ cho các mục tiêu của tổ chức.

3. An toàn, an ninh thông tin: là đảm bảo thông tin được bảo mật, sẵn sàng và toàn vẹn.

4. Tính tin cậy: là đảm bảo thông tin chỉ có thể được truy cập bởi những người được cấp quyền truy cập.

5. Tính toàn vẹn: là bảo vệ tính chính xác, tính đầy đủ của thông tin và các phương pháp xử lý thông tin.

6. Tính sẵn sàng: là đảm bảo những người được cấp quyền có thể truy cập thông tin và các tài liệu có liên quan ngay khi có nhu cầu.

7. Log File: là một tập tin được tạo ra bởi một máy chủ web hoặc máy chủ proxy có chứa tất cả thông tin về các hoạt động trên máy chủ đó.

8. Firewall (tường lửa): là rào chắn (phần cứng, phần mềm) được lập ra nhằm kiểm soát người dùng mạng Internet truy nhập vào các thông tin không mong muốn và người dùng từ bên ngoài truy nhập trái phép thông tin trong mạng nội bộ.

9. Môi trường mạng bao gồm: Mạng nội bộ (LAN); mạng diện rộng của Ủy ban nhân dân tỉnh, của ngành (WAN); mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước; mạng riêng ảo (VPN), mạng Intranet; mạng Internet.

10. TCVN 7562:2005: Tiêu chuẩn Việt Nam về mã thực hành quản lý an toàn thông tin.

11. TCVN ISO/IEC 27001:2009: Tiêu chuẩn Việt Nam về quản lý an toàn thông tin số.

## **Chương II**

### **QUY ĐỊNH ĐẢM BẢO AN TOÀN THÔNG TIN**

#### **Điều 5. Điều kiện đảm bảo thực hiện nhiệm vụ an toàn, an ninh thông tin**

1. Cán bộ, công chức, viên chức, người sử dụng hệ thống thông tin phải nắm vững các kiến thức cơ bản, quy định pháp luật và nội quy của cơ quan, đơn vị về an toàn, an ninh thông tin.

2. Các cơ quan, đơn vị, tổ chức, doanh nghiệp bố trí cán bộ phụ trách CNTT phải có chuyên ngành phù hợp và được đào tạo, bồi dưỡng kịp thời về chuyên môn đối với lĩnh vực an toàn, an ninh thông tin.

3. Xác định và ưu tiên phân bổ kinh phí cần thiết cho các hoạt động liên quan đến việc bảo vệ hệ thống thông tin, thông qua việc đầu tư các thiết bị tường lửa, các chương trình chống thư rác, virus máy tính trên hệ thống máy chủ, máy trạm và các công tác khác liên quan đến việc bảo đảm an toàn, an ninh thông tin.

4. Cán bộ tham gia đoàn kiểm tra công tác bảo đảm an toàn, an ninh thông tin phải được trang bị đầy đủ những kiến thức và được tập huấn nghiệp vụ về công tác an toàn, an ninh thông tin theo yêu cầu công việc.

5. Các cơ quan, đơn vị cấp sở, ban, ngành, Ủy ban nhân dân các huyện, thành phố phải xây dựng, ban hành quy chế nội bộ về bảo đảm an toàn, an ninh thông tin; phải căn cứ các nội dung của tiêu chuẩn TCVN 7562:2005 và TCVN ISO/IEC 27001:2009;

6. Duy trì và đảm bảo công tác theo dõi, kiểm tra, thống kê, tổng hợp, báo cáo định kỳ và đột xuất; Có hình thức khen thưởng hoặc xử lý kịp thời theo quy định.

