ỦY BAN NHÂN DÂN TỈNH BÌNH PHƯỚC	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc
Số: 29 /2020/QĐ-UBND	*Bình Phước, ngày 20 tháng 10 năm 2020*

QUYẾT ĐỊNH

Ban hành Quy chế bảo đảm an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin trên địa bàn tỉnh Bình Phước

ỦY BAN NHÂN DÂN TỈNH BÌNH PHƯỚC

Căn cứ Luật Giao dịch điện tử ngày 29 tháng 11 năm 2005;

Căn cứ Luật Công nghệ thông tin ngày 29 tháng 6 năm 2006;

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

Căn cứ Luật Ban hành văn bản quy phạm pháp luật ngày 22 tháng 6 năm 2015;

Căn cứ Luật Giao dịch điện tử ngày 29 tháng 11 năm 2005;

Căn cứ Luật Công nghệ thông tin ngày 29 tháng 6 năm 2006;

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Luật An ninh mạng ngày 12 tháng 6 năm 2018;

Căn cứ Luật sửa đổi, bổ sung một số điều của Luật Tổ chức Chính phủ và Luật Tổ chức chính quyền địa phương ngày 22 tháng 11 năm 2019;

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 của cơ quan Nhà nước;

Căn cứ Nghị định số 72/2013/NĐ-CP ngày 15 tháng 7 năm 2013 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Nghị định số 142/2016/NĐ-CP ngày 14 tháng 10 năm 2016 của Chính phủ về ngăn chặn xung đột thông tin trên mạng;

Căn cứ Thông tư số 03/2017/TT-BTTTT ngày 24 tháng 4 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc;

Căn cứ Thông tư số 27/2017/TT-BTTTT ngày 20 tháng 10 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về việc quản lý, vận hành, kết nối, sử dụng và bảo đảm an toàn thông tin trên mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước;

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

Thực hiện Quyết định số 63/QĐ-TTg ngày 13 tháng 01 năm 2010 của Thủ tướng Chính phủ phê quyệt Quy hoạch phát triển an toàn thông tin số quốc gia đến năm 2020;

Theo đề nghị của Giám đốc Sở Thông tin và Truyền thông tại Tờ trình số 130/TTr-STTTT ngày 02 tháng 10 năm 2020.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin trên địa bàn tỉnh Bình Phước.

Điều 2. Quyết định này có hiệu lực kể từ ngày 05/11/2020 và thay thế Quyết định số 30/2016/QĐ-UBND ngày 01/7/2016 của UBND tỉnh ban hành Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin trên địa bàn tỉnh Bình Phước.

Điều 3. Các ông/bà: Chánh Văn phòng UBND tỉnh; Giám đốc Sở Thông tin và Truyền thông; Thủ trưởng các sở, ban, ngành; 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./.

***Nơi nhận*:**
- Văn phòng Chính phủ;
- Bộ Thông tin và Truyền thông;
- Cục Kiểm tra văn bản - Bộ Tư pháp;
- TTTU, TTHĐND tỉnh;
- CT, các PCT UBND tỉnh;
- UBMTTQVN tỉnh;
- Như Điều 3;
- Trung tâm CNTT&TT;
- LĐVP, các phòng;
- Lưu: VT, P.KGVX,TD2.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Trần Tuệ Hiền

ỦY BAN NHÂN DÂN TỈNH BÌNH PHƯỚC	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc

QUY CHẾ
Bảo đảm an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin trên địa bàn tỉnh Bình Phước

(Ban hành kèm theo Quyết định số 29 /2020/QĐ-UBND ngày 20 tháng 10 năm 2020 của Ủy ban nhân dân tỉnh Bình Phước)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định về công tác đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin (CNTT) trong cơ quan Nhà nước, cơ quan đoàn thể, tổ chức chính trị, tổ chức chính trị xã hội, các doanh nghiệp Nhà nước, doanh nghiệp viễn thông, CNTT trên địa bàn tỉnh.

Điều 2. Đối tượng áp dụng

1. Các sở, ban, ngành; các đơn vị sự nghiệp công lập trực thuộc Ủy ban nhân dân (UBND) tỉnh; UBND các huyện, thị xã, thành phố; các cơ quan chuyên môn thuộc UBND các huyện, thị xã, thành phố; các hội đoàn thể; UBND các xã, phường, thị trấn trên địa bàn tỉnh (các cơ quan, đơn vị).

