ỦY BAN NHÂN DÂN TỈNH LONG AN	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 19 /2014/QĐ-UBND	*Long An, ngày 03 tháng 10 năm 2014*

QUYẾT ĐỊNH

Ban hành Quy định đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước trên địa bàn tỉnh Long An

ỦY BAN NHÂN DÂN TỈNH LONG AN

Căn cứ Luật Tổ chức HĐND và UBND ngày 26/11/2003;

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

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

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

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

Căn cứ Thông tư liên tịch số 06/2008/TTLT-BTTTT-BCA ngày 28/11/2008 của Bộ Thông tin và Truyền thông và Bộ Công an về bảo đảm an toàn cơ sở hạ tầng và an ninh thông tin trong hoạt động bưu chính, viễn thông và công nghệ thông tin;

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;

Theo đề nghị của Sở Thông tin và Truyền thông tại tờ trình số 870/TTr-STTTT ngày 23/9/2014,

QUYẾT ĐỊNH:

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

Điều 2. Giao Sở Thông tin và Truyền thông chủ trì, phối hợp với các cơ quan, đơn vị tổ chức triển khai, hướng dẫn, đôn đốc, kiểm tra việc thực hiện nội dung Quyết định này.

Quyết định này có hiệu lực thi hành sau 10 (mười) ngày kể từ ngày ký và thay thế Quyết định số 49/2010/QĐ-UBND ngày 01/12/2010 của UBND tỉnh về việc ban hành quy định về đảm bảo an toàn, an ninh thông tin và bảo mật trên môi trường mạng trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Long An.

Điều 3. Chánh Văn phòng UBND tỉnh; Thủ trưởng các sở ngành tỉnh; Chủ tịch UBND các huyện, thị xã, thành phố, các xã, phường, thị trấn và các đơn vị, 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;
- Cục Kiểm tra văn bản QPPL-Bộ Tư pháp;
- TT.TU, TT.HĐND tỉnh;
- TT.UBMTTQ và đoàn thể tỉnh;
- CT, PCT.UBND tỉnh;
- Trung tâm Công báo tỉnh;
- Cổng thông tin điện tử tỉnh;
- Phòng NCVX;
- Lưu: VT, STTTT, M.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Đỗ Hữu Lâm

ỦY BAN NHÂN DÂN TỈNH LONG AN	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc

QUY ĐỊNH

Đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước trên địa bàn tỉnh Long An

(Kèm theo Quyết định số 19 /2014/QĐ-UBND ngày 03 / 10 /2014 của UBND tỉnh)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi và đối tượng áp dụng

1. Quy định này quy định về công tác đảm bảo an toàn thông tin số và trách nhiệm của tổ chức, cá nhân có liên quan trong hoạt động ứng dụng công nghệ thông tin (CNTT) trên môi trường mạng của các cơ quan nhà nước trên địa bàn tỉnh Long An.

2. Quy định này áp dụng đối với:

a) Các cơ quan, đơn vị sau:

- Ủy ban nhân dân (UBND) các cấp;

- Các sở, ngành tỉnh; các đơn vị sự nghiệp thuộc UBND tỉnh; các tổ chức đoàn thể tỉnh;

- Các cơ quan chuyên môn, đơn vị thuộc UBND cấp huyện.

b) Cán bộ, công chức, viên chức (CBCC-VC), người lao động trong các cơ quan, đơn vị nêu tại điểm a khoản này và các tổ chức, cá nhân có liên quan đến hoạt động ứng dụng CNTT trên môi trường mạng của các cơ quan nhà.

Điều 2. Giải thích từ ngữ

1. *Mạng* là khái niệm chung dùng để chỉ mạng viễn thông (cố định, di động, Internet), mạng máy tính (WAN, LAN). Trong Quy định này các vùng mạng ngoài (Public Zone), vùng mạng DMZ, vùng mạng làm việc (Working Zone) hiểu như sau:

a) *Vùng mạng ngoài (Public Zone)* là vùng mạng Internet ;

b) *Vùng DMZ (DMZ - DeMilitarized Zone)* là một vùng mạng trung lập giữa mạng nội bộ và mạng Internet, chứa các thông tin cho phép người dùng từ Internet truy xuất vào mạng nội bộ. Các thiết bị tại vùng này bao gồm các thiết bị mạng phục vụ cho vùng và các máy chủ ứng dụng;

c) *Vùng làm việc (Working Zone)* là vùng mạng cục bộ của cơ quan và nơi bố trí các mạng nội bộ ảo trực thuộc mạng nội bộ của đơn vị. Các mạng nội bộ ảo này có thể kết nối với nhau thông qua lớp trung gian hoặc kết nối trực tiếp với nhau.

