ỦY BAN NHÂN DÂN TỈNH THÁI BÌNH	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 1874 /QĐ-UBND	*Thái Bình, ngày 13 tháng 7 năm 2017*

QUYẾT ĐỊNH

Ban hành Quy định đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan, đơn vị trên địa bàn tỉnh

ỦY BAN NHÂN DÂN TỈNH THÁI BÌNH

Căn cứ Luật Tổ chức Chính quyền địa phương ngày 19/6/2015;

Căn cứ Luật Giao dịch điện tử ngày 29/11/2005; Luật Công nghệ thông tin ngày 29/6/2006; Luật An toàn thông tin mạng ngày 19/11/2015;

Căn cứ các Nghị định của Chính phủ: Nghị định số 64/2007/NĐ-CP ngày 10/4/2007 về ứng dụng công nghệ thông tin trong hoạt động của cơ quan Nhà nước; Nghị định số 90/2008/NĐ-CP ngày 13/8/2008 về chống thư rác; Nghị định số 77/2012/NĐ-CP ngày 05/10/2012 về sửa đổi, bổ sung một số điều của Nghị định số 90/2008/NĐ-CP ngày 13/8/2008 của Chính phủ về chống thư rác; Nghị định số 72/2013/NĐ-CP ngày 15/7/2013 về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng; Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ; Nghị định số 142/2016/NĐ-CP ngày 14/10/2016 về ngăn chặn xung đột thông tin trên mạng;

Căn cứ Quyết định số 898/QĐ-TTg ngày 27/5/2016 của Thủ tướng Chính phủ phê duyệt phương hướng, mục tiêu, nhiệm vụ bảo đảm an toàn thông tin mạng giai đoạn 2016 - 2020;

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

Căn cứ 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 21/TTr-STTTT ngày 19/6/2017,

QUYẾT ĐỊNH:

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

Điều 2. Quyết định này có hiệu lực 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 thuộc tỉnh; Chủ tịch Ủy ban nhân dân huyện, thành phố; Chủ tịch Ủy ban nhân dân xã, phường, thị trấn; các doanh nghiệp viễn thông, công nghệ thông tin trên địa bàn và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Bộ Thông tin và Truyền thông;
- Chủ tịch, các PCT UBND tỉnh;
- Lưu: VT, KGVX.

TM. ỦY BAN NHÂN DÂN TỈNH
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Nguyễn Hoàng Giang

ỦY BAN NHÂN DÂN TỈNH THÁI BÌNH	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc

QUY ĐỊNH

Đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan, đơn vị trên địa bàn tỉnh

(Ban hành kèm theo Quyết định số: 1874 /QĐ-UBND ngày 13 /7/2017 của Ủy ban nhân dân tỉnh)

Chương I
NHỮNG QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy định này bao gồm các nội dung về công tác đảm bảo an toàn thông tin mạng trong thiết kế, xây dựng, quản lý, vận hành, sử dụng, nâng cấp hệ thống thông tin của các cơ quan, đơn vị trên địa bàn tỉnh.

Điều 2. Đối tượng áp dụng

1. Các sở, ban, ngành; Ủy ban nhân dân huyện, thành phố; các đơn vị sự nghiệp thuộc tỉnh; Ủy ban nhân dân xã, phường, thị trấn; các tổ chức, đoàn thể (sau đây gọi tắt là các cơ quan, đơn vị).

2. Các doanh nghiệp viễn thông, công nghệ thông tin và các đơn vị có tham gia vào các hoạt động ứng dụng công nghệ thông tin của tỉnh.

3. Cán bộ, công chức, viên chức và người lao động đang công tác trong các cơ quan, đơn vị nêu tại khoản 1, khoản 2 Điều này và những cá nhân, tổ chức có liên quan áp dụng quy định này trong việc vận hành, khai thác các hệ thống công nghệ thông tin dùng chung của tỉnh, các hệ thống thông tin tại các cơ quan, đơn vị.

Điều 3. Giải thích từ ngữ

Trong Quy định này, các từ ngữ dưới đây được hiểu như sau:

1. Hệ thống thông tin dùng chung của tỉnh, hệ thống thông tin tại các cơ quan, đơn vị là tập hợp các thiết bị viễn thông, công nghệ thông tin bao gồm phần cứng, phần mềm và cơ sở dữ liệu phục vụ cho hoạt động lưu trữ, xử lý, truyền đưa, chia sẻ, trao đổi, cung cấp và sử dụng thông tin số tại Trung tâm Tích hợp dữ liệu của tỉnh, tại các cơ quan, đơn vị.

2. Trung tâm Tích hợp dữ liệu của tỉnh là một công trình bao gồm: Nhà trạm, hệ thống cáp và hệ thống máy tính cùng các thiết bị phụ trợ lắp đặt vào đó để lưu trữ, trao đổi và quản lý tập trung dữ liệu của tỉnh.