2. Cán bộ, công chức, viên chức, người lao động và các tổ chức, cá nhân có liên quan tham gia vận hành, khai thác các hệ thống thông tin tại cơ quan, đơn vị quy định tại khoản 1 Điều này.

3. Các doanh nghiệp cung cấp dịch vụ viễn thông, CNTT, Internet; các doanh nghiệp, tổ chức, cá nhân có tham gia vào các hoạt động ứng dụng CNTT của các cơ quan, đơn vị thuộc khoản 1 Điều này.

4. Các tổ chức, cá nhân có liên quan đến việc thực hiện đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin trên địa bàn tỉnh.

Điều 3. Giải thích từ ngữ

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

Máy chủ (server) là máy tính được kết nối với hệ thống mạng LAN, WAN hoặc mạng internet, có năng lực xử lý cao, trên đó có cài đặt các phần mềm để phục vụ cho các máy tính khác truy cập, yêu cầu cung cấp các dịch vụ và tài nguyên.

Điều 4. Quy định bảo đảm an toàn thông tin mạng

1. Các cơ quan, tổ chức, cá nhân và cán bộ, công chức, viên chức, người lao động chịu trách nhiệm trước pháp luật về nội dung thông tin đã chuyển đi

trên mạng nội bộ (LAN), mạng truyền số liệu chuyên dùng của các cơ quan Đảng và Nhà nước (mạng WAN) và mạng Internet.

2. Tuân thủ các nguyên tắc, các tiêu chuẩn, quy chuẩn kỹ thuật về bảo mật, an toàn thông tin số; chấp hành hướng dẫn của cơ quan chuyên môn quản lý Nhà nước về thông tin và truyền thông về các giải pháp, biện pháp, kỹ thuật về quản lý, bảo mật, an toàn thông tin số.

3. Các văn bản có nội dung "Mật" trở lên khi được soạn thảo phải trên thiết bị không kết nối mạng và được kiểm định; khi gửi, nhận qua mạng phải được thủ trưởng cơ quan, đơn vị cho phép và phải được mã hóa theo quy định của Luật Cơ yếu và các văn bản pháp luật liên quan.

4. Kết hợp nhiều biện pháp bảo đảm an toàn thông tin số, nhằm phát hiện và ngăn chặn kịp thời các nguy cơ mất an toàn thông tin.

5. Công tác đảm bảo an toàn thông tin mạng phải được thực hiện trên cơ sở có sự phối hợp chặt chẽ giữa các cơ quan, đơn vị và cá nhân.

Điều 5. Các hành vi bị nghiêm cấm

1. Lưu trữ trên máy tính có kết nối mạng các văn bản, tài liệu, số liệu thuộc bí mật Nhà nước hoặc những thông tin, tài liệu mật khác do pháp luật quy định và chỉ được phép cung cấp, chia sẻ cho bên thứ ba có thẩm quyền trong những trường hợp nhất định theo quy định của pháp luật.

2. Các hành vi phá hoại, sử dụng các phương tiện kỹ thuật gây nguy hại cho hệ thống thông tin, làm rối loạn, tê liệt một phần hoặc toàn bộ hệ thống thông tin của các cơ quan Nhà nước.

3. Truy nhập khai thác, sử dụng, phát tán, thay đổi, phá hủy các thông tin số thuộc sở hữu của các cá nhân, tổ chức khác khi chưa được phép của chủ sở hữu.

4. Tạo ra, cài đặt, phát tán vi rút, mã độc vào máy tính, mạng LAN, mạng truyền số liệu chuyên dùng của các cơ quan Nhà nước.

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

6. Bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã của tổ chức và cá nhân khác trên môi trường mạng.

7. Tổ chức, cá nhân, cán bộ công chức, viên chức che giấu tên của mình hoặc giả mạo tên của tổ chức, cá nhân khác khi gửi thông tin trên môi trường mạng LAN, mạng truyền số liệu chuyên dùng của các cơ quan Nhà nước.

8. Lợi dụng chức vụ, quyền hạn trong quản lý về an ninh thông tin để gây cản trở hoạt động hợp pháp của các chủ thể tham gia hệ thống mạng LAN, mạng truyền số liệu chuyên dùng của các cơ quan Nhà nước, dịch vụ hành chính công; xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức và công dân.