2. *An toàn thông tin* là sự bảo vệ thông tin và hệ thống thông tin tránh bị truy cập, 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.

3. *Đảm bảo an toàn thông tin* là đảm bảo tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin, trong đó:

a) *Tính bảo mật* là đảm bảo thông tin chỉ có thể được truy nhập bởi những người được cấp quyền sử dụng ;

b) *Tính nguyên vẹn* là bảo vệ sự chính xác và đầy đủ của thông tin và các phương pháp xử lý;

c) *Tính khả dụng* là đảm bảo những người được cấp quyền có thể truy nhập thông tin và các tài sản liên quan ngay khi có nhu cầu.

4. *Hệ thống thông tin* là tập hợp thiết bị phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin.

5. *Bản ghi nhật ký hệ thống (Logfile)* là tập tin được tạo ra trên mỗi thiết bị của hệ thống thông tin như: Tường lửa, máy chủ ứng dụng,... có chứa tất cả thông tin về các hoạt động xảy ra trên thiết bị đó. Bản ghi nhật ký hệ thống dùng để phân tích những sự kiện đã xảy ra, truy tìm nguồn gốc và kết quả để từ đó có các biện pháp xử lý thích hợp.

6. *Người dùng* là cán bộ, công chức, viên chức, nhân viên hợp đồng của cơ quan, đơn vị được sử dụng máy tính truy cập vào các hệ thống ứng dụng CNTT tại cơ quan, đơn vị để xử lý công việc.

7. *ISO/IEC 27001 (ISMS)* là tiêu chuẩn về hệ thống quản lý an toàn thông tin do Tổ chức tiêu chuẩn hóa quốc tế và Ủy ban kỹ thuật điện quốc tế ban hành.

8. *Đánh giá an toàn thông tin* là việc xác định, phân tích nguy cơ mất an toàn thông tin có thể có và dự báo mức độ, phạm vi ảnh hưởng và khả năng gây thiệt hại khi xảy ra sự cố mất an toàn thông tin.

9. *Tấn công từ chối dịch vụ* là một kiểu tấn công mà một người làm cho một hệ thống không thể sử dụng, hoặc làm cho hệ thống đó chậm đi một cách đáng kể với người dùng bình thường, bằng cách làm quá tải tài nguyên của hệ thống.

10. *Máy tính làm việc bao gồm*: Máy chủ, máy quản trị và máy tính cá nhân do cơ quan cấp cho người dùng để phục vụ công việc và được quản lý theo các quy định của pháp luật về quản lý tài sản nhà nước.

Điều 3. Nguyên tắc chung về đảm bảo an toàn thông tin

1. Các cơ quan, đơn vị, CBCC-VC tham gia hoạt động trên môi trường mạng không được xâm phạm an toàn thông tin của cơ quan, đơn vị, CBCC-VC khác; trường hợp phát hiện hành vi xâm phạm an toàn thông tin hoặc sự cố mất an toàn thông tin, cơ quan, đơn vị, CBCC-VC có trách nhiệm thông báo kịp thời cho cơ quan chức năng liên quan, đồng thời tiến hành các biện pháp khắc phục nhanh chóng, hạn chế thiệt hại tại cơ quan, đơn vị.

2. Các cơ quan, đơn vị, CBCC-VC chịu trách nhiệm bảo đảm an toàn thông tin đối với thông tin và hệ thống thông tin thuộc thẩm quyền quản lý; tuân thủ các nguyên tắc, các tiêu chuẩn, quy chuẩn kỹ thuật về bảo mật, an toàn thông tin số; chịu sự quản lý, thanh tra, kiểm tra và thực hiện các yêu cầu về bảo

đảm an toàn thông tin của cơ quan nhà nước có thẩm quyền; phối hợp với cơ quan quản lý nhà nước có thẩm quyền và tổ chức, cá nhân có liên quan trong việc bảo đảm an toàn thông tin trên môi trường mạng.

