| ỦY BAN NHÂN DÂN<br>TỈNH QUẢNG TRỊ | CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM<br>Độc lập - Tự do - Hạnh phúc |
|---|---|
| Số: 35/2016/QĐ-UBND | *Quảng Trị, ngày 29 tháng 8 năm 2016* |

# QUYẾT ĐỊNH
## 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 tỉnh Quảng Trị

## ỦY BAN NHÂN DÂN TỈNH QUẢNG TRỊ

*Căn cứ Luật Tổ chức chính quyền địa phương ngày 19 tháng 6 năm 2015;*

*Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015; Luật Giao dịch điện tử ngày 29 tháng 11 năm 2005; Luật Công nghệ thông tin ngày 29 tháng 6 năm 2006; Luật Ban hành văn bản quy phạm pháp luật của HĐND, UBND ngày 03 tháng 12 năm 2004;*

*Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động cơ quan nhà nước;*

*Xét đề nghị của Giám đốc Sở Thông tin và Truyền thông.*

## 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 tỉnh Quảng Trị.

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

Chánh Văn phòng UBND tỉnh; Giám đốc các Sở, Thủ trưởng các Ban ngành cấp tỉnh; Chủ tịch UBND các huyện, thị xã, thành phố và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

**TM. ỦY BAN NHÂN DÂN**
**CHỦ TỊCH**

**Nguyễn Đức Chính**

| ỦY BAN NHÂN DÂN<br>TỈNH QUẢNG TRỊ | CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM<br>Độc lập - Tự do - Hạnh phúc |
|---|---|

# 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 tỉnh Quảng Trị

*(Ban hành kèm theo Quyết định số 35/2016/QĐ-UBND ngày 29 tháng 8 năm 2016 của UBND tỉnh Quảng Trị)*

## Chương I
## QUY ĐỊNH CHUNG

### Điều 1. Phạm vi điều chỉnh

Quy chế này quy định về việc đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin (CNTT) của các cơ quan nhà nước tỉnh Quảng Trị, bao gồm: công tác quản lý đảm bảo an toàn, an ninh thông tin mạng; việc áp dụng các biện pháp quản lý kỹ thuật, quản lý vận hành đảm bảo an toàn, an ninh thông tin đối với các hệ thống thông tin.

### Điều 2. Đối tượng áp dụng

1. Quy chế này được áp dụng đối với các cơ quan nhà nước trên địa bàn tỉnh Quảng Trị, bao gồm: các cơ quan chuyên môn thuộc UBND tỉnh và các đơn vị sự nghiệp trực thuộc; các đơn vị sự nghiệp thuộc tỉnh; UBND các huyện, thị xã, thành phố; UBND các xã, phường, thị trấn (sau đây gọi tắt là cơ quan, đơn vị).

2. Cán bộ, công chức, viên chức đang làm việc trong các cơ quan, đơn vị nêu tại Khoản 1 Điều này và những cá nhân, tổ chức có liên quan áp dụng Quy định này trong việc vận hành, khai thác hệ thống thông tin tại các cơ quan, đơn vị.

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

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 hoạt động ứng dụng CNTT của các cơ quan, đơn vị.

Các hoạt động ứng dụng công nghệ thông tin phải tuân theo nguyên tắc đảm bảo an toàn thông tin được quy định tại Điều 4, Luật An toàn thông tin mạng; Điều 41, Nghị định 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.

### 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 công nghệ thông tin.

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: 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 UBND 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 AN NINH THÔNG TIN

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

1. Các cơ quan, đơn vị phải phổ biến những kiến thức cơ bản về an toàn, an ninh thông tin cho cán bộ, công chức, viên chức trước khi tham gia sử dụng các hệ thống thông tin.

2. Các cơ quan, đơn vị bố trí cán bộ, công chức, viên chức làm công tác chuyên trách hoặc phụ trách kiêm nhiệm về công nghệ thông tin phải thường xuyên được đào tạo, bồi dưỡng nghiệp vụ về 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, công chức, viên chức tham gia đoàn kiểm tra công tác đảm bảo an toàn, an ninh thông tin phải được trang bị đầy đủ những kiến thức và được tập huấn hàng năm về công tác đảm bảo an toàn, an ninh thông tin.