9. Nghiêm cấm tiết lộ tài khoản truy nhập, đấu nối, truy nhập trái phép vào các hệ thống thông tin dùng chung của tỉnh.

Chương II
NỘI DUNG BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Điều 6. Bảo đảm an toàn vật lý và môi trường

1. Các khu vực xử lý, lưu trữ thông tin, phương tiện xử lý thông tin, phương tiện bảo đảm an toàn thông tin mạng phải được đặt ở vị trí an toàn, bảo vệ bằng tường bao và kiểm soát ra vào, bảo đảm chỉ có người có nhiệm vụ mới được vào và phải có nội quy riêng khi làm việc trong các khu vực này.

2. Các khu vực tại khoản 1 Điều này phải có biện pháp bảo vệ phòng chống cháy nổ, ngập lụt, động đất, chống sét, tác động của môi trường và các thảm họa khác do thiên nhiên và con người gây ra.

3. Khu vực an toàn, bảo mật phải được kiểm soát và cách ly với khu vực sử dụng chung.

4. Bảo đảm thiết bị lưu trữ dữ liệu quan trọng, phần mềm bản quyền lưu trữ trên thiết bị phải được kiểm tra, xóa hoặc ghi đè không có khả năng khôi phục trước khi loại bỏ hoặc tái sử dụng cho mục đích khác.

Điều 7. Bảo đảm an toàn trong phát triển hệ thống thông tin, trao đổi thông tin trên môi trường mạng

1. Các hoạt động liên quan đến xây dựng, thiết lập, quản lý, vận hành, nâng cấp mở rộng hệ thống thông tin phải thực hiện xác định cấp độ và phương án bảo đảm an toàn thông tin theo quy định tại Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ và hướng dẫn tại Thông tư số 03/2017/TT-BTTTT ngày 24 tháng 4 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông.

2. Phân loại thông tin theo các tiêu chí về giá trị và tầm quan trọng, tần suất sử dụng, thời gian lưu trữ để áp dụng phương thức bảo vệ thích hợp.

3. Việc gửi thông tin trên mạng phải bảo đảm:

a) Không giả mạo nguồn gốc gửi thông tin.

b) Tuân thủ Quy định này và quy định của pháp luật có liên quan.

4. Khi kết nối từ xa vào máy chủ để quản trị, phải sử dụng phương thức kết nối có mã hóa.

5. Sử dụng Mạng truyền số liệu chuyên dùng của tỉnh để truy cập, khai thác các hệ thống thông tin dùng chung của tỉnh.

6. Chỉ sử dụng thư điện tử công vụ và các công cụ trao đổi thông tin do các cơ quan Nhà nước hoặc tổ chức có thẩm quyền cung cấp để trao đổi thông tin, tài liệu trong hoạt động công vụ.

Điều 8. Quản lý truy cập

1. Các hệ thống thông tin, mạng phải sử dụng tường lửa để ngăn chặn và phát hiện các xâm nhập trái phép vào hệ thống nội bộ.

2. Phải có quy định về quản lý truy cập vào hệ thống thông tin, mạng tại mỗi đơn vị.

3. Mỗi tài khoản truy cập vào hệ thống thông tin chỉ được cấp cho một người quản lý và sử dụng.

4. Cán bộ, công chức, viên chức và người lao động chỉ được phép truy cập thông tin theo đúng chức năng, trách nhiệm, quyền hạn của mình.

5. Các hệ thống thông tin phải giới hạn số lần đăng nhập sai liên tiếp vào hệ thống. Thiết lập chế độ tự động khoá tạm thời tài khoản nếu liên tục đăng nhập sai vượt quá số lần quy định.

6. Hủy bỏ quyền truy cập vào hệ thống thông tin, thu hồi lại tất cả các tài sản liên quan tới hệ thống thông tin của cơ quan (khóa, thẻ nhận dạng, thư mục lưu trữ, thư điện tử công vụ, máy vi tính, tài khoản) khi cán bộ, công chức, viên chức và người lao động chuyển công tác, nghỉ hưu hoặc chấm dứt lao động hợp đồng.

7. Tất cả máy trạm, máy chủ phải được đặt mật khẩu truy cập và thiết lập chế độ tự động bảo vệ màn hình sau tối đa 10 phút không sử dụng.