3. Các cơ quan, đơn vị có liên quan phải triển khai các giải pháp tăng cường khả năng phòng, chống các nguy cơ tấn công, xâm nhập các hệ thống thông tin; ngăn chặn, khắc phục kịp thời các sự cố mất an toàn thông tin trên mạng máy tính và các hệ thống thông tin thuộc thẩm quyền quản lý. Ngăn ngừa việc lộ, lọt tài liệu, thông tin bí mật nhà nước.

Điều 4. Các hành vi bị nghiêm cấm

1. Lợi dụng mạng và thông tin trên mạng nhằm mục đích:

a) Tuyên truyền chống lại Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; thực hiện các hành vi xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, gây ảnh hưởng xấu tới thuần phong, mỹ tục của dân tộc;

b) Tiết lộ bí mật nhà nước và những bí mật khác do pháp luật quy định;

c) Đưa thông tin xuyên tạc, vu khống, xúc phạm uy tín của tổ chức, danh dự và nhân phẩm của cá nhân.

2. Ngăn chặn trái phép việc truyền tải thông tin trên mạng; can thiệp trái phép, gây nguy hại, xóa, thay đổi, sửa chữa làm sai lệch thông tin trên mạng.

3. Đánh cắp và sử dụng trái phép mật khẩu, khoá mật mã, thông tin riêng của tổ chức, cá nhân; ngăn cản bất hợp pháp việc truy nhập thông tin của tổ chức, cá nhân.

4. Cản trở bất hợp pháp, gây ảnh hưởng tới hoạt động bình thường của hệ thống thông tin; Lợi dụng sơ hở, điểm yếu của hệ thống thông tin để vô hiệu hóa, vượt qua biện pháp kiểm soát truy cập, tấn công, chiếm quyền điều khiển trái phép đối với hệ thống thông tin.

5. Phát tán thư rác, thư giả mạo, tin nhắn rác, phần mềm độc hại, thiết lập hệ thống thông tin giả mạo, lừa đảo.

6. Các hành vi trái pháp luật khác liên quan đến hoạt động đảm bảo an toàn thông tin.

Chương II
NỘI DUNG ĐẢM BẢO AN TOÀN THÔNG TIN
Mục 1
ĐỐI VỚI CƠ SỞ HẠ TẦNG

Điều 5. Đảm bảo an toàn cơ sở hạ tầng công nghệ thông tin

1. Bảo vệ cơ sở hạ tầng CNTT của cơ quan, đơn vị nhằm ngăn chặn các hoạt động tấn công, đột nhập, phá hoại; phòng, chống sự cố do cháy, nổ và các sự cố khác do thiên tai gây ra.

2. Triển khai các giải pháp và hệ thống thiết bị dự phòng để bảo đảm cơ sở hạ tầng CNTT hoạt động liên tục và an toàn.

3. Triển khai các biện pháp ngăn chặn việc sử dụng, lợi dụng mạng lưới, thiết bị, các công cụ phần cứng, phần mềm để cản trở, gây nhiễu, gây rối loạn,

làm hư hỏng, hủy hoại hoạt động cơ sở hạ tầng CNTT; phòng, chống virus, thư rác, phần mềm gián điệp; phòng, chống hành vi đánh cắp và sử dụng trái phép mật khẩu, khoá mật mã, thông tin riêng của các tổ chức, cá nhân.

Điều 6. Đảm bảo an toàn sử dụng máy tính làm việc

1. Máy tính làm việc chỉ được cài đặt phần mềm thông dụng do cán bộ chuyên trách CNTT quản lý hoặc những phần mềm được cung cấp theo các chương trình ứng dụng CNTT của cơ quan nhà nước có thẩm quyền; hệ điều hành được cập nhật bản vá lỗi kịp thời, cài đặt phần mềm phòng chống, diệt virus có bản quyền và cập nhật phiên bản mới nhất; thường xuyên rà quét để phát hiện và loại bỏ mã độc trong máy tính.

2. Máy tính dùng để quản trị hệ thống chỉ được cài đặt các phần mềm cần thiết phục vụ cho hoạt động quản trị hệ thống, đặt trong vùng mạng phục vụ công tác quản trị hệ thống và chỉ được cấp quyền truy cập cho các cá nhân được giao trách nhiệm quản trị hệ thống.