**Điều 6. Xây dựng quy chế nội bộ về đảm bảo an toàn, an ninh thông tin**

Các cơ quan, đơn vị phải xây dựng, ban hành quy chế nội bộ về đảm bảo an toàn, an ninh thông tin; phải căn cứ các nội dung của tiêu chuẩn TCVN 7562:2005 và TCVN ISO/IEC 27001:2009 để quy định rõ các vấn đề sau:

a) Mục tiêu, phạm vi, đối tượng áp dụng:

Quy định rõ mục tiêu, phạm vi, đối tượng áp dụng của quy chế nội bộ: Phòng ban chuyên môn và đơn vị trực thuộc.

b) Nội dung bảo đảm an toàn thông tin:

- Nêu rõ các biện pháp quản lý kỹ thuật cơ bản cho công tác an toàn thông tin;

- Nêu rõ các biện pháp quản lý vận hành trong công tác an toàn thông tin;

c) Quy định cụ thể quyền và trách nhiệm của từng đối tượng:

- Quyền và trách nhiệm của lãnh đạo đơn vị;

- Quyền và trách nhiệm của lãnh đạo cấp phòng;

- Quyền và trách nhiệm của cán bộ, công chức, viên chức làm công tác chuyên trách về công nghệ thông tin (CNTT);

- Quyền và trách nhiệm của cán bộ, công chức, viên chức thực hiện công tác đảm bảo an toàn thông tin;

- Quyền và trách nhiệm của người sử dụng.

d) Quy định về cấp phát, thu hồi, cập nhật và quản lý các tài khoản truy cập vào hệ thống thông tin:

- Nêu rõ quy định về cấp phát, thu hồi, cập nhật và quản lý các tài khoản truy cập vào từng hệ thống thông tin.

đ) Quy định về công tác bảo vệ bí mật nhà nước về an toàn thông tin trên môi trường mạng.

e) Cơ chế sao lưu dữ liệu, cơ chế thông tin, báo cáo và phối hợp khắc phục sự cố:

- Nêu rõ cơ chế sao lưu dữ liệu, cơ chế thông tin;

- Nêu rõ nội dung báo cáo và phối hợp khắc phục sự cố.

g) Theo dõi, kiểm tra, thống kê, tổng hợp, báo cáo theo định kỳ và đột xuất:

- Nêu rõ việc theo dõi, thời gian kiểm tra các hệ thống thông tin;

- Nêu rõ việc thống kê, tổng hợp, báo cáo theo định kỳ và đột xuất.

h) Khen thưởng, kỷ luật:

- Các hình thức khen thưởng, kỷ luật.

i) Tổ chức thực hiện:

- Cách thức tổ chức thực hiện.

**Điều 7. Trang thiết bị và hạ tầng công nghệ thông tin**

1. Phòng máy chủ của các cơ quan, đơn vị:

- 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 hoạt động liên tục;

- 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;

- Bố trí cán bộ, công chức, viên chức 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. 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. 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. Thiết bị chuyển mạch (Switch):

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 khống 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. 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 hóa tích hợp để tăng khả năng

mã hóa 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 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 8. Quy định về quản trị phần mềm ứng dụng**

Trong quá trình đầu tư, thiết kế, xây dựng, nâng cấp các phần mềm hệ thống, các phần mềm ứng dụng dùng chung trong các cơ quan nhà nước phải đáp ứng yêu cầu quản trị, vận hành đảm bảo an toàn, an ninh thông tin mạng.

1. Quản lý tài nguyên: Cán bộ, công chức, viên chức làm công tác 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 khóa 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, viên 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 làm công tác 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 9. 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 theo danh mục quy định; 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, công chức, viên chức làm công tác chuyên trách công nghệ thông tin phải dùng các biện pháp kỹ thuật xoá bỏ vĩnh viễn dữ liệu trong ổ cứng máy tính.

**Điều 10. Quản lý, vận hành hệ thống thông tin của cơ quan, 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 các cơ quan, đơn vị (như hệ thống thư điện tử, hệ thống thông tin điều hành tác nghiệp nội bộ…) phải có cơ chế giới hạn một số hữu hạn lần đăng nhập sai liên tiếp. Nếu liên tục đăng nhập sai vượt quá số lần quy định thì hệ thống sẽ tự động khóa hoặc cô lập tài khoản trong một khoảng thời gian nhất định trước khi tiếp tục cho đăng nhập.