8. Khi thiết lập mạng không dây trong nội bộ đơn vị, phải đặt mật khẩu truy cập vào mạng không dây. Mật khẩu được đặt theo quy định tại khoản 9 Điều này.

9. Mật khẩu truy cập vào các hệ thống thông tin phải có độ phức tạp cao (có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự hoa, ký tự số và ký tự đặc biệt) và phải thiết lập chính sách hết hạn mật khẩu phù hợp với mức độ quan trọng của hệ thống thông tin.

10. Không đặt chế độ tự động ghi nhớ mật khẩu của các trình duyệt trong mọi trường hợp sử dụng.

Điều 9. Phòng chống phần mềm độc hại

1. Tất cả các máy trạm, máy chủ phải được trang bị phần mềm phòng chống phần mềm độc hại. Các phần mềm phòng chống phần mềm độc hại phải được thiết lập chế độ tự động cập nhật; chế độ tự động quét phần mềm độc hại khi sao chép, mở các tập tin.

2. Hệ điều hành, phần mềm cài đặt trên máy chủ phải được cập nhật vá lỗ hổng bảo mật thường xuyên, kịp thời.

3. Cán bộ, công chức, viên chức và người lao động không được tự ý gỡ bỏ các phần mềm phòng, chống phần mềm độc hại trên máy tính trạm khi chưa có sự đồng ý của người có thẩm quyền trong cơ quan.

4. Tất cả các máy tính của đơn vị phải được cấu hình vô hiệu hóa tính năng tự động thực thi (autoplay) các tập tin trên các thiết bị lưu trữ di động.

5. Tất cả các tập tin, thư mục phải được quét phần mềm độc hại trước khi sao chép, sử dụng.

6. Máy chủ chỉ được dùng để cài đặt các phần mềm, dịch vụ dùng chung của cơ quan, đơn vị; không cài đặt phần mềm không rõ nguồn gốc, phần mềm phục vụ mục đích cá nhân và mục đích khác, không phục vụ công việc. Các hệ điều hành cài trên máy chủ, máy trạm phải có bản quyền của đơn vị cung cấp hệ điều hành; không sử dụng hệ điều hành đã bị bẻ khóa.

7. Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại trên máy trạm, người sử dụng phải kịp thời thông báo cho bộ phận có trách nhiệm của đơn vị để xử lý.

Điều 10. Sao lưu dữ liệu dự phòng

1. Các cơ quan phải ban hành, thực hiện quy trình sao lưu dữ liệu dự phòng và phục hồi phù hợp cho các hệ thống thông tin và dữ liệu.

2. Các cơ quan phải lập danh sách dữ liệu cần sao lưu, phân loại theo thời gian lưu trữ, thời gian sao lưu, phương pháp sao lưu và thời gian kiểm tra khả năng phục hồi hệ thống từ dữ liệu sao lưu.

3. Dữ liệu sao lưu phải được lưu trữ an toàn và được kiểm tra thường xuyên bảo đảm khả năng sẵn sàng cho việc sử dụng khi cần. Có kế hoạch kiểm tra khả năng phục hồi từ dữ liệu sao lưu.

Điều 11. Quản lý nhật ký trong quá trình vận hành hệ thống thông tin

1. Các cơ quan phải thực hiện việc ghi nhật ký (log) các thiết bị mạng, bảo mật, máy chủ, phần mềm ứng dụng, hệ điều hành, cơ sở dữ liệu. Bảo đảm các sự kiện xảy ra đều được ghi nhận và lưu giữ.

2. Nhật ký phải được bảo vệ an toàn phục vụ công tác kiểm tra, phân tích khi cần thiết.

3. Các công việc tối thiểu cần phải được ghi nhật ký gồm: Quá trình truy cập hệ thống; tạo, cập nhật hoặc xóa dữ liệu; các hành vi xem, thiết lập cấu hình hệ thống; việc thiết lập các kết nối bất thường vào và ra hệ thống; thay đổi quyền truy cập hệ thống.

4. Thường xuyên theo dõi nhật ký của hệ thống và các sự kiện khác có liên quan để đánh giá, báo cáo mức độ nghiêm trọng của các rủi ro có thể xảy ra.