3. An toàn thông tin mạng là sự bảo vệ thông tin và các hệ thống thông tin tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

4. Thiết bị di động thông minh được hiểu là thiết bị di động tích hợp một nền tảng hệ điều hành di động với nhiều tính năng hỗ trợ tiên tiến về điện toán và kết nối dựa trên nền tảng cơ bản của thiết bị di động thông thường.

Điều 4. Các hành vi bị nghiêm cấm

1. Tạo ra, cài đặt, phát tán virus máy tính, phần mềm độc hại trái pháp luật.

2. Xâm nhập, sửa đổi, xóa bỏ nội dung thông tin của cơ quan, cá nhân khác.

3. Cản trở hoạt động cung cấp dịch vụ của hệ thống thông tin.

4. Ngăn chặn việc truy nhập đến thông tin của cơ quan, cá nhân khác trên môi trường mạng, trừ trường hợp pháp luật cho phép.

5. Bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã và thông tin của cơ quan, cá nhân khác trên môi trường mạng.

6. Các hành vi khác làm mất an toàn, bí mật thông tin của cơ quan, cá nhân khác được trao đổi, truyền đưa, lưu trữ trên môi trường mạng.

Chương II

NỘI DUNG ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG

Điều 5. Các quy định chung về đảm bảo an toàn thông tin

1. Các văn bản có nội dung mật không được truyền trên mạng mà phải được quản lý theo chế độ mật theo quy định pháp luật hiện hành. Không sử dụng các thiết bị di động thông minh để soạn thảo văn bản, lưu giữ thông tin có nội dung mật theo quy định. Trường hợp đặc biệt, cần truyền thông tin mật trên mạng phải được Thủ trưởng cơ quan, đơn vị cho phép, trước khi truyền thông tin phải được mã hóa theo quy định của Luật Cơ yếu. Các thiết bị viễn thông, máy tính được sử dụng để lưu giữ và truyền thông tin bí mật nhà nước phải được chứng nhận của cơ quan chức năng kiểm tra, kiểm định trước khi đưa vào sử dụng.

2. Trao đổi văn bản, tài liệu điện tử chỉ thực hiện trên hệ thống thông tin dùng chung của tỉnh và hệ thống thông tin của cơ quan. Không trao đổi văn bản, tài liệu điện tử qua mạng xã hội, qua thư điện tử công cộng (gmail, yahoo mail,...), không sử dụng dịch vụ lưu trữ trực tuyến (Google Drive, Dropbox,..) để lưu trữ, chia sẻ văn bản, tài liệu của cơ quan.

3. Các cơ quan, đơn vị phải sử dụng phần mềm diệt vius có bản quyền cho 100% máy tính của cơ quan, đơn vị khi kết nối mạng nội bộ, Mạng diện rộng của tỉnh để khai thác sử dụng các hệ thống thông tin dùng chung của tỉnh.

4. Các cơ quan, đơn vị khi quản trị các hệ thống thông tin dùng chung của tỉnh; triển khai, sử dụng hội nghị truyền hình, phần mềm diệt vius tập trung, cơ sở dữ liệu chuyên ngành phải thực hiện trên Mạng diện rộng của tỉnh.

5. Phải có phương án tổ chức sao lưu dữ liệu dự phòng cho mọi dữ liệu quan trọng của tỉnh, của cơ quan, đơn vị mình. Lãnh đạo cơ quan, đơn vị phải chịu trách nhiệm nếu để xảy ra mất mát dữ liệu do không tiến hành sao lưu dự phòng.

6. Để phục vụ hoạt động theo dõi, giám sát, phân tích và điều tra, các cơ quan, đơn vị quản trị các hệ thống công nghệ thông tin phải thực hiện việc lưu trữ

nhật ký của các hệ thống công nghệ thông tin tại các máy chủ (của hệ điều hành và các phần mềm ứng dụng) trong thời gian ít nhất là 30 ngày.

7. Các thiết bị viễn thông, máy tính có chứa tài liệu của cơ quan nhà nước khi đưa đi công tác nước ngoài phải thực hiện theo quy định của pháp luật về bảo vệ bí mật nhà nước.

8. Chú trọng phát triển nguồn nhân lực có trình độ về công nghệ thông tin đặc biệt là an toàn thông tin để nâng cao năng lực bảo đảm an toàn thông tin. Tạo điều kiện cho cán bộ phụ trách công nghệ thông tin được đào tạo, bồi dưỡng nâng cao kỹ năng nghiệp vụ về an toàn thông tin.