4. Hệ thống thông tin của các cơ quan, 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.

5. Hệ thống mạng không dây (Wireless) của các cơ quan, đơn vị phải được thiết lập khóa khi truy cập với tối thiểu 8 ký tự. Phải triển khai các giải pháp phòng chống xâm nhập, tấn công mạng WLAN (mạng cục bộ không dây) của các cơ quan, đơn vị.

6. 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.

7. 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 8 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; quyền truy cập của tài khoản phải được thiết lập phù hợp cho từng đối tượng.

**Điều 11. Cán bộ, công chức, viên chức làm công tác chuyên trách về công nghệ thông tin của cơ quan, đơn vị**

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 công nghệ thông tin 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.

**Điều 12. Giải quyết và khắc phục sự cố an toàn, an ninh thông tin**

1. Đối với người sử dụng:

a) Thông tin, báo cáo kịp thời cho cán bộ, công chức, viên chức làm công tác chuyên trách về CNTT của cơ quan, đơn vị khi phát hiện các sự cố gây mất an toàn, an ninh thông tin mạng trong quá trình tham gia vào hệ thống thông tin của đơn vị;

b) Phối hợp tích cực trong suốt quá trình giải quyết và khắc phục sự cố.

2. Đối với cán bộ, công chức, viên chức làm công tác chuyên trách về công nghệ thông tin:

a) Xử lý khẩn cấp: 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.

b) Trong trường hợp phát hiện sự cố xảy ra ngoài khả năng giải quyết của cơ quan, 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.

3. Sở Thông tin và Truyền thông:

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 Trung tâm CNTT và Truyền thông 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 hệ thống thông tin của các cơ quan, đơn vị nhằm phục vụ công tác khắc phục sự cố 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;

e) 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 UBND tỉnh, Bộ Thông tin và Truyền thông.

## Chương III
## TRÁCH NHIỆM ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

### Điều 13. Trách nhiệm của Sở Thông tin và Truyền thông

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

2. Thực hiện công tác tham mưu UBND tỉnh ban hành:

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

b) 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 cán bộ, công chức, viên chức; nhất là đối tượng cán bộ, công chức, viên chức làm công tác chuyên trách CNTT nhằm 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, UBND tỉnh và các cơ quan, đơn vị có liên quan.

10. Tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin.

**Điều 14. Trách nhiệm của các cơ quan, đơn vị**

1. Thủ trưởng các cơ quan, đơn vị có trách nhiệm tuyên truyền, nâng cao nhận thức cho cán bộ, công chức, viên chức về các nguy cơ mất an toàn, an ninh hệ thống thông tin; tổ chức triển khai thực hiện các quy định tại Quy chế này và chịu trách nhiệm trước UBND tỉnh trong công tác đảm bảo an toàn, an ninh thông tin của cơ quan, đơn vị mình.

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

3. Cử cán bộ, công chức, viên chức làm công tác chuyên trách về công nghệ thông tin tham gia các khóa đào tạo, bồi dưỡng chuyên môn trong lĩnh vực an toàn, an ninh thông tin mạng.

4. 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 thông tin phải kịp thời chỉ đạo khắc phục ngay; ưu tiên sử dụng cán bộ, công chức, viên chức làm công tác kỹ thuật chuyên trách trong cơ quan, đơn vị và thông báo bằng văn bản cho Sở Thông tin và

Truyền thông, cơ quan cấp trên quản lý trực tiếp biết. Trường hợp không khắc phục được thì phối hợp với Sở Thông tin và Truyền thông hoặc cơ quan cấp trên quản lý để được hướng dẫn, hỗ trợ.

6. Phối hợp chặt chẽ với cơ quan Công an trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động vi phạm an toàn, an ninh thông tin. Tạo điều kiện thuận lợi cho các cơ quan chức năng tham gia khắc phục sự cố và thực hiện đúng theo hướng dẫn.

7. Phối hợp với đoàn kiểm tra để triển khai công tác kiểm tra khắc phục sự cố; đồng thời cung cấp đầy đủ các thông tin khi đoàn kiểm tra yêu cầu.

8. Báo cáo tình hình và kết quả thực hiện công tác đảm bảo an toàn, an ninh thông tin tại cơ quan, đơn vị và gửi về Sở Thông tin và Truyền thông định kỳ hàng năm (trước ngày 15 tháng 12).