Điều 12. Quản lý sự cố

1. Phân loại mức độ nghiêm trọng của các sự cố, bao gồm:

a) Thấp: sự cố gây ảnh hưởng cá nhân và không làm gián đoạn hay đình trệ hoạt động chính của cơ quan.

b) Trung bình: sự cố ảnh hưởng đến một nhóm người dùng nhưng không gây gián đoán hay đình trệ hoạt động chính của cơ quan.

c) Cao: sự cố làm cho thiết bị, phần mềm hay hệ thống không thể sử dụng được và có ảnh hưởng đến hoạt động của cơ quan.

d) Khẩn cấp: sự cố ảnh hưởng đến sự liên tục của nhiều hoạt động chính của cơ quan.

2. Trường hợp có sự cố nghiêm trọng ở mức độ cao, khẩn cấp hoặc vượt quá khả năng khắc phục của đơn vị, lãnh đạo đơn vị phải chỉ đạo tạm dừng hoạt động của hệ thống đồng thời báo cáo khẩn cấp cho cơ quan cấp trên quản lý trực tiếp và Sở Thông tin và Truyền thông để được hướng dẫn, hỗ trợ.

3. Quá trình xử lý sự cố phải được ghi chép và lưu trữ tại đơn vị; bảo toàn bằng chứng, chứng cứ phục vụ cho việc kiểm tra, xử lý, khắc phục và phòng ngừa sự cố. Trong trường hợp sự cố có liên quan đến các vi phạm pháp luật, đơn vị có trách nhiệm thu thập và cung cấp chứng cứ cho cơ quan có thẩm quyền theo quy định của pháp luật.

4. Quy trình ứng cứu sự cố thực hiện theo quy định tại Điều 11 Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông.

Điều 13. Bảo vệ bí mật nhà nước trong hoạt động ứng dụng công nghệ thông tin

1. Không được sử dụng máy tính nối mạng 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 thông tin bí mật Nhà nước trên mạng.

2. Không được in, sao chụp tài liệu bí mật Nhà nước trên các thiết bị kết nối mạng.

3. Khi sửa chữa, khắc phục sự cố của máy tính dùng soạn thảo văn bản mật, các cơ quan phải báo cáo và có sự giám sát, quản lý chặt chẽ của người có thẩm quyền trong cơ quan.

4. Có biện pháp quản lý chặt chẽ trong việc sử dụng và thanh lý tài sản, các trang thiết bị công nghệ thông tin lưu trữ các thông tin thuộc danh mục bí mật Nhà nước. Tuân thủ các quy định có liên quan về công tác bảo vệ bí mật nhà nước.

5. Không trao đổi thông tin, gửi dữ liệu mang nội dung bí mật Nhà nước qua mạng xã hội, thư điện tử công vụ, thư điện tử công cộng dưới mọi hình thức, trừ trường hợp thông tin, dữ liệu đã được mã hóa theo quy định của Luật Cơ yếu.

Điều 14. Quy trình phối hợp ứng cứu sự cố mạng bảo đảm an toàn thông tin số

1. Quy trình xử lý khẩn cấp

Khi phát hiện hệ thống có nguy cơ mất an toàn thông tin như: Hệ thống hoạt động chậm bất thường, không truy cập được hệ thống ứng dụng, nội dung cổng/trang thông tin điện tử hoặc giao diện ứng dụng bị thay đổi, các sự cố khác có liên quan thực hiện các bước cơ bản:

a) Bước 1: ngắt kết nối hệ thống máy chủ ra khỏi hệ thống mạng, báo cáo sự cố đến Thủ trưởng cơ quan, đơn vị.

b) Bước 2: sao chép nhật ký truy cập của người dùng (logfile) và toàn bộ dữ liệu của hệ thống ra thiết bị lưu trữ (phục vụ cho công tác phân tích).

c) Bước 3: khôi phục lại hệ thống, hoặc sử dụng hệ thống dự phòng và chuyển dữ liệu sao lưu dự phòng (backup) mới nhất để hệ thống hoạt động.

d) Bước 4: tổng hợp, báo cáo sự cố và nội dung khắc phục gửi về Đội ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh (Đội ứng cứu) để tổng hợp.

2. Nguyên tắc phối hợp trong ứng cứu sự cố

a) Đơn vị vận hành hệ thống thông tin

- Thực hiện các bước khắc phục sự cố theo khoản 1 Điều này.