Điều 6. Đảm bảo an toàn thông tin cho các hệ thống thông tin và các thiết bị công nghệ thông tin

1. Đảm bảo an toàn thông tin cho các hệ thống thông tin dùng chung của tỉnh, bao gồm:

a) Xây dựng giải pháp đảm bảo an toàn thông tin cho các hệ thống công nghệ thông tin dùng chung của tỉnh để tăng hiệu quả sử dụng, tiết kiệm đầu tư, đảm bảo tính liên thông giữa các hệ thống trong Trung tâm Tích hợp dữ liệu của tỉnh;

b) Tổ chức thực hiện giám sát, đánh giá và đảm bảo an toàn thông tin cho các hệ thống thông tin dùng chung và các hệ thống cơ sở dữ liệu quan trọng của tỉnh;

c) Chủ trì, phối hợp với các cơ quan, đơn vị trong tỉnh để thực hiện quản lý chặt chẽ tài khoản người dùng của các hệ thống thông tin dùng chung của tỉnh. Đối với cán bộ, công chức, viên chức đã nghỉ việc, chuyển công tác, phải có biện pháp khóa hoặc hủy tài khoản, quyền truy nhập, thu hồi các thiết bị liên quan tới hệ thống thông tin dùng chung của tỉnh (như chứng thư số,...);

d) Chủ trì, phối hợp với các cơ quan, đơn vị liên quan tổ chức lên phương án sao lưu và phục hồi dữ liệu khi xảy ra sự cố đối với các hệ thống thông tin dùng chung của tỉnh; tổ chức sao lưu dữ liệu các hệ thống thông tin dùng chung của tỉnh và hướng dẫn về sao lưu dự phòng các dữ liệu quan trọng cho các cơ quan nhà nước thuộc tỉnh.

2. Đảm bảo an toàn thông tin cho các hệ thống thiết bị mạng, máy chủ, máy tính cá nhân và các hệ thống lưu trữ tại các cơ quan:

Nội dung bảo vệ hệ thống thông tin được thực hiện theo các quy định tại Điều 22, 23 của Luật an toàn thông tin mạng; Điều 19, 20, 22 của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ.

a) Khi xây dựng, nâng cấp, mở rộng hạ tầng kỹ thuật công nghệ thông tin; các hệ thống thông tin của cơ quan, đơn vị phải có phương án đảm bảo an toàn thông tin mạng và phải được Sở Thông tin và Truyền thông thẩm định trước khi trình cấp có thẩm quyền phê duyệt;

b) Việc quản lý gửi thông tin trên mạng phải tuân thủ theo các nội dung quy định tại Điều 10 Luật an toàn thông tin mạng và các quy định sau:

- Việc trao đổi văn bản, tài liệu điện tử của cơ quan (kể cả tài liệu tham khảo) chỉ thực hiện trên các hệ thống ứng dụng công nghệ thông tin dùng chung của tỉnh hoặc trên các phần mềm ứng dụng của nội bộ ngành chuyển giao ứng dụng.

- Khi phát hành và gửi văn bản qua mạng, các cơ quan nhà nước phải thực hiện ký số và xác thực văn bản điện tử trước khi gửi.

c) Máy chủ, máy tính cá nhân, hệ thống lưu trữ nội bộ, thiết bị mạng phải được bảo vệ bởi mật khẩu an toàn, tuyệt đối không sử dụng mật khẩu ngắn, mặc định; thực hiện việc bảo vệ an toàn vật lý cho hệ thống công nghệ thông tin của cơ quan, đơn vị;

d) 100% máy tính tại các cơ quan, đơn vị phải được cài đặt các phần mềm diệt virus có bản quyền. Khi phát hiện hoặc có thông tin trong hệ thống mạng bị lây nhiễm các phần mềm gián điệp, độc hại phải khẩn trương và kiên quyết khắc phục sớm và báo cáo tình hình mất an toàn thông tin mạng thông qua đường dây nóng của Sở Thông tin và Truyền thông;

e) Phối hợp xây dựng phương án, tổ chức khắc phục khi xảy ra sự cố mất an toàn thông tin mạng.

Điều 7. Đảm bảo an toàn thông tin cho Trung tâm Tích hợp dữ liệu của tỉnh

1. Đảm bảo an toàn thông tin cho Trung tâm Tích hợp dữ liệu của tỉnh bao gồm: Các điều kiện về hạ tầng kỹ thuật, an toàn thông tin đối với hệ thống máy chủ, thiết bị kết nối mạng đặt tại Trung tâm Tích hợp dữ liệu của tỉnh. Xây dựng giải pháp đảm bảo an toàn thông tin cho dữ liệu của các cơ quan, đơn vị đặt tại Trung tâm Tích hợp dữ liệu của tỉnh nhưng phải đảm bảo thuận lợi cho việc truy xuất và sử dụng các dữ liệu này.

2. Các cơ quan, đơn vị đặt dữ liệu hoặc kết nối vào Trung tâm Tích hợp dữ liệu của tỉnh phải tuân thủ các chính sách an toàn thông tin liên quan đến việc kết nối vào Trung tâm Tích hợp dữ liệu của tỉnh do Sở Thông tin và Truyền thông hướng dẫn.