3. Người dùng không tự ý thay đổi cấu hình máy tính, kết nối máy tính cá nhân do cơ quan cấp vào các mạng thông tin khác (ngoài hệ thống thông tin của cơ quan); không tự ý sử dụng máy tính cấp cho người sử dụng khác; phải sử dụng mật khẩu cho tài khoản đăng nhập vào máy tính và tuân thủ các quy định tại Điều 13 Quy định này.

4. Người dùng khi sử dụng các thiết bị lưu trữ di động cá nhân phải tiến hành quét virus trước khi đưa vào sử dụng trên máy tính làm việc của mình.

Điều 7. Đảm bảo an toàn hệ thống mạng nội bộ

1. Mạng nội bộ của các cơ quan, đơn vị phải được kết nối mạng truyền số liệu chuyên dùng của tỉnh để đảm bảo an toàn thông tin theo quy định về quản lý, vận hành, sử dụng và bảo đảm an toàn thông tin Mạng truyền số liệu chuyên dùng trong các cơ quan nhà nước trên địa bàn tỉnh Long An.

2. Hệ thống mạng nội bộ của cơ quan, đơn vị phải được bảo vệ bằng thiết bị tường lửa và phải đáp ứng các yêu cầu sau:

a) Phân chia hệ thống mạng nội bộ thành các vùng mạng theo phạm vi truy cập và kiểm soát truy cập giữa các vùng bằng thiết bị tường lửa, phải phân chia tối thiểu thành các vùng mạng sau: Vùng mạng ngoài (Public Zone); vùng DMZ; vùng làm việc (Working Zone) và vùng mạng riêng cho khách (áp dụng đối với các cơ quan, đơn vị cho phép khách đến làm việc được truy cập hệ thống mạng của đơn vị để sử dụng Internet).

b) Vô hiệu hoá tất cả các dịch vụ không sử dụng tại từng phân vùng mạng.

c) Cài đặt các bản cập nhật, vá lỗi đúng hạn cho các thiết bị tường lửa để khắc phục các điểm yếu nghiêm trọng của thiết bị; có cơ chế dự phòng phù hợp để đảm bảo hoạt động liên tục của các thiết bị tường lửa.

3. Đối với việc truy cập từ xa vào hệ thống mạng nội bộ:

a) Thủ trưởng cơ quan, đơn vị quyết định việc cho phép hoặc không cho phép thiết lập các kết nối từ xa vào hệ thống thông tin của cơ quan, đơn vị.

b) Cán bộ chuyên trách CNTT phải tham mưu lãnh đạo triển khai giải pháp áp dụng các tiêu chuẩn kỹ thuật để đảm bảo các kết nối từ xa vào hệ thống thông tin của cơ quan, đơn vị được giám sát chặt chẽ, cùng với các biện pháp đảm bảo an toàn thông tin; đảm bảo việc quản lý, giám sát và sử dụng các kết nối từ xa vào hệ thống thông tin của cơ quan, đơn vị tuân thủ các quy định về đảm bảo an toàn thông tin như các kết nối trực tiếp trong hệ thống mạng nội bộ của cơ quan, đơn vị.

c) Người dùng được cấp tài khoản để thực hiện kết nối từ xa vào hệ thống thông tin của cơ quan phải tuân thủ các quy định tại Điều 12 của Quy định này.

4. Không được kết nối điện thoại thông minh, máy tính bảng với hệ thống nội bộ khi chưa có sự cho phép của lãnh đạo cơ quan, đơn vị.

Điều 8. Đảm bảo an toàn thông tin khi kết nối và sử dụng mạng Internet

1. Khi kết nối hệ thống thông tin của cơ quan, đơn vị với mạng Internet để sử dụng các dịch vụ ứng dụng CNTT cung cấp qua mạng Internet, cung cấp thông tin và dịch vụ công trực tuyến cho tổ chức, cá nhân theo quy định của pháp luật, cơ quan, đơn vị phải trang bị thiết bị kiểm soát truy cập Internet; kiểm soát, hạn chế hoặc không cho phép người dùng kết nối Internet để sử dụng các dịch vụ làm tiêu tốn nhiều thời gian, băng thông phục vụ cho mục đích cá nhân trong giờ làm việc hành chính tại cơ quan, đơn vị (như: các dạng tải dữ liệu dung lượng lớn, kết nối mạng và chuyển dữ liệu trực tiếp với máy tính bên ngoài hệ thống thông tin, trao đổi trực tuyến có sử dụng giao tiếp âm thanh và hình ảnh, xem phim, chơi trò chơi trực tuyến,…).