#### **Điều 6. Quản lý trang thiết bị và hạ tầng công nghệ thông tin**

1. Đối với phòng máy chủ tại Trung tâm CNTT và Truyền thông tỉnh:

a) Các thiết bị mạng quan trọng như tường lửa (firewall), thiết bị định tuyến (router), hệ thống máy chủ, ... phải được đặt trong phòng máy chủ và có các biện pháp bảo vệ, ngăn chặn xâm nhập trái phép vào phòng máy chủ. Là khu vực hạn chế tiếp cận và được lắp đặt hệ thống camera giám sát. Phòng máy chủ phải có hệ thống máy phát điện, hệ thống lưu điện đủ công suất để đảm bảo duy trì hệ thống thiết bị và máy chủ được liên tục.

b) Chỉ những người có trách nhiệm theo quy định của Thủ trưởng cơ quan mới được phép vào phòng máy chủ. Quá trình vào, ra phòng máy chủ phải được ghi nhận vào nhật ký quản lý phòng máy chủ.

c) Bố trí cán bộ có năng lực chuyên môn cao để quản lý, vận hành phòng máy chủ và duy trì chế độ trực 24/7 để đảm bảo an toàn thông tin mạng.

## 2. Đối với máy chủ:

Cấu hình máy chủ phải đủ mạnh để đáp ứng công việc. Máy chủ của các cơ quan chỉ dùng để triển khai phần mềm hệ thống, các dữ liệu lưu trữ cần thiết và các phần mềm chống virus, ngoài ra không được cài thêm bất cứ phần mềm khác.

## 3. Đối với thiết bị chống sét, phòng cháy, chữa cháy:

Các cơ quan phải lắp đặt thiết bị chống sét, trang bị thiết bị phòng cháy, chữa cháy để bảo vệ các hệ thống công nghệ thông tin.

## 4. Đối với thiết bị chuyển mạch:

Thiết bị chuyển mạch mạng tin học của các cơ quan phải đảm bảo khả năng cung cấp các chức năng quản trị nhằm tăng cường độ an toàn và bảo mật cho hệ thống mạng như: Cung cấp khả năng từ chối các kết nối không mong muốn hay trái phép vào hệ thống và không chế số lượng kết nối vào hệ thống mạng nội bộ thông qua thiết bị chuyển mạch. Phải có ít nhất 01 thiết bị chuyển mạch hỗ trợ định tuyến IP cho mỗi mạng nội bộ, hỗ trợ chức năng điều khiển truy cập, chức năng xác thực thiết bị, xác thực người sử dụng và chức năng bảo mật quản trị mạng.

## 5. Đối với Tường lửa (Firewall):

Các cơ quan phải xây dựng tường lửa đảm bảo các yêu cầu gồm khả năng xử lý được số lượng kết nối đồng thời cao và chịu được thông lượng cao, hỗ trợ các công nghệ mạng riêng ảo thông dụng và có phần cứng mã hoá tích hợp để tăng khả năng mã hoá dữ liệu, cung cấp đầy đủ các cơ chế bảo mật cơ bản, quản lý luồng dữ liệu ra, vào và có khả năng bảo vệ hệ thống trước các loại tấn công từ chối dịch vụ.

6. Trong quá trình đầu tư mua sắm trang thiết bị CNTT, các phần mềm ứng dụng đi kèm cần lưu ý đến xuất xứ hàng hóa để đảm bảo an toàn, an ninh thông tin mạng.

## **Điều 7. Quy định về quản trị phần mềm ứng dụng**

1. Quản lý tài nguyên: Cán bộ quản trị mạng có trách nhiệm kiểm tra, giám sát chức năng chia sẻ thông tin; tổ chức cấp phát tài nguyên trên máy chủ theo danh mục thư mục cho từng phòng/ban; khuyến cáo người dùng cân nhắc việc chia sẻ tài nguyên cục bộ trên máy đang sử dụng, tuyệt đối không được chia sẻ toàn bộ ổ cứng. Khi thực hiện chia sẻ tài nguyên trên máy chủ hoặc trên máy cục bộ phải sử dụng mật khẩu để bảo vệ thông tin.