3. Các cơ quan, đơn vị khi kết nối vào Trung tâm Tích hợp dữ liệu của tỉnh phải tự bảo vệ hệ thống đầu cuối của mình và phải chịu trách nhiệm nếu để tin tặc kiểm soát máy tính và tấn công ngược vào Trung tâm Tích hợp dữ liệu của tỉnh.

Chương III

TRÁCH NHIỆM ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 8. Trách nhiệm chung của các cơ quan, đơn vị

1. Các cơ quan, đơn vị nếu triển khai các hệ thống thông tin độc lập thì phải tuân thủ các quy định tại khoản 2, Điều 6 và khoản 2, khoản 3 Điều 7 của Quy định này đồng thời tự chịu trách nhiệm đảm bảo an toàn thông tin như: Cập nhật kịp thời các bản vá lỗ hổng bảo mật từ nhà cung cấp, nhà sản xuất cho các hệ thống thông tin, cơ sở dữ liệu; có cơ chế sao lưu dữ liệu dự phòng, dữ liệu được lưu trữ tại nơi an toàn để sẵn sàng phục hồi cơ sở dữ liệu khi xảy ra sự cố an toàn thông tin mạng; tổ chức phân quyền truy cập cho các đối tượng người dùng tham gia vận hành, khai thác các hệ thống thông tin đúng quy trình, chặt chẽ gắn với trách nhiệm của từng tổ chức, cá nhân để đảm bảo an toàn thông tin mạng cho các hệ thống thông tin cơ quan, đơn vị đang quản lý, vận hành và phối hợp với Sở Thông tin và Truyền thông khi được yêu cầu.

2. Thủ trưởng các cơ quan, đơn vị có trách nhiệm bố trí cán bộ chuyên trách công nghệ thông tin; giao nhiệm vụ giám sát an toàn hệ thống thông tin của cơ quan, quản lý chặt chẽ các tài khoản đã cung cấp cho người dùng trong cơ quan, đơn vị. Cán bộ chuyên trách được đảm bảo điều kiện học tập, tiếp cận công nghệ, kiến thức an toàn bảo mật thông tin trước khi tiến hành các hoạt động quản lý hay kỹ thuật nghiệp vụ.

3. Tuyên truyền, nâng cao nhận thức cho cán bộ công chức, viên chức về các nguy cơ mất an toàn của hệ thống thông tin; tổ chức triển khai thực hiện các quy định tại Quy chế này và chịu trách nhiệm trước Ủy ban nhân dân tỉnh trong công tác đảm bảo an toàn thông tin của cơ quan, đơn vị mình.

4. Trang bị đầy đủ các kiến thức bảo mật cơ bản cho cán bộ công chức, viên chức về an toàn thông tin trước khi cho phép truy nhập và sử dụng hệ thống thông tin dùng chung của tỉnh.

5. Triệt để sử dụng chứng thư số chuyên dùng ký số và xác thực văn bản điện tử để đảm bảo xác định nguồn gốc, tính toàn vẹn của văn bản và mã hoá các tài liệu quan trọng.

6. Phân công cán bộ giám sát, theo dõi thường xuyên hoạt động của Cổng thông tin điện tử của cơ quan để phát hiện kịp thời và có giải pháp xử lý khi bị thay đổi thông tin, bị đăng tải những thông tin lạ.

7. Quan tâm và ưu tiên bố trí kinh phí cho việc mua sắm, nâng cấp các trang thiết bị phần cứng, phần mềm bảo mật để đảm bảo và tăng cường an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của cơ quan, đơn vị. Duy trì thường xuyên công tác kiểm tra, đánh giá an toàn thông tin đối với hệ thống thông tin của đơn vị.

8. Khi có sự cố hoặc có nguy cơ mất an toàn thông tin phải kịp thời chỉ đạo khắc phục ngay, ưu tiên sử dụng cán bộ kỹ thuật chuyên trách trong cơ quan, đơn vị, kịp thời báo cho doanh nghiệp cung cấp dịch vụ 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.

9. Xây dựng quy định, quy trình nội bộ về đảm bảo an toàn thông tin trong khai thác, sử dụng các hệ thống thông tin của cơ quan, đơn vị phù hợp với Quy định này và các quy định khác của pháp luật.

10. Khi triển khai đầu tư ứng dụng công nghệ thông tin phải có phương án đảm bảo an toàn thông tin từ khâu thiết kế và phải tự chịu trách nhiệm đảm bảo an toàn thông tin cho các hệ thống thông tin của cơ quan, đơn vị mình.