- Các sự cố vượt quá khả năng xử lý, đơn vị thông báo đến Đội ứng cứu để hỗ trợ khắc phục và thực hiện báo cáo sự cố mạng.

b) Đội ứng cứu

- Tiếp nhận thông tin, báo cáo sự cố mất an toàn thông tin của đơn vị.

- Phản hồi cho đơn vị, cá nhân gửi thông báo, báo cáo ban đầu ngay sau khi nhận được để xác nhận về việc đã nhận được thông báo, báo cáo sự cố.

- Thẩm tra, xác minh, phân loại và giám sát diễn biến tình hình ứng cứu sự cố an toàn thông tin mạng để lựa chọn phương án ứng cứu phù hợp hoặc đề xuất với Ban Chỉ đạo xây dựng Chính quyền điện tử tỉnh hướng giải quyết trong trường hợp vượt thẩm quyền.

- Chủ động hỗ trợ ngay đơn vị cần ứng cứu, xử lý sự cố trong khả năng và trách nhiệm của mình, cử cán bộ kỹ thuật của Đội ứng cứu có mặt tại đơn vị báo sự cố để phối hợp, hướng dẫn, ghi nhận giải quyết sự cố, trong trường hợp sự cố phức tạp, nguy cơ cao về an toàn thông tin mà không thể hướng dẫn, trao đổi qua điện thoại, email với đơn vị bị sự cố.

- Tổng hợp, báo cáo Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam - VNCERT (Cơ quan điều phối quốc gia) theo quy định và báo cáo đột xuất khi có yêu cầu.

c) Sở Thông tin và Truyền thông báo cáo về UBND tỉnh; đồng thời thông báo đến Bộ Thông tin và Truyền thông (qua Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam) để được hỗ trợ khắc phục các sự cố vượt quá khả năng xử lý của địa phương.

Chương III
TRÁCH NHIỆM ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG

Điều 15. Trách nhiệm của Ban Chỉ đạo xây dựng Chính quyền điện tử tỉnh

Đảm nhiệm chức năng Ban Chỉ đạo ứng cứu sự cố an toàn thông tin mạng tại tỉnh; có trách nhiệm, quyền hạn theo quy định tại Điều 5 Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 2017 của Thủ tướng Chính Phủ.

Điều 16. Trách nhiệm của cán bộ, công chức trong cơ quan Nhà nước

1. Trách nhiệm của cán bộ, công chức, viên chức và người lao động

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

b) Tự quản lý, bảo quản, bảo đảm an toàn cho các thiết bị mà mình được giao sử dụng.

c) Khi phát hiện sự cố mất an toàn thông tin mạng phải thông báo ngay với cấp trên và cán bộ chuyên trách, phụ trách CNTT để kịp thời ngăn chặn, xử lý.

d) Tham gia đầy đủ các chương trình đào tạo, tập huấn về an toàn thông tin mạng do UBND tỉnh chỉ đạo hoặc cơ quan chuyên trách về an toàn thông tin tổ chức.

2. Trách nhiệm của cán bộ chuyên trách, phụ trách công nghệ thông tin

Ngoài các quy định tại khoản 1 Điều này, cán bộ chuyên trách, phụ trách CNTT có trách nhiệm:

a) Tham mưu với lãnh đạo cơ quan thực hiện các nội dung của Quy định này và các quy định pháp luật có liên quan đến an toàn thông tin.

b) Tham mưu lãnh đạo cơ quan ban hành các quy định, quy trình nội bộ, triển khai các giải pháp kỹ thuật bảo đảm an toàn thông tin mạng.

c) Trực tiếp thiết lập các biện pháp kỹ thuật bảo đảm an toàn cho hạ tầng kỹ thuật, hệ thống thông tin trong cơ quan, đơn vị mình; hướng dẫn cán bộ, công chức, viên chức và người lao động trong cơ quan, đơn vị tuân thủ các biện pháp bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng CNTT.

d) Thực hiện việc giám sát, đánh giá, ghi nhật ký và báo cáo ngay thủ trưởng cơ quan các sự cố mất an toàn thông tin mạng và mức độ nghiêm trọng của các sự cố đó.

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

Điều 17. Trách nhiệm của các cơ quan Nhà nước trên địa bàn tỉnh

1. Thủ trưởng cơ quan, đơn vị có trách nhiệm tổ chức thực hiện các quy định tại Quy định này và chịu trách nhiệm trước UBND tỉnh trong công tác bảo đảm an toàn thông tin mạng của đơn vị mình.