2. Quản lý đăng nhập hệ thống: Các hệ thống thông tin cần giới hạn số lần đăng nhập vào hệ thống. Hệ thống tự động khoá tài khoản hoặc cô lập tài khoản khi liên tục đăng nhập sai vượt quá số lần quy định. Tổ chức theo dõi, giám sát tất cả các phương tiện đăng nhập từ xa; yêu cầu người sử dụng đặt mật khẩu với độ an toàn cao, giám sát, nhắc nhở, khuyến cáo nên thay đổi mật khẩu thường xuyên.

3. Quản lý tài khoản: Các tài khoản và định danh người dùng trong các hệ thống thông tin, bao gồm: Tạo mới, kích hoạt, sửa đổi và loại bỏ các tài khoản, đồng thời tổ chức kiểm tra các tài khoản của hệ thống thông tin ít nhất 6 tháng/lần thông qua các công cụ của hệ thống. Hủy tài khoản, quyền truy cập hệ thống đối với cán bộ, công chức đã chuyển công tác hoặc thôi việc.

4. Quản lý nhật ký (log file): Hệ thống thông tin phải ghi nhận các sự kiện như: Quá trình đăng nhập vào hệ thống, các thao tác cấu hình hệ thống. Thường xuyên kiểm tra, sao lưu các log file theo từng tháng để lưu vết theo dõi, xác định những sự kiện đã xảy ra của hệ thống và hạn chế việc tràn log file gây ảnh hưởng đến hoạt động của hệ thống.

5. Phòng chống mã độc, virus: Trên các máy chủ, các thiết bị di động trong mạng và hệ thống thông tin phải cài đặt phần mềm chống virus, thư rác phù hợp để phát hiện, loại trừ mã độc, virus và cài đặt các phần mềm này trên máy trạm.

6. Quản lý cài đặt: Cán bộ, công chức, viên chức không được tự ý cài đặt thêm chương trình khác trên máy tính cá nhân nhằm tránh sự lây lan của virus. Cán bộ chuyên trách CNTT có trách nhiệm kiểm tra, cài đặt và chịu trách nhiệm về mức độ an toàn, bảo mật các phần mềm ứng dụng phục vụ công tác chuyên ngành tại các máy tính công vụ của cán bộ, công chức, viên chức.

7. Xung đột phần mềm: Trong quá trình thiết kế, nâng cấp các phần mềm chuyên ngành phải đảm bảo tương thích và tích hợp được với các phần mềm dùng chung đảm bảo tránh được các xung đột và gây mất an toàn thông tin.

### **Điều 8. Bảo vệ bí mật nhà nước trong hoạt động ứng dụng CNTT**

1. Quy định về soạn thảo, in ấn, phát hành và sao chụp tài liệu mật:

a) Không được sử dụng máy tính nối mạng internet để soạn thảo văn bản, chuyển giao, lưu trữ thông tin có nội dung thuộc bí mật nhà nước; cung cấp tin, tài liệu và đưa thông tin bí mật nhà nước trên Cổng/Trang thông tin điện tử.

b) Không được in, sao chụp tài liệu bí mật nhà nước trên các thiết bị kết nối mạng internet.

2. Khi sửa chữa, khắc phục các sự cố của máy tính dùng soạn thảo văn bản mật, các cơ quan phải báo cáo cho cơ quan có thẩm quyền. Không được cho phép các công ty tư nhân hoặc người không có trách nhiệm trực tiếp sửa chữa, xử lý, khắc phục sự cố.

3. Trước khi thanh lý các máy tính trong các cơ quan nhà nước, cán bộ phụ trách CNTT phải dùng các biện pháp kỹ thuật xóa bỏ vĩnh viễn dữ liệu trong ổ cứng máy tính.