11. Phối hợp chặt chẽ với Công an tỉnh trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn, an ninh thông tin.

12. Phối hợp với Sở Thông tin và Truyền thông và các cơ quan, đơn vị liên quan thực hiện công tác kiểm tra khắc phục sự cố đồng thời cung cấp đầy đủ các thông tin khi đoàn kiểm tra yêu cầu. Không được che dấu thông tin về sự cố nhằm gây khó khăn cho các cơ quan chức năng đánh giá thiệt hại để có phương án xử lý.

13. Định kỳ hàng quý, các cơ quan, đơn vị lập báo cáo về tình hình an toàn thông tin và gửi về Sở Thông tin và Truyền thông. Báo cáo cả năm kết quả thực hiện công tác đảm bảo an toàn thông tin tại cơ quan, đơn vị gửi về Sở Thông tin và Truyền thông (trước ngày 15/11) để tổng hợp báo cáo Ban chỉ đạo ứng dụng công nghệ thông tin tỉnh Thái Bình.

Điều 9. Trách nhiệm của Sở Thông tin và Truyền thông

1. Chủ trì, phối hợp với các đơn vị liên quan của Bộ Thông tin và Truyền thông và các cơ quan có liên quan tổ chức thực hiện các giải pháp ngăn chặn xung đột thông tin trên mạng bao gồm: Giám sát, phát hiện, cảnh báo, xác định nguồn gốc, khắc phục xung đột thông tin trên mạng; triển khai các phương án bảo vệ thuộc phạm vi quản lý theo quy định của pháp luật.

2. Chủ trì, phối hợp với các cơ quan có liên quan tham mưu, đề xuất Ủy ban nhân dân tỉnh đầu tư trang bị các thiết bị, phần mềm bảo mật chuyên dùng để đáp ứng phương tiện, công cụ nâng cao năng lực đảm bảo an toàn thông tin mạng trong Trung tâm Tích hợp dữ liệu của tỉnh và chịu trách nhiệm trước Ủy ban nhân dân tỉnh trong việc đảm bảo an toàn cho các hệ thống thông tin dùng chung của tỉnh theo quy định tại khoản 1, Điều 6 và khoản 1, Điều 7 của Quy định này.

3. Là cơ quan đầu mối về ứng cứu sự cố máy tính của tỉnh, tham gia vào mạng lưới điều phối ứng cứu sự cố Internet và là đầu mối về tiếp nhận và xử lý các vấn đề liên quan đến các sự cố về an toàn thông tin mạng.

4. Chịu trách nhiệm xây dựng và trình Ủy ban nhân dân tỉnh ban hành các cơ chế, chính sách về đảm bảo an toàn thông tin cho các cơ quan, đơn vị trong tỉnh.

5. Nghiên cứu, tham mưu Ủy ban nhân dân tỉnh xây dựng đội ngũ cán bộ chuyên trách về an toàn thông tin có trình độ đáp ứng yêu cầu theo quy định.

6. Chủ trì hoạt động kiểm tra đánh giá công tác đảm bảo an toàn thông tin trong các cơ quan, đơn vị trong tỉnh và thực hiện đánh giá an toàn thông tin cho các hệ thống thông tin dùng chung của tỉnh.

7. Xây dựng kế hoạch, chương trình, dự án hàng năm để triển khai công tác đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin chung của tỉnh. Đồng thời xây dựng kế hoạch ứng phó sự cố bảo đảm an toàn thông tin mạng của tỉnh Thái Bình trình Ủy ban nhân dân tỉnh phê duyệt.

8. Xây dựng và triển khai các chương trình đào tạo chuyên sâu về an toàn, an ninh thông tin cho cán bộ chuyên trách công nghệ thông tin của các cơ quan, đơn vị; tổ chức hội nghị tuyên truyền an toàn thông tin trong công tác quản lý nhà nước, trong khai khác sử dụng các hệ thống thông tin, cơ sở dữ liệu dùng chung của tỉnh với các đối tượng thuộc phạm vi điều chỉnh của Quy định này.

9. Là đầu mối của tỉnh, phối hợp với Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT), các cơ quan, đơn vị có liên quan xử lý, ứng cứu các sự cố mất an toàn thông tin trên địa bàn tỉnh. Chủ động hỗ trợ, hướng dẫn cụ thể về nghiệp vụ quản lý vận hành, kỹ thuật đảm bảo an toàn thông tin cho các cơ quan, đơn vị, các tổ chức, đoàn thể thuộc tỉnh ứng cứu, xử lý sự cố của các hệ thống thông tin trong khả năng và trách nhiệm của mình. Giám sát diễn biến tình hình

ứng cứu sự cố và báo cáo Ban Chỉ đạo ứng dụng công nghệ thông tin tỉnh Thái Bình và cơ quan điều phối quốc gia để đề xuất, xin ý kiến chỉ đạo trong trường hợp vượt khả năng xử lý của mình.

10. Thiết lập đường dây nóng, bố trí cán bộ thường trực để tiếp nhận các phản ánh của các cơ quan, đơn vị về nguy cơ gây mất an toàn thông tin; phối hợp hướng dẫn, xử lý kịp thời.