**Điều 15. Trách nhiệm của cán bộ, công chức, viên chức trong các cơ quan, đơn vị**

1. Trách nhiệm của cán bộ, công chức, viên chức làm công tác 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 theo nội dung Quy chế 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.

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

a) Nghiêm túc thực hiện các nội quy, quy chế, quy trình nội bộ về đảm bảo an toàn, an ninh thông tin mạng của đơn vị cũng như các quy định khác của pháp luật về nội dung này;

b) Khi phát hiện nguy cơ hoặc sự cố mất an toàn, an ninh thông tin mạng phải báo cáo kịp thời cho cán bộ, công chức, viên chức làm công tác chuyên trách công nghệ thông tin của đơn vị mình để kịp thời ngăn chặn và xử lý;

c) Nâng cao ý thức cảnh giác và trách nhiệm về an toàn, an ninh thông tin.

## Chương IV
## KIỂM TRA CÔNG TÁC ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

**Điều 16. Kế hoạch kiểm tra hàng năm**

1. Sở Thông tin và Truyền thông chủ trì, phối hợp với Công an tỉnh và các đơn vị có liên quan tiến hành kiểm tra công tác đảm bảo an toàn, an ninh thông tin định kỳ hàng năm đối với các cơ quan, đơn vị.

2. 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.

**Điều 17. Quan hệ phối hợp và trách nhiệm của các ngành liên quan**

1. Sở Thông tin và Truyền thông có trách nhiệm:

a) Chủ trì, phối hợp với các cơ quan chức năng liên quan để thành lập Đoàn kiểm tra công tác đảm bảo an toàn, an ninh thông tin, triển khai và báo cáo kết quả kiểm tra cho UBND tỉnh;

b) Tuyên truyền công tác an toàn, an ninh thông tin cho các cơ quan, đơn vị trên địa bàn tỉnh.

2. Công an tỉnh có trách nhiệm:

a) Phối hợp Sở Thông tin và Truyền thông kiểm tra công tác an toàn, an ninh thông tin;

b) Điều tra và xử lý các trường hợp vi phạm an toàn, an ninh thông tin theo thẩm quyền.

3. Trách nhiệm các cơ quan liên quan:

a) Cử cán bộ, công chức, viên chức chuyên trách tham gia Đoàn kiểm tra, đánh giá công tác an toàn, an ninh thông tin khi có yêu cầu;

b) Phối hợp xây dựng các tiêu chí và quy trình kỹ thuật kiểm tra công tác an toàn, an ninh thông tin trên địa bàn tỉnh.

## Chương V
## TỔ CHỨC THỰC HIỆN

**Điều 18. Khen thưởng và xử lý vi phạm**

1. Hàng 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 lập bảng xếp hạng an toàn, an ninh thông tin, đề xuất UBND tỉnh xem xét khen thưởng theo quy định.

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

**Điều 19. Điều khoản thi hành**

Sở Thông tin và Truyền thông hướng dẫn triển khai thực hiện Quy chế này.

Trong quá trình thực hiện, nếu có vướng mắc, phát sinh, các cơ quan, đơn vị kịp thời phản ánh về Sở Thông tin và Truyền thông để tổng hợp, báo cáo UBND tỉnh xem xét sửa đổi, bổ sung Quy chế cho phù hợp./.

**TM. ỦY BAN NHÂN DÂN**
**CHỦ TỊCH**

**Nguyễn Đức Chính**

**Phụ lục số I**

**CÁC BƯỚC CƠ BẢN ĐỂ XÂY DỰNG KHUNG QUY CHẾ NỘI BỘ ĐẢM BẢO AN TOÀN THÔNG TIN TRONG HOẠT ĐỘNG ỨNG DỤNG CÔNG NGHỆ THÔNG TIN**

*(Ban hành kèm theo Quyết định số 35/2016/QĐ-UBND ngày 29 tháng 8 năm 2016 của UBND tỉnh Quảng Trị*

**Bước 1. Lập Kế hoạch bảo vệ an toàn thông tin cho hệ thống thông tin:**

a) Thành lập bộ phận, tổ quản lý an toàn thông tin;

b) Xây dựng định hướng cơ bản cho công tác đảm bảo an toàn thông tin, trong đó chỉ rõ:

- Mục đích ngắn hạn, trung hạn và dài hạn;
- Phương hướng và văn bản pháp quy, tiêu chuẩn cần tuân thủ và tham khảo;
- Ước lượng nhân lực và kinh phí đầu tư.