### **Điều 9. Quản lý, vận hành hệ thống thông tin của đơn vị**

1. Hệ thống thông tin của các cơ quan, đơn vị phải có cơ chế sao lưu dữ liệu ở mức hệ thống, dữ liệu của các ứng dụng, dữ liệu của người sử dụng; cơ chế sao lưu dữ liệu phải được thực hiện thường xuyên; thiết bị lưu trữ dữ liệu

được sao lưu phải đảm bảo yêu cầu kỹ thuật; dữ liệu được sao lưu phải đảm bảo tính sẵn sàng và toàn vẹn đáp ứng yêu cầu phục hồi dữ liệu cho hệ thống thông tin hoạt động bình thường khi có sự cố xảy ra.

2. Hệ thống thông tin của các cơ quan, đơn vị phải được triển khai cơ chế bảo mật, an toàn thông tin bằng các thiết bị phần cứng và phần mềm phù hợp với quy mô của đơn vị.

3. Hệ thống thông tin của đơn vị phải được triển khai chức năng giám sát truy cập từ ngoài vào hệ thống, từ hệ thống gửi ra bên ngoài; ghi lại nhật ký (log file) ra, vào hệ thống để phục vụ công tác khắc phục sự cố, điều tra, phân tích và làm rõ các nguy cơ gây ra mất an toàn, an ninh thông tin; chức năng không cho người dùng truy cập một số website không phù hợp với quy định hiện hành.

4. Hệ thống mạng không dây (wireless) của các cơ quan, đơn vị phải được thiết lập khoá khi truy cập tối thiểu 8 ký tự.

5. Mạng riêng ảo (VPN) của các cơ quan, đơn vị kết nối để truy cập vào hệ thống thông tin phải được bảo mật; quản lý và kiểm soát chặt chẽ các kết nối; hủy bỏ kết nối khi không còn sử dụng.

6. Tất cả các tài khoản truy cập vào hệ thống máy chủ, thiết bị mạng, máy tính, các ứng dụng phải được thiết lập mật khẩu; mật khẩu phải được đặt ở mức bảo mật cao (*số lượng ký tự và nội dung của mật khẩu*); mật khẩu có tối thiểu 6 ký tự bao gồm chữ hoa, chữ thường, chữ số và ký tự đặc biệt; phải thường xuyên thay đổi mật khẩu với tần suất phù hợp; danh sách tài khoản phải được quản lý, kiểm tra và cập nhật kịp thời; quyền truy cập của tài khoản phải được thiết lập phù hợp cho từng đối tượng.

#### **Điều 10. Quyền hạn, nhiệm vụ của cán bộ phụ trách CNTT của cơ quan, đơn vị, tổ chức, doanh nghiệp**

1. Được đảm bảo điều kiện về đào tạo, bồi dưỡng, học tập, nghiên cứu, tiếp thu kiến thức, kỹ thuật và công nghệ mới đối với lĩnh vực an toàn, an ninh thông tin.

2. Quản lý chặt chẽ việc di chuyển các trang thiết bị CNTT lưu trữ các thông tin thuộc danh mục bí mật nhà nước.

3. Thực hiện cấp phát, thu hồi, cập nhật và quản lý tất cả các tài khoản truy cập vào hệ thống thông tin của đơn vị; hướng dẫn người sử dụng thay đổi mật khẩu ngay sau khi đăng nhập lần đầu tiên; bảo vệ thông tin của tài khoản theo quy định.

4. Triển khai áp dụng các giải pháp tổng thể đảm bảo an toàn, an ninh thông tin mạng trong toàn hệ thống; triển khai các giải pháp kỹ thuật phòng chống virus, mã độc hại, thư rác cho hệ thống và máy tính cá nhân; kiểm soát và có giải pháp kỹ thuật chống truy cập trái phép vào hệ thống thông tin.