2. Người dùng không được phép truy cập các trang thông tin có nghi ngờ chứa mã độc, không rõ nguồn gốc hoặc có nội dung không phù hợp (phản động hoặc trái thuần phong mỹ tục). Ngoại trừ những người có chức năng, thẩm quyền quản lý nhà nước lĩnh vực Internet có quyền truy cập để phục vụ cho công tác điều tra, xử lý.

3. Đối với máy chủ và thiết bị CNTT khác, chỉ thiết lập kết nối Internet cho các hệ thống cần phải có giao tiếp với Internet (các máy chủ, thiết bị cung cấp giao diện ra Internet của trang thông tin điện tử, dịch vụ công trực tuyến, thư điện tử,...).

4. Nghiêm cấm dùng máy tính kết nối vào hệ thống mạng để soạn thảo, in ấn, sao chép, lưu trữ tài liệu có nội dung liên quan đến bí mật Nhà nước.

Điều 9. Đảm bảo an toàn trong thu hồi, thanh lý, sửa chữa thiết bị

1. Các thiết bị (máy chủ, máy tính xách tay, phương tiện lưu trữ, máy tính để bàn, smartphone,…) khi không còn sử dụng cho công việc của cơ quan, đơn vị thì tiến hành thu hồi, thanh lý và đơn vị đang sử dụng, quản lý phải tiến hành xóa dữ liệu, ghi đè hoặc phá hủy vật lý, đảm bảo dữ liệu được xoá không thể khôi phục lại được.

2. Đối với các phương tiện lưu trữ có chứa dữ liệu quan trọng, phương án xử lý và ghi đè dữ liệu phải được bộ phận chuyên trách CNTT xem xét và có ý kiến phê duyệt của lãnh đạo cơ quan, đơn vị.

3. Trường hợp bắt buộc phải sửa chữa, bảo hành các thiết bị (máy chủ, máy tính để bàn, máy tính xách tay, ổ cứng, thiết bị lưu trữ di động,...) phải có ý kiến của bộ phận chuyên trách CNTT và được lãnh đạo phê duyệt.

4. Trường hợp thay đổi mục đích hoặc bàn giao thiết bị mạng, đơn vị quản trị loại bỏ hoàn toàn các cấu hình hiện tại trên thiết bị, khôi phục về trạng thái mặc định của nhà sản xuất trước khi thay đổi mục đích sử dụng hoặc bàn giao.

5. Trường hợp bàn giao các thiết bị (máy chủ, máy tính để bàn, máy tính xách tay, các thiết bị lưu trữ,...) cho bên thứ ba sửa chữa phải có biện pháp đảm bảo dữ liệu bên trong thiết bị được an toàn, không bị lộ, lọt thông tin, dữ liệu.

Điều 10. Giám sát an toàn hệ thống thông tin

1. Giám sát an toàn hệ thống thông tin là hoạt động giám sát nhằm phát hiện hành vi xâm phạm an toàn thông tin hoặc có khả năng gây ra sự cố mất an toàn thông tin đối với hệ thống thông tin.

2. Hoạt động giám sát an toàn hệ thống thông tin bao gồm:

a) Giám sát luồng thông tin được gửi, nhận qua mạng;

b) Giám sát hoạt động tại máy tính, thiết bị xử lý thông tin có kết nối mạng.

3. Cơ quan, đơn vị quản lý hệ thống thông tin quan trọng có trách nhiệm thực hiện giám sát an toàn hệ thống thông tin và lưu trữ thông tin giám sát theo quy định.

4. Doanh nghiệp viễn thông, doanh nghiệp cung cấp dịch vụ CNTT có trách nhiệm thực thi đầy đủ yêu cầu của cơ quan nhà nước khi được yêu cầu phối hợp giám sát an toàn hệ thống thông tin.

Mục 2
ĐỐI VỚI PHẦN MỀM ỨNG DỤNG

Điều 11. Đảm bảo an toàn phần mềm ứng dụng

1. Yêu cầu về đảm bảo an toàn thông tin phải được đưa vào tất cả các công đoạn liên quan đến công tác triển khai ứng dụng CNTT từ khâu thiết kế, xây dựng, triển khai và vận hành, sử dụng.