c) Lập Kế hoạch xây dựng hệ thống bảo vệ an toàn thông tin:

- Xác định và phân loại các nguy cơ gây sự cố an toàn thông tin;
- Rà soát và lập danh sách các đối tượng cần được bảo vệ với những mô tả đầy đủ về: Nhiệm vụ; Chức năng; Mức độ quan trọng và các đặc điểm đối tượng (phần mềm, phần cứng…);
- Xây dựng phương án bảo đảm an toàn cho các đối tượng trong danh sách cần được bảo vệ: nguyên tắc quản lý, vận hành: các giải pháp bảo vệ và khắc phục sự cố…
- Liên lạc và hợp tác chặt chẽ với Sở Thông tin và Truyền thông, Công an tỉnh cũng như các cơ quan, tổ chức nghiên cứu và cung cấp dịch vụ an toàn mạng;
- Lập kế hoạch dự trù kinh phí đầu tư cho hệ thống bảo vệ.

**Bước 2. Xây dựng hệ thống bảo vệ an toàn thông tin:**

- Tổ chức đội ngũ cán bộ, công chức, viên chức chuyên trách về công nghệ thông tin; cán bộ, công chức, viên chức thực hiện công tác đảm bảo an toàn thông tin đủ năng lực đảm bảo an toàn thông tin cho các hệ thống thông tin;
- Xây dựng hệ thống bảo vệ an toàn thông tin theo kế hoạch.

**Bước 3. Quản lý và vận hành hệ thống bảo vệ an toàn thông tin:**

- Vận hành và quản lý chặt chẽ phần cứng, phần mềm theo quy định đã đặt ra;
- Khi phát hiện sự cố cần nhanh chóng xác định nguyên nhân, tìm biện pháp khắc phục và báo cáo sự cố cho các cơ quan chức năng;
- Cài đặt đầy đủ, thường xuyên cập nhật phần mềm, các bản vá lỗi theo hướng dẫn của nhà cung cấp, thường xuyên thay đổi mật khẩu, sử dụng mật khẩu với độ an toàn cao.

**Bước 4. Kiểm tra đánh giá hoạt động của hệ thống an toàn thông tin:**

- Thường xuyên kiểm tra giám sát các hoạt động của hệ thống bảo vệ an toàn thông tin nói riêng cũng như toàn bộ hệ thống thông tin nói chung.
- Báo cáo tổng kết tình hình theo định kỳ và đột xuất.

**Bước 5. Bảo trì và nâng cấp hệ thống bảo vệ an toàn thông tin:**

Thường xuyên kiểm tra, bảo trì hệ thống bảo vệ an toàn thông tin. Cần nhanh chóng mở rộng, nâng cấp hoặc thay thế khi cần thiết.

**Phụ lục số II**

**KHUNG QUY CHẾ NỘI BỘ ĐẢM BẢO AN TOÀN THÔNG TIN TRONG HOẠT ĐỘNG ỨNG DỤNG CÔNG NGHỆ THÔNG TIN**

*(Ban hành kèm theo Quyết định số 35/2016/QĐ-UBND ngày 29 tháng 8 năm 2016 của UBND tỉnh Quảng Trị*

1. Mục tiêu, phạm vi, đối tượng áp dụng:

Quy định rõ mục tiêu, phạm vi, đối tượng áp dụng của quy chế nội bộ: Phòng, ban chuyên môn và đơn vị trực thuộc.

2. Nội dung bảo đảm an toàn thông tin:

- Nêu rõ các biện pháp quản lý kỹ thuật cơ bản cho công tác an toàn thông tin;

- Nêu rõ các biện pháp quản lý vận hành trong công tác an toàn thông tin;

3. Quy định cụ thể quyền và trách nhiệm của từng đối tượng:

- Quyền và trách nhiệm của lãnh đạo đơn vị;

- Quyền và trách nhiệm của lãnh đạo cấp phòng;

- Quyền và trách nhiệm của cán bộ, công chức, viên chức làm công tác chuyên trách về CNTT;

- Quyền và trách nhiệm của cán bộ, công chức, viên chức thực hiện công tác đảm bảo an toàn thông tin;

- Quyền và trách nhiệm của người sử dụng.