5. Thường xuyên cập nhật các bản vá lỗi đối với hệ thống, cập nhật các phiên bản mới đối với chương trình chống virus.



6. Thường xuyên sao lưu dữ liệu theo quy định; kiểm tra dữ liệu sao lưu phải đảm bảo tính sẵn sàng, tin cậy và toàn vẹn.

7. Thường xuyên thực hiện phân tích, đánh giá và báo cáo các rủi ro và nguy cơ gây mất an toàn, an ninh thông tin đối với hệ thống thông tin của đơn vị; nguyên nhân gây ra các rủi ro và nguy cơ gây mất an toàn, an ninh thông tin mạng bao gồm: Hiện tượng tự nhiên (nhiệt độ, không khí, mưa bão, sét), truy cập trái phép, virus, cố ý làm thay đổi thông số cấu hình hệ thống và phá hủy dữ liệu. Đồng thời tham mưu và xây dựng phương án hạn chế, khắc phục các rủi ro và nguy cơ có thể xảy ra.

### **Chương III**

## **TRÁCH NHIỆM ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN MẠNG**

### **Điều 11. Trách nhiệm của các cơ quan, đơn vị**

1. Người đứng đầu các cơ quan, đơn vị, địa phương chịu trách nhiệm trong công tác đảm bảo an toàn, an ninh thông tin đối với toàn bộ hệ thống thông tin mạng của cơ quan, đơn vị, địa phương mình.

2. Thực hiện và chỉ đạo cán bộ, công chức thuộc thẩm quyền quản lý thực hiện nghiêm túc Quy định này.

3. Tạo điều kiện thuận lợi cho cán bộ phụ trách về CNTT được đào tạo, bồi dưỡng chuyên môn trong lĩnh vực an toàn, an ninh thông tin mạng.

4. Quan tâm đầu tư các thiết bị phần cứng, phần mềm liên quan đến công tác đảm bảo an toàn, an ninh thông tin.

5. Khi có sự cố hoặc nguy cơ mất an toàn, an ninh thông tin mạng phải chỉ đạo khắc phục sự cố kịp thời và hạn chế thấp nhất mức thiệt hại có thể xảy ra, ưu tiên sử dụng lực lượng kỹ thuật tại chỗ của đơn vị mình, đồng thời lập biên bản và báo cáo bằng văn bản cho cơ quan có liên quan.

6. Tạo điều kiện thuận lợi cho các cơ quan chức năng trong công tác điều tra, làm rõ nguyên nhân gây ra sự cố; lực lượng kỹ thuật tham gia khắc phục sự cố thực hiện đúng theo hướng dẫn chuyên môn của Sở Thông tin và Truyền thông.

### **Điều 12. Trách nhiệm của Sở Thông tin và Truyền thông**

1. Chịu trách nhiệm toàn diện trước Ủy ban nhân dân tỉnh về công tác đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng CNTT của các cơ quan nhà nước trên phạm vi toàn tỉnh.

2. Chủ trì, phối hợp với các đơn vị liên quan tham mưu Ủy ban nhân dân tỉnh ban hành:

a) Văn bản chỉ đạo, kế hoạch, đề án nhằm đảm bảo an toàn, an ninh thông tin.

b) Xây dựng tiêu chuẩn đánh giá mức độ an toàn, an ninh thông tin đối với hệ thống thông tin của các đơn vị.

c) Xây dựng Danh mục các loại phần mềm được phép triển khai cài đặt tại Trung tâm dữ liệu (*đặt tại Trung tâm Công nghệ thông tin và Truyền thông*) để đảm bảo sử dụng Hạ tầng chung chung và Cơ sở dữ liệu tập trung. Danh mục các phần mềm chuyên ngành, phần mềm thương mại được phép cài đặt trên máy tính của cán bộ, công chức, viên chức để đảm bảo an toàn, an ninh thông tin và tiết kiệm ngân sách nhà nước.

d) Xây dựng Quy định danh mục các phần mềm bắt buộc vận hành trong hệ thống mạng WAN của tỉnh và danh mục những phần mềm có thể triển khai trên hệ thống mạng Internet.