2. Ứng dụng do cơ quan, đơn vị phát triển hoặc thuê phát triển phải đáp ứng các yêu cầu sau:

a) Mã hoá thông tin bí mật hoặc nhạy cảm bằng thuật toán mã hoá an toàn.

b) Kiểm tra tính hợp lệ của dữ liệu đầu vào và đầu ra để đảm bảo dữ liệu chính xác và phù hợp.

c) Thực hiện các quy trình kiểm soát việc cài đặt phần mềm trên các máy chủ, máy tính của người dùng, thiết bị mạng đang hoạt động thuộc hệ thống mạng nội bộ.

d) Hạn chế truy cập tới mã nguồn chương trình và phải đặt mã nguồn trong môi trường an toàn do bộ phận chuyên trách CNTT quản lý.

đ) Thực hiện kiểm tra phát hiện và khắc phục lỗ hổng bảo mật của ứng dụng trước khi đưa vào sử dụng và kiểm tra định kỳ tối thiểu 6 tháng/01 lần trong quá trình sử dụng.

3. Đối với ứng dụng mua ở dạng đóng gói:

a) Theo dõi nắm bắt thông tin về các lỗ hổng bảo mật mới và cập nhật thường xuyên bản vá lỗi về bảo mật cho ứng dụng;

b) Trường hợp lỗ hổng đã được phát hiện mà chưa có bản vá lỗi của đơn vị sản xuất phần mềm, phải thực hiện đánh giá rủi ro và có biện pháp phòng tránh phù hợp.

Điều 12. Đảm bảo an toàn cơ sở dữ liệu

1. Các nội dung quan trọng hoặc nhạy cảm khi lưu trữ trên thiết bị di động hoặc truyền nhận trên môi trường mạng phải được mã hóa, trong đó:

a) Áp dụng mã hoá kênh kết nối cho các hoạt động sau: Quản trị hệ thống; đăng nhập mạng, ứng dụng; gửi nhận dữ liệu tự động giữa các máy chủ; nhập và biên tập dữ liệu; tra cứu dữ liệu;

b) Áp dụng chữ ký số để xác thực và bảo mật dữ liệu, đặc biệt trong trường hợp cần đảm bảo chống từ chối nguồn gốc dữ liệu;

c) Văn bản điện tử có nội dung cần hạn chế tiếp cận nhưng không thuộc danh mục bí mật Nhà nước được sử dụng tính năng mã hoá (đặt mật khẩu) của các ứng dụng văn phòng (phần mềm soạn thảo, đọc văn bản, nén tập tin), nhưng phải sử dụng mật khẩu an toàn.

2. CBCC-VC, người lao động thực hiện soạn thảo, gửi, nhận dữ liệu có trách nhiệm xác định mức độ quan trọng của dữ liệu để thực hiện phương thức bảo vệ dữ liệu phù hợp hoặc yêu cầu bộ phận chuyên trách CNTT hướng dẫn, hỗ trợ phương thức bảo vệ trong trường hợp cần thiết.

3. Cơ quan, đơn vị, CBCC-VC, người lao động bắt buộc phải sử dụng hộp thư điện tử của tỉnh (@longan.gov.vn) hoặc của ngành dọc (.gov.vn) để trao đổi thông tin, gửi nhận tài liệu, văn bản phục vụ cho công việc. Tuyệt đối không được sử dụng các địa chỉ thư điện tử miễn phí khác (gmail, yahoo mail,...) để trao đổi thông tin, gửi nhận tài liệu phục vụ cho công việc.

Điều 13. Quản lý, sử dụng tài khoản và mật khẩu

1. Mật khẩu của tất cả các tài khoản (ở cả cấp độ quản trị hệ thống và cấp độ người sử dụng) phải tuân thủ đồng thời các yêu cầu sau:

a) Có chứa cả các ký tự chữ in và chữ thường.

b) Có chứa ký tự số, các ký tự dấu câu hoặc các ký tự đặc biệt (!, @, #, ...).

c) Có ít nhất 08 ký tự đối với tài khoản người dùng, ít nhất 15 ký tự đối với tài khoản quản trị hệ thống.

d) Không phải là một từ hoàn chỉnh trong các ngôn ngữ thông dụng (Tiếng Việt, Tiếng Anh, Tiếng Pháp,…).