2. Phân công bộ phận hoặc cán bộ chuyên trách bảo đảm an toàn thông tin mạng của đơn vị; tạo điều kiện để các cán bộ phụ trách an toàn thông tin mạng được học tập, nâng cao trình độ về an toàn thông tin mạng; thường xuyên tổ chức quán triệt các quy định về an toàn thông tin mạng trong cơ quan; xác định các yêu cầu, trách nhiệm đảm bảo an toàn thông tin mạng đối với các vị trí cần tuyển dụng hoặc phân công.

3. Ban hành quy định, quy trình nội bộ về bảo đảm an toàn thông tin mạng phù hợp với Quy định này và các quy định của pháp luật.

4. Các cơ quan, đơn vị có trách nhiệm thực hiện xác định cấp độ an toàn thông tin và đảm bảo an toàn cho hệ thống thông tin của đơn vị quản lý theo quy định.

5. Phối hợp, cung cấp thông tin và tạo điều kiện cho các đơn vị có thẩm quyền triển khai công tác kiểm tra khắc phục sự cố an toàn thông tin mạng kịp thời, nhanh chóng và đạt hiệu quả.

6. Phối hợp chặt chẽ với Công an tỉnh, Sở Thông tin và Truyền thông và các đơn vị liên quan trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn thông tin mạng.

7. Các cơ quan, đơn vị thuộc đối tượng tại Điều 2 Quy định này gửi báo cáo định kỳ 06 tháng (trước ngày 10/6), 01 năm (trước ngày 10/12) hoặc đột xuất khi có yêu cầu về công tác bảo đảm an toàn thông tin theo phạm vi quản lý về Sở Thông tin và Truyền thông.

Điều 18. Trách nhiệm của Sở Thông tin và Truyền thông

1. Tham mưu và chịu trách nhiệm trước UBND tỉnh trong công tác đảm bảo an toàn cho các hệ thống thông tin trên địa bàn tỉnh.

2. Xây dựng và triển khai các kế hoạch, chương trình, dự án đầu tư, đào tạo về an toàn thông tin trong ứng dụng CNTT trên địa bàn tỉnh.

3. Tùy theo mức độ sự cố, phối hợp Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam và các đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố an toàn thông tin trên địa bàn tỉnh; cảnh báo các vấn đề về an toàn thông tin trong các cơ quan Nhà nước trên địa bàn tỉnh.

4. Quản lý vận hành, hướng dẫn kết nối mạng truyền số liệu chuyên dùng của các cơ quan Đảng và Nhà nước trên địa bàn tỉnh; xử lý các vấn đề liên quan sự cố mạng truyền số liệu chuyên dùng.

5. Hướng dẫn, hỗ trợ sao lưu dự phòng các thông tin, cơ sở dữ liệu của các cơ quan Nhà nước một cách an toàn.

6. Hướng dẫn, đôn đốc, theo dõi, kiểm tra các đơn vị xây dựng Quy chế và thực hiện việc đảm bảo an toàn cho hệ thống thông tin theo quy định.

7. Tuyên truyền và định hướng tuyên truyền về công tác bảo đảm an toàn thông tin.

8. Hằng năm, tổ chức đào tạo chuyên sâu về an toàn thông tin mạng cho cán bộ, công chức chuyên trách CNTT đảm bảo an toàn thông tin mạng của các cơ quan, đơn vị.

9. Cung cấp, hỗ trợ các cơ quan đơn vị thiết bị CNTT soạn thảo và lưu trữ văn bản mật. Chủ trì, phối hợp với Công an tỉnh thẩm định; bảo hành, bảo trì; đảm bảo an toàn thông tin của thiết bị CNTT soạn thảo và lưu trữ văn bản mật của các cơ quan, đơn vị.

10. Khảo sát, triển khai, xây dựng mô hình kết nối mạng nội bộ (LAN) đảm bảo an toàn thông tin chung cho các cơ quan, đơn vị triển khai thực hiện.

11. Phối hợp với Công an tỉnh và các đơn vị có liên quan tổ chức kiểm tra định kỳ đảm bảo an toàn thông tin mạng, hệ thống thông tin theo cấp độ của các cơ quan, đơn vị.