đ) Thành lập đoàn kiểm tra liên ngành về đảm bảo an toàn, an ninh thông tin mạng trong hoạt động ứng dụng công nghệ thông tin trong các cơ quan nhà nước.

3. Hàng năm, tổ chức đào tạo chuyên sâu về an toàn, an ninh thông tin mạng cho lực lượng đảm bảo an toàn, an ninh thông tin mạng của các cơ quan, đơn vị.

4. Thực hiện nhiệm vụ cảnh báo về nguy cơ hoặc sự cố mất an toàn, an ninh thông tin.

5. Tổ chức Hội nghị, Hội thảo chuyên đề về an toàn, an ninh thông tin.

6. Phối hợp với Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) và các đơn vị có liên quan trong thực hiện nhiệm vụ đảm bảo an toàn, an ninh thông tin mạng.

7. Phối hợp với Công an tỉnh và các cơ quan, đơn vị có liên quan tổ chức đoàn kiểm tra về an toàn, an ninh thông tin mạng để kịp thời phát hiện, xử lý các hành vi vi phạm theo thẩm quyền quy định.

8. Chủ động hướng dẫn các cơ quan, đơn vị xây dựng quy chế nội bộ, hỗ trợ kỹ thuật, nội dung, thời gian báo cáo công tác đảm bảo an toàn, an ninh thông tin.

9. Tổng hợp báo cáo và thông báo về tình hình an toàn, an ninh thông tin mạng theo định kỳ cho Bộ Thông tin và Truyền thông, Ủy ban nhân dân tỉnh và các cơ quan, đơn vị có liên quan.

10. Tổ chức thực hiện việc tiếp nhận và xử lý, khắc phục các sự cố về an toàn, an ninh thông tin. Cụ thể:

a) Quyết định toàn diện về mặt kỹ thuật đối với các cơ quan, đơn vị trong quá trình khắc phục sự cố về an toàn, an ninh thông tin.

b) Chỉ đạo các đơn vị trực thuộc nhanh chóng hỗ trợ, phối hợp và hướng dẫn các cơ quan, đơn vị khắc phục sự cố mất an toàn, an ninh thông tin.

c) Yêu cầu ngưng hoạt động một phần hoặc toàn bộ các hệ thống thông tin của các cơ quan, đơn vị nhằm phục vụ công tác khắc phục sự cố về an toàn, an ninh thông tin.

d) Phối hợp với Công an tỉnh trong điều tra làm rõ các nguyên nhân gây ra sự cố mất an toàn, an ninh thông tin.

đ) Trong trường hợp sự cố xảy ra có phạm vi rộng, ảnh hưởng và liên quan đến nhiều ngành, nhiều lĩnh vực phải thông báo khẩn cấp và xin ý kiến chỉ đạo của Ủy ban nhân dân tỉnh, Bộ Thông tin và Truyền thông.

### **Điều 13. Trách nhiệm của Công an tỉnh**

1. Tham mưu cho cấp ủy, lãnh đạo các cơ quan Đảng, Nhà nước trên địa bàn tỉnh Kon Tum công tác chỉ đạo, tổ chức triển khai, thực hiện các Chỉ thị, Nghị quyết của Đảng, pháp luật của Nhà nước về công tác đảm bảo an toàn, an ninh thông tin mạng.

2. Chủ trì, phối hợp với Sở Thông tin và Truyền thông và các cơ quan, đơn vị có liên quan xây dựng kế hoạch và chịu trách nhiệm kiểm soát, phòng ngừa, đấu tranh, ngăn chặn các loại tội phạm lợi dụng hệ thống thông tin gây hại đến an toàn, an ninh thông tin trong cơ quan nhà nước. Phối hợp với các cơ quan chức năng trong trao đổi biện pháp kỹ thuật, kiểm tra, đánh giá nhằm đảm bảo an toàn, an ninh thông tin.