4. Quy định về cấp phát, thu hồi, cập nhật và quản lý các tài khoản truy cập vào hệ thống thông tin:

Nêu rõ quy định về cấp phát, thu hồi, cập nhật và quản lý các tài khoản truy cập vào từng hệ thống thông tin.

5. Quy định về công tác bảo vệ bí mật nhà nước về an toàn thông tin trên môi trường mạng.

6. Cơ chế sao lưu dữ liệu, cơ chế thông tin, báo cáo và khắc phục sự cố:

- Nêu rõ cơ chế sao lưu dữ liệu, cơ chế thông tin;

- Nêu rõ nội dung báo cáo và phối hợp khắc phục sự cố.

7. Theo dõi, kiểm tra, thống kê, tổng hợp, báo cáo theo định kỳ và đột xuất:

- Nêu rõ việc theo dõi, thời gian kiểm tra các hệ thống thông tin;

- Nêu rõ việc thống kê, tổng hợp, báo cáo theo định kỳ và đột xuất.

8. Khen thưởng, kỷ luật:

Các hình thức khen thưởng, kỷ luật.

9. Tổ chức thực hiện:

Cách thức tổ chức thực hiện.

**Phụ lục số III**
**MẪU BÁO CÁO SỰ CỐ**
*(Ban hành kèm theo Quyết định số 35/2016/QĐ-UBND ngày 29 tháng 8 năm 2016 của UBND tỉnh Quảng Trị*

UBND TỈNH QUẢNG TRỊ
**TÊN ĐƠN VỊ**

**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**
**Độc lập - Tự do - Hạnh phúc**

*Quảng Trị, ngày tháng năm 20…*

**BÁO CÁO SỰ CỐ THÁNG/NĂM……...**

**1. Thông tin chung**

Đại diện lãnh đạo: .....

Tên cơ quan: .....

E-mail cơ quan: .....

Điện thoại cơ quan: .....

**2. Thông tin về sự cố:**

Số lượng máy chủ bị sự cố: …….. máy

a) Hệ điều hành:

☐ Windows phiên bản: .....

☐ Linux phiên bản: .....

☐ Ubuntu phiên bản: .....

☐ Khác: .....

b) Chức năng của máy chủ: .....

.....

c) Thời gian xảy ra sự cố: ……..giờ…..phút, ngày…..tháng…..năm .....

d) Mô tả sơ bộ về sự cố: .....

.....

.....

e) Các dịch vụ có trên máy chủ:

☐ Web server ☐ Mail server ☐ Database server

☐ FPT server ☐ Proxy server ☐ Application server

Dịch vụ khác: .....

f) Cách thức phát hiện:

☐ Người dùng cuối ☐ Quản trị hệ thống

☐ Qua hệ thống IDS/IPS ☐ Kiểm tra Log File

☐ Kiểm tra đường truyền ☐ Công ty, tổ chức tư vấn

Khác: .....

g) Các biện pháp đã xử lý khi gặp sự cố:

☐ Không làm gì cả ☐ Tự xử lý

☐ Báo cáo cấp trên ☐ Hỗ trợ từ Sở Thông tin và Truyền thông

☐ Hỗ trợ từ VNCERT

Khác: .....

***Nơi nhận:***
- Sở TT & TT;
- …

**THỦ TRƯỞNG ĐƠN VỊ**
*(Ký tên và đóng dấu)*

**Phụ lục số IV**
**MẪU BÁO CÁO TÌNH HÌNH AN TOÀN THÔNG TIN**
*(Ban hành kèm theo Quyết định số 35/2016/QĐ-UBND ngày 29 tháng 8 năm 2016 của UBND tỉnh Quảng Trị*

UBND TỈNH QUẢNG TRỊ
**TÊN ĐƠN VỊ**

**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**
**Độc lập - Tự do - Hạnh phúc**

*Quảng Trị, ngày tháng năm 20…*

**BÁO CÁO TÌNH HÌNH AN TOÀN THÔNG TIN NĂM….**

**I. ĐÁNH GIÁ HIỆN TRẠNG VÀ DỰ KIẾN**

1. Về chính sách, quản lý

- Xây dựng quy chế nội bộ đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin:

☐ Không ☐ Có, số văn bản …… ngày…….