12. Hướng dẫn các cơ quan, đơn vị về khung báo cáo; định kỳ tổng hợp, báo cáo Bộ Thông tin và Truyền thông, UBND tỉnh trước ngày 15/6 và ngày 15/12 hằng năm.

Điều 19. Trách nhiệm của Công an tỉnh

1. 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 quản lý, kiểm soát, phòng ngừa, đấu tranh, ngăn chặn các loại tội phạm lợi dụng hệ thống thông tin gây phương hại đến an toàn thông tin mạng trong cơ quan Nhà nước.

- Tổ chức Đoàn kiểm tra về an toàn thông tin mạng để kịp thời phát hiện, xử lý các hành vi vi phạm theo quy định của pháp luật.

2. Phối hợp Sở Thông tin và Truyền thông thẩm định; bảo hành, bảo trì; đảm bảo an toàn thông tin của thiết bị CNTT soạn thảo và lưu trữ văn bản mật của các cơ quan, đơn vị.

3. Cử cán bộ phối hợp, tham gia đoàn kiểm tra, đánh giá công tác đảm bảo an toàn thông tin trong hoạt động ứng dụng CNTT của các cơ quan, đơn vị; điều tra và xử lý các trường hợp vi phạm các quy định về an toàn thông tin mạng theo thẩm quyền.

4. Cử cán bộ chuyên môn phối hợp với Sở Thông tin và Truyền thông kiểm tra đột xuất các cơ quan, đơn vị khi phát hiện có dấu hiệu vi phạm pháp luật về an toàn thông tin trong hoạt động ứng dụng CNTT theo đúng quy định của pháp luật.

Điều 20. Trách nhiệm của Sở Tài chính, Kế hoạch và Đầu tư

1. Sở Tài chính: tham mưu UBND tỉnh trong việc bố trí kinh phí cho các hoạt động đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng CNTT của các cơ quan Nhà nước trên địa bàn tỉnh.

2. Sở Kế hoạch và Đầu tư: tham mưu UBND tỉnh bố trí vốn đầu tư đối với các chương trình, dự án, CNTT có sử dụng vốn đầu tư công.

Điều 21. Trách nhiệm của các doanh nghiệp cung cấp dịch vụ viễn thông, công nghệ thông tin và Internet cho các cơ quan quản lý Nhà nước trên địa bàn tỉnh

1. Đầu tư xây dựng, trang bị hạ tầng kỹ thuật đáp ứng đầy đủ các yêu cầu, tiêu chuẩn kỹ thuật theo quy định của Bộ Thông tin và Truyền thông về an toàn thông tin và các nội dung quy định tại Quy chế này.

2. Phối hợp với Sở Thông tin và Truyền thông để tham gia các hoạt động điều phối, ứng cứu, khắc phục sự cố thông tin đảm bảo an toàn thông tin mạng cho các cơ quan, đơn vị trong quá trình sử dụng, khai thác sử dụng dịch vụ.

3. Viễn thông Bình Phước:

a) Đảm bảo đúng trách nhiệm hợp đồng với Sở Thông tin và Truyền thông, bảo đảm mạng truyền số liệu chuyên dùng cung cấp cho các cơ quan, đơn vị được thông suốt, ổn định.

b) Chịu hoàn toàn trách nhiệm nếu có sự cố xảy ra mà thời gian xử lý vượt quá 04 giờ kể từ thời điểm nhận được thông tin sự cố.

c) Chịu hoàn toàn trách nhiệm trước UBND tỉnh về chất lượng dịch vụ nếu để số sự cố xảy ra quá 03 lần/tháng/đơn vị.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 22. Điều khoản thi hành

1. Đối với các nội dung khác liên quan đến công tác đảm bảo an toàn thông tin trong hoạt động ứng dụng CNTT không được quy định trong Quy chế này thì thực hiện theo quy định về đảm bảo an toàn thông tin trong hoạt động ứng dụng CNTT đã được quy định trong các văn bản quy phạm pháp luật theo quy định.

2. Trong quá trình thực hiện, nếu có những vấn đề cần sửa đổi, bổ sung, các đơn vị gửi về Sở Thông tin và Truyền thông để tổng hợp, báo cáo UBND tỉnh xem xét, điều chỉnh cho phù hợp./.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Trần Tuệ Hiền