3. Tăng cường công tác phòng ngừa, phát hiện và tuyên truyền, phổ biến pháp luật về xử lý tội phạm trong việc đảm bảo an toàn, an ninh thông tin. Điều tra và xử lý các trường hợp vi phạm pháp luật về an toàn, an ninh thông tin theo thẩm quyền.

4. Thực hiện nhiệm vụ bảo vệ an toàn các công trình quan trọng về an ninh quốc gia trong lĩnh vực CNTT trên địa bàn tỉnh.

### **Điều 14. Trách nhiệm của cán bộ, công chức, viên chức và người lao động tại các cơ quan, đơn vị**

1. Trách nhiệm của cán bộ chuyên trách công nghệ thông tin:

a) Chịu trách nhiệm triển khai các biện pháp quản lý vận hành, quản lý kỹ thuật và tham mưu xây dựng các quy định về đảm bảo an toàn, an ninh thông tin mạng cho toàn bộ hệ thống thông tin của đơn vị mình đúng theo nội dung Quy định này.

b) Chủ động phối hợp với cá nhân, đơn vị có liên quan trong việc kiểm tra, phát hiện và khắc phục sự cố về an toàn, an ninh thông tin.

c) Tuân thủ theo sự hướng dẫn kỹ thuật của Sở Thông tin và Truyền thông trong quá trình khắc phục sự cố về an toàn, an ninh thông tin. Khi phát hiện hệ thống nội bộ bị tấn công, thông qua các dấu hiệu như luồng tin (traffic) tăng lên bất ngờ, nội dung bị thay đổi, hệ thống hoạt động chậm bất thường cần thực hiện các bước cơ bản sau:

Bước 1: Ngắt kết nối máy chủ ra khỏi mạng;

Bước 2: Sao chép nhật ký (log file) và toàn bộ dữ liệu của hệ thống ra thiết bị lưu trữ;

Bước 3: Khôi phục lại hệ thống bằng cách chuyển dữ liệu sao lưu mới nhất để hệ thống hoạt động trở lại bình thường.

Lập biên bản ghi nhận sự cố gây ra mất an toàn, an ninh thông tin đối với hệ thống thông tin của cơ quan, đơn vị; đồng thời thu thập các chứng cứ, dấu vết và nguyên nhân gây ra sự cố (nếu có); đồng thời báo cáo sự cố và kết quả khắc phục sự cố cho Thủ trưởng cơ quan, đơn vị.

d) Trong trường hợp phát hiện sự cố xảy ra ngoài khả năng giải quyết của cơ quan (Hệ thống lưu trữ tại Trung tâm Thông tin dữ liệu điện tử), đơn vị phải báo cáo ngay cho cơ quan cấp trên quản lý trực tiếp và Sở Thông tin và Truyền thông để được hỗ trợ, hướng dẫn và phối hợp khắc phục sự cố; đồng thời tham mưu văn bản báo cáo sự cố gửi Sở Thông tin và Truyền thông, Công an tỉnh và các đơn vị có liên quan.

**2. Trách nhiệm của cán bộ, công chức, viên chức và người lao động tham gia sử dụng và khai thác hệ thống thông tin:**

a) Nghiêm túc chấp hành các quy định, quy trình nội bộ, Quy chế này và các quy định khác của pháp luật về an toàn thông tin. Chịu trách nhiệm đảm bảo an toàn thông tin trong phạm vi trách nhiệm và quyền hạn được giao

b) Quản lý chặt chẽ việc di chuyển các trang thiết bị CNTT lưu trữ các thông tin thuộc danh mục bí mật nhà nước.

c) Khi phát hiện nguy cơ hoặc sự cố mất an toàn, an ninh thông tin mạng phải báo cáo kịp thời cho cán bộ chuyên trách CNTT của đơn vị mình để kịp thời ngăn chặn và xử lý. Phối hợp tích cực trong suốt quá trình giải quyết và khắc phục sự cố.