11. Thông báo cho các cơ quan, đơn vị biết và có biện pháp phòng ngừa, ngăn chặn các nguy cơ mất an toàn thông tin do virus, phần mềm gián điệp gây ra.

12. Tổng hợp báo cáo Bộ Thông tin và Truyền thông, cơ quan điều phối quốc gia theo định kỳ và đột xuất khi được yêu cầu.

13. Đẩy mạnh và tăng cường công tác quản lý nhà nước về công tác đảm bảo an toàn thông tin mạng trên địa bàn tỉnh. Theo dõi, đôn đốc việc chấp hành các nội dung của Quy định này.

Điều 10. Trách nhiệm của Công an tỉnh, Bộ chỉ huy quân sự tỉnh

1. Chủ trì, phối hợp với Sở Thông tin và Truyền thông và các ngành liên quan tham mưu cho Chủ tịch Ủy ban nhân dân tỉnh chỉ đạo công tác bảo vệ an ninh chính trị nội bộ; tăng cường nắm bắt, dự báo tình hình; kiểm tra công tác an toàn thông tin mạng đối với các cơ quan, đơn vị trên địa bàn tỉnh.

2. Thường xuyên thông báo cho các cơ quan, đơn vị về phương thức, thủ đoạn của các loại tội phạm xâm phạm an toàn thông tin mạng để có biện pháp phòng ngừa, phát hiện, đấu tranh, ngăn chặn.

3. Chịu trách nhiệm triển khai các biện pháp, công tác nghiệp vụ để kiểm soát, phòng ngừa, điều tra, phát hiện, ngăn chặn kịp thời, xử lý nghiêm minh các hành vi xâm phạm an toàn thông tin mạng; các loại tội phạm lợi dụng hệ thống thông tin gây tổn hại đến an ninh chính trị, an toàn thông tin mạng theo thẩm quyền.

4. Chủ động và sẵn sàng tham gia các hoạt động ứng cứu các sự cố thông tin mạng trên địa bàn tỉnh

Điều 11. Trách nhiệm của Sở Tài chính, Sở Kế hoạch và Đầu tư

Tham mưu Ủy ban nhân dân tỉnh bố trí kinh phí để đầu tư, quản lý, duy trì, vận hành an toàn các hệ thống thông tin dùng chung của tỉnh bao gồm: kinh phí triển khai các nội dung thuộc khoản 7, Điều 9 của Quy định này; kinh phí dự phòng ứng cứu, xử lý sự cố cho các hệ thống thông tin dùng chung của tỉnh; kinh phí tổ chức đào tạo, huấn luyện, diễn tập và hoạt động ứng cứu sự cố; kinh phí giám sát, kiểm tra, rà quét, đánh giá an toàn thông tin; kinh phí hỗ trợ triển khai các hoạt động nghiệp vụ đặc thù bảo đảm an toàn thông tin mạng cho các hệ thống thông tin dùng chung của tỉnh.

Điều 12. Đài Phát thanh và Truyền hình Thái Bình, Báo Thái Bình

Chủ động triển khai để đẩy mạnh các hoạt động tuyên truyền, nâng cao nhận thức về đảm bảo an toàn thông tin mạng trên các phương tiện thông tin đại chúng.

Điều 13. Trách nhiệm của các doanh nghiệp viễn thông, công nghệ thông tin cung cấp hạ tầng, dịch vụ phục vụ ứng dụng công nghệ thông tin trong cơ quan nhà nước

Thực hiện các nội dung liên quan đến hoạt động bảo đảm an toàn thông tin mạng theo Điều 22 Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ; và các quy định sau:

1. Có trách nhiệm đầu tư, phát triển hạ tầng viễn thông, công nghệ thông tin, đường truyền phục vụ việc phát triển ứng dụng công nghệ thông tin gắn với việc đảm bảo an toàn thông tin mạng. Chủ động phối hợp với Sở Thông tin và Truyền thông và các đơn vị liên quan kiểm tra, phát hiện đối tượng vi phạm an toàn thông tin mạng.

2. Triển khai kế hoạch ứng phó sự cố của doanh nghiệp, dự phòng ứng cứu, xử lý sự cố cho các hệ thống thông tin do doanh nghiệp quản lý; phối hợp giám sát, cung cấp thông tin, tham gia ứng cứu sự cố; tổ chức đào tạo, huấn luyện, diễn tập, duy trì hoạt động ứng cứu sự cố và các nhiệm vụ khác do doanh nghiệp thực hiện.

3. Bảo đảm kinh phí để giám sát, ứng cứu sự cố đảm bảo an toàn thông tin mạng trên các kênh kết nối Internet do doanh nghiệp cung cấp dịch vụ.