- Có thường xuyên cập nhật công nghệ đảm bảo an toàn thông tin:

☐ Có ☐ Không

2. Về đầu tư

- Đã và dự kiến đầu tư vào các nội dung nào dưới đây:

| Nội dung | Năm ……. | Dự kiến năm tiếp theo |
|---|---|---|
| Mua thiết bị (phần cứng và phần mềm) an toàn thông tin | ☐ | ☐ |
| Nghiên cứu sử dụng phần mềm mã nguồn mở | ☐ | ☐ |
| Đào tạo nguồn nhân lực | ☐ | ☐ |
| Các nội dung khác: | ……..<br>……..<br>…….. | ……..<br>……..<br>…….. |

- Đã và dự kiến sử dụng những công cụ nào để bảo đảm an toàn thông tin:

| Công cụ | Năm ……. | Dự kiến năm tiếp theo |
|---|---|---|
| Phần mềm diệt virus | ☐ | ☐ |
| Mật khẩu | ☐ | ☐ |
| Tường lửa | ☐ | ☐ |
| Công cụ mã hóa tập tin | ☐ | ☐ |
| Chữ ký điện tử | ☐ | ☐ |
| Mạng riêng ảo VPN | ☐ | ☐ |
| Hệ thống phát hiện xâm nhập | ☐ | ☐ |
| Những công cụ khác: | ……..<br>……..<br>…….. | ……..<br>……..<br>…….. |

3. Về tình hình an ninh mạng và xử lý sự cố

- Tổng kết các sự cố an ninh mạng đã xảy ra trong năm:

| Sự cố | Số lượng |
|---|---|
| Virus | |
| Lừa đảo | |
| Spyware/Adware | |
| Tấn công từ chối dịch vụ (Dos, Ddos) | |
| Nội dung Website đơn vị bị thay đổi (deface website) | |
| Sự cố khác: ..... ..... | |

- Mức độ thiệt hại ước tính trong năm do các sự cố an toàn thông tin gây ra:

☐ Thiệt hại gián tiếp: ……triệu đồng

☐ Thiệt hại trực tiếp: ……triệu đồng

☐ Chi phí khắc phục: ……triệu đồng

- Biện pháp xử lý đã áp dụng khi gặp sự cố:

| Phương pháp | Số lần |
|---|---|
| Không làm gì cả | |
| Tự xử lý | |
| Báo cáo cấp trên | |
| Yêu cầu hỗ trợ từ nơi khác | |
| Phương pháp khác:..... ..... | |

- Công việc mà cơ quan đã thực hiện sau khi khắc phục được sự cố:

☐ Sửa đổi chính sách/hướng dẫn

☐ Nâng cao ý thức

☐ Đầu tư thêm thiết bị

☐ Rà soát lại hệ thống

☐ Đào tạo nâng cao cho quản trị

☐ Đào tạo nâng cao cho người dùng, .....

4. Tổ chức nhân lực và bồi dưỡng nghiệp vụ:

- Số lượng cán bộ chuyên trách và kiêm nhiệm về công nghệ thông tin:

☐ Cán bộ chuyên trách về CNTT, ….. người, trình độ chuyên môn: .....

☐ Cán bộ kiêm nhiệm về CNTT, ….. người, trình độ chuyên môn: .....

- Số lượng cán bộ thực hiện công tác đảm bảo an toàn thông tin trong hoạt động ứng dụng CNTT:

☐ Cán bộ thực hiện công tác đảm bảo an toàn thông tin là cán bộ chuyên trách/ kiêm nhiệm về CNTT, ….. người, trình độ chuyên môn: .....

☐ Cán bộ thực hiện công tác đảm bảo an toàn thông tin không là cán bộ chuyên trách/ kiêm nhiệm về CNTT, ….. người, trình độ chuyên môn: .....

- Đơn vị có nhu cầu bồi dưỡng nghiệp vụ an toàn thông tin:

☐ Dành cho lãnh đạo và cán bộ quản lý, số lượng dự kiến …… người

☐ Cơ bản/Nâng cao về an toàn thông tin cho cán bộ thực hiện công tác đảm bảo an toàn thông tin, số lượng dự kiến …… người

☐ Cho người dùng, số lượng dự kiến ……. người

**II. Ý KIẾN PHẢN HỒI VÀ GÓP Ý THÊM**

.....

.....

.....

.....

.....

***Nơi nhận:***
- Sở TT & TT;
- …

**THỦ TRƯỞNG ĐƠN VỊ**
*(Ký tên và đóng dấu)*