**Điều 15. Trách nhiệm của các doanh nghiệp cung cấp hạ tầng mạng và dịch vụ Internet.**

Các doanh nghiệp cung cấp hạ tầng mạng viễn thông và dịch vụ internet phải thiết lập đầu mối liên lạc để phối hợp và tuân thủ việc điều phối của cơ quan chức năng và tham gia vào công tác ứng cứu, khắc phục sự cố cho hệ thống thông tin quan trọng của tỉnh.

## **Chương IV TỔ CHỨC THỰC HIỆN**

**Điều 16. Công tác kiểm tra, giám sát**

**1.** Hàng năm, Sở Thông tin và Truyền thông chủ trì, phối hợp với Công an tỉnh và các đơn vị có liên quan tham mưu Ủy ban nhân dân tỉnh thành lập đoàn kiểm tra, giám sát tình hình thực hiện công tác đảm bảo an toàn, an ninh thông tin đối với các đơn vị, địa phương theo quy định. Đồng thời, tiến hành kiểm tra đột xuất các cơ quan, đơn vị khi phát hiện có dấu hiệu vi phạm an toàn, an ninh thông tin theo đúng quy định của pháp luật.

2. Công an tỉnh cử cán bộ phối hợp, tham gia đoàn kiểm tra, đánh giá công tác đảm bảo an toàn, an ninh thông tin mạng trong các cơ quan, đơn vị; điều tra và xử lý các trường hợp vi phạm các quy định về an toàn, an ninh thông tin mạng theo thẩm quyền;

3. Các cơ quan liên quan được mời tham gia đoàn kiểm tra: Cử cán bộ có chuyên môn về công nghệ thông tin tham gia đoàn kiểm tra do Sở Thông tin và Truyền thông tổ chức; phối hợp với đoàn kiểm tra xây dựng các tiêu chí và quy trình kỹ thuật kiểm tra công tác đảm bảo an toàn, an ninh thông tin.

4. Các đơn vị, địa phương chủ động tiến hành kiểm tra và báo cáo khi phát hiện có dấu hiệu vi phạm pháp luật về an toàn, an ninh thông tin trong hệ thống thông tin của đơn vị thuộc quyền quản lý theo đúng quy định của pháp luật.

### **Điều 17. Khen thưởng và xử lý vi phạm**

1. Hằng năm, Sở Thông tin và Truyền thông dựa trên các điều tra, báo cáo công tác an toàn, an ninh thông tin của các cơ quan, đơn vị để xác lập bảng xếp hạng an toàn, an ninh thông tin, trên cơ sở đó đề xuất Ủy ban nhân dân tỉnh xem xét khen thưởng theo quy định hiện hành.

2. Các cơ quan, đơn vị có hành vi vi phạm Quy chế này tùy theo tính chất, mức độ vi phạm mà bị xử lý theo quy định của pháp luật hiện hành.

### **Điều 18. Điều khoản thi hành**

1. Thủ trưởng các Sở, Ban, Ngành; Chủ tịch Ủy ban nhân dân các huyện, thành phố chịu trách nhiệm tổ chức triển khai thực hiện Quy chế tại đơn vị mình.

2. Sở Kế hoạch và Đầu tư, Sở Tài chính phối hợp Sở Thông tin và Truyền thông ưu tiên bố trí kinh phí thực hiện các nhiệm vụ đảm bảo an toàn thông tin của tỉnh.

3. Trong quá trình thực hiện, nếu có những vấn đề cần sửa đổi, bổ sung, đề nghị các đơn vị gửi về Sở Thông tin và Truyền thông để tổng hợp, báo cáo Ủy ban nhân dân tỉnh xem xét, quyết định./.

TM. ỦY BAN NHÂN DÂN  
CHỦ TỊCH



**Đào Xuân Quý**