4. Viễn thông Thái Bình có trách nhiệm đảm bảo an toàn cho Mạng diện rộng của tỉnh quy định tại Điều 9 của Quyết định số 20/2014/QĐ-UBND ngày 26/9/2014 ban hành Quy chế quản lý, vận hành, sử dụng và bảo đảm an toàn thông tin trên Mạng diện rộng của tỉnh Thái Bình; phối hợp với Sở Thông tin và Truyền thông trong việc xử lý khắc phục sự cố đảm bảo an toàn thông tin trong Mạng diện rộng của tỉnh.

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

1. Trách nhiệm của cán bộ chuyên trách hoặc cán bộ được giao phụ trách công nghệ thông tin trong các cơ quan, đơn vị:

a) Tham mưu cho lãnh đạo cơ quan triển khai thực hiện các biện pháp vận hành, quản lý kỹ thuật; thường xuyên nghiên cứu, cập nhật các kiến thức về an toàn, an ninh thông tin, có biện pháp phòng tránh các nguy cơ tiềm ẩn có thể gây mất thông tin khi tiến hành các hoạt động quản lý hay kỹ thuật nghiệp vụ.

b) Tham mưu xây dựng quy định về đảm bảo an toàn cho hệ thống thông tin của cơ quan, đơn vị theo Quy định này.

c) Thường xuyên kiểm tra, thiết lập cấu hình chuẩn cho các thành phần của hệ thống thông tin để đảm bảo duy trì hoạt động thường xuyên của hệ thống thông tin nhưng chỉ cung cấp những chức năng thiết yếu nhất; xác định các chức năng, cổng giao tiếp mạng, giao thức và dịch vụ không cần thiết để cấm hoặc hạn chế sử dụng.

d) Thường xuyên thực hiện việc theo dõi bản ghi nhật ký hệ thống, kiểm soát chặt chẽ việc cài đặt thêm phần mềm vào máy trạm, máy chủ và các sự kiện khác có liên quan để đánh giá, báo cáo các rủi ro và mức độ nghiêm trọng của các rủi ro do sự truy nhập trái phép, sử dụng trái phép, mất, thay đổi hoặc phá hủy thông tin và hệ thống thông tin.

đ) Phối hợp với các cá nhân, các cơ quan, đơn vị có liên quan trong việc kiểm tra, phát hiện và khắc phục các sự cố mất an toàn thông tin.

2. Trách nhiệm của cán bộ, công chức, viên chức, người lao động:

a) Chấp hành nghiêm túc các quy định về an toàn thông tin của cơ quan, đơn vị cũng như các quy định khác của pháp luật, nâng cao ý thức cảnh giác và trách nhiệm đảm bảo an toàn thông tin tại cơ quan, đơn vị.

b) Thường xuyên cập nhật chính sách an toàn thông tin của cơ quan, đơn vị và thực hiện đúng hướng dẫn về an toàn, an ninh thông tin của cán bộ chuyên trách. Hạn chế việc sử dụng chức năng chia sẻ tài nguyên, khi sử dụng chức năng này cần bật thuộc tính bảo mật bằng mật khẩu và thu hồi chức năng ngay sau khi đã sử dụng xong.

c) Các máy tính khi không sử dụng cần thiết lập chế độ tắt chờ (standby) tối đa 30 phút để tránh bị các tin tặc lợi dụng, sử dụng chức năng điều khiển từ xa dùng máy tính của mình tấn công vào các hệ thống thông tin khác.

d) Phải thực hiện quét virus trước khi mở các tập tin đính kèm theo thư điện tử, không mở các thư điện tử khi chưa rõ người gửi hoặc tập tin đính kèm có nguồn gốc không rõ ràng để tránh virus, phần mềm gián điệp lây nhiễm máy tính.

đ) Phải đặt mật khẩu an toàn cho máy tính (mật khẩu đăng nhập, mật khẩu bảo vệ màn hình). Sử dụng các thiết bị lưu trữ thông tin (USB, ổ cứng gắn ngoài, thẻ nhớ) đảm bảo an toàn, đúng cách để phòng ngừa virus, phần mềm gián điệp xâm nhập máy tính nhằm phá hoại, đánh cắp thông tin.

e) Khi phát hiện sự cố phải báo ngay với thủ trưởng cơ quan và cán bộ chuyên trách hoặc phụ trách công nghệ thông tin của cơ quan, đơn vị để kịp thời ngăn chặn, xử lý.

f) Tham gia đầy đủ các chương trình đào tạo, hội nghị về an toàn thông tin do Sở Thông tin và Truyền thông hoặc các cơ quan, đơn vị chuyên môn tổ chức.

Chương IV

CÔNG TÁC THANH TRA, KIỂM TRA AN TOÀN THÔNG TIN

Điều 15. Kế hoạch thanh tra, kiểm tra hàng năm

1. Định kỳ hàng năm tối thiểu 01 lần, tiến hành kiểm tra đột xuất các cơ quan, đơn vị khi có dấu hiệu vi phạm an toàn thông tin.

2. Sở Thông tin và Truyền thông chủ trì, phối hợp Công an tỉnh và các cơ quan, đơn vị có liên quan để tham mưu thành lập Đoàn kiểm tra; xây dựng kế hoạch kiểm tra và tiến hành công tác kiểm tra an toàn thông tin tại tất cả các cơ quan, đơn vị (nếu cần thiết).

Chủ trì hoạt động thanh tra và xử lý các hành vi vi phạm về an toàn thông tin mạng và phát tán tin nhắn rác trên địa bàn tỉnh. Phối hợp với Công an tỉnh tiến hành xử phạt các hành vi vi phạm an toàn thông tin mạng gây thiệt hại cho hệ thống thông tin của các cơ quan, đơn vị, tổ chức, đoàn thể thuộc tỉnh.

Điều 16. Báo cáo sự cố an toàn thông tin mạng

1. Báo cáo sự cố an toàn thông tin mạng:

a) Đơn vị vận hành hệ thống thông tin của các cơ quan có trách nhiệm báo cáo sự cố tới Thủ trưởng cơ quan và Sở Thông tin và Truyền thông ngay khi phát hiện sự cố;

b) Các tổ chức, cá nhân khi phát hiện dấu hiệu tấn công hoặc sự cố an toàn thông tin mạng cần nhanh chóng thông báo cho đơn vị vận hành hệ thống thông tin của cơ quan và các đơn vị có trách nhiệm liên quan.

2. Báo cáo sự cố phải được thực hiện ngay lập tức và được duy trì trong suốt quá trình ứng cứu sự cố gồm: Báo cáo ban đầu; báo cáo diễn biến tình hình; báo cáo phương án ứng cứu cụ thể; báo cáo xin ý kiến chỉ đạo, chỉ huy; báo cáo đề nghị hỗ trợ, phối hợp; báo cáo kết thúc ứng phó.

3. Hình thức báo cáo bằng công văn, fax, thư điện tử, nhắn tin đa phương tiện tới các cá nhân và đơn vị có liên quan theo quy định tại khoản 1 Điều này;

4. Nội dung báo cáo gồm:

a) Tên, địa chỉ Đơn vị vận hành hệ thống thông tin; cơ quan chủ quản hệ thống thông tin; hệ thống thông tin bị sự cố; thời điểm phát hiện sự cố;

b) Đầu mối liên lạc về sự cố của đơn vị vận hành hệ thống bị sự cố: Tên, chức vụ, điện thoại, thư điện tử;

c) Mô tả về sự cố: Loại sự cố, hiện tượng, đánh giá sơ bộ mức độ nguy hại, mức độ lây lan, tác động của sự cố đến hoạt động bình thường của tổ chức;

d) Đơn vị cung cấp dịch vụ hạ tầng công nghệ thông tin, viễn thông;

đ) Liệt kê các biện pháp đã triển khai hoặc dự kiến triển khai để xử lý khắc phục sự cố;

e) Các tổ chức, doanh nghiệp đang hỗ trợ ứng cứu, xử lý và kết quả xử lý sự cố tính đến thời điểm báo cáo;

g) Kết quả ứng cứu sự cố ban đầu;

h) Kiến nghị đề xuất hướng ứng cứu xử lý sự cố (nếu có).

5. Nguyên tắc báo cáo, trao đổi thông tin trong ứng cứu sự cố:

a) Cơ quan, đơn vị vận hành hệ thống thông tin báo cáo Thủ trưởng cơ quan, Sở Thông tin và Truyền thông;

b) Sở Thông tin và Truyền thông báo cáo Ban Chỉ đạo ứng dụng công nghệ thông tin tỉnh Thái Bình và cơ quan điều phối quốc gia (nếu cần phối hợp giải quyết);

c) Ban Chỉ đạo ứng dụng công nghệ thông tin tỉnh Thái Bình báo cáo Cơ quan thường trực và Ban Chỉ đạo quốc gia.

Chương V
TỔ CHỨC THỰC HIỆN

Điều 17. 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 thông tin của các cơ quan, đơn vị để lập bảng xếp hạng an toàn thông tin, trên cơ sở đó đề xuất Ủy ban nhân dân tỉnh xem xét khen thưởng theo quy định.

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

Điều 18. Điều khoản thi hành

1. Giao Sở Thông tin và Truyền thông chủ trì, phối hợp với các cơ quan, tổ chức có liên quan hướng dẫn, triển khai thực hiện Quy định này.

2. Trong quá trình thực hiện, nếu có vướng mắc phát sinh hoặc các vấn đề cần bổ sung đề nghị các cơ quan, đơn vị kịp thời phản ánh 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 TỈNH
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Nguyễn Hoàng Giang