đ) Không phải là một dãy ký tự lặp lại có quy luật;

e) Không dựa vào thông tin cá nhân (ngày sinh, số điện thoại,…), tên người, tên địa danh, tên cơ quan hoặc các tên gọi khác.

2. Người dùng phải thay đổi mật khẩu ngay lần đầu tiên đăng nhập vào hệ thống và thường xuyên thay đổi mật khẩu ít nhất 03 tháng/01 lần.

3. Tất cả các tài khoản quản trị hệ thống thông tin của cơ quan, đơn vị (bao gồm máy chủ, thiết bị mạng, ứng dụng và cơ sở dữ liệu trong hệ thống thông tin), thường xuyên thay đổi mật khẩu, ít nhất 02 tháng/01 lần.

4. Khi quên mật khẩu hoặc nghi ngờ mật khẩu tài khoản của mình bị người khác biết ngoài ý muốn, phải báo cáo sự việc với thủ trưởng cơ quan và cán bộ chuyên trách CNTT để có phương án xử lý kịp thời; không sử dụng mật khẩu đã bị đánh cắp hoặc nghi ngờ bị đánh cắp cho tài khoản cũ hoặc các tài khoản khác do cơ quan cấp.

5. Các quyết định, thông báo về việc người dùng điều chuyển công tác, thôi việc hoặc nghỉ việc phải được đồng thời chuyển đến cán bộ chuyên trách CNTT, đơn vị chủ trì quản lý hệ thống thông tin để thực hiện điều chỉnh, thu hồi, hủy bỏ các quyền sử dụng của người dùng đó.

Mục 3
KỸ THUẬT, BIỆN PHÁP ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 14. Các biện pháp kỹ thuật đảm bảo an toàn thông tin cơ sở hạ tầng

1. Tổ chức quản lý các tài khoản của hệ thống thông tin, bao gồm: Tạo mới, kích hoạt, sửa đổi, vô hiệu và loại bỏ các tài khoản, đồng thời định kỳ tổ chức kiểm tra các tài khoản của hệ thống thông tin ít nhất 02 lần/01 năm và triển khai hệ thống quản lý người dùng để hỗ trợ việc quản lý các tài khoản của hệ thống thông tin.

2. Hệ thống thông tin phải giới hạn số lần đăng nhập sai liên tiếp (không quá 05 lần). 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.

3. Hệ thống thông tin phải ghi nhận được các sự kiện về quá trình đăng nhập hệ thống, các thao tác cấu hình hệ thống, quá trình truy xuất hệ thống, đồng thời ghi nhận đầy đủ các thông tin liên quan vào các bản ghi nhật ký hệ thống nhằm xác định những sự kiện nào đã xảy ra, nguồn gốc và kết quả của sự kiện đó; có cơ chế bảo vệ và lưu giữ bản ghi nhật ký hệ thống trong một khoảng thời gian nhất định.

4. Hệ thống thông tin tại các cơ quan, đơn vị cần có cơ chế ngăn chặn hoặc hạn chế các sự cố do tấn công từ chối dịch vụ (DoS, DDoS) gây ra. Sử dụng các thiết bị chuyên dụng để lọc gói tin nhằm bảo vệ các thiết bị bên trong, tránh bị ảnh hưởng trực tiếp bởi tấn công từ chối dịch vụ. Đối với hệ thống thông tin cho phép truy nhập công cộng có thể thực hiện bảo vệ bằng cách tăng dung lượng, băng thông hoặc thiết lập hệ thống dự phòng.

5. Xây dựng cơ chế kiểm tra, cho phép tương ứng với mỗi phương pháp truy cập từ xa và cơ chế tự động giám sát, điều khiển các truy cập từ xa; phải thiết lập phương pháp hạn chế truy cập mạng không dây, giám sát và điều khiển truy cập mạng không dây, tổ chức sử dụng chứng thực và mã hóa để bảo vệ truy cập mạng không dây tới hệ thống thông tin.

6. Lựa chọn, triển khai các phần mềm chống virus, thư rác có hiệu quả trên các máy chủ, máy trạm, các thiết bị, phương tiện kỹ thuật trong mạng,...;

đồng thời, thường xuyên cập nhật bản vá lỗi, phiên bản mới cho các phần mềm chống virus, nhằm kịp thời phát hiện, loại trừ mã độc máy tính (virus, trojan, worms,...).

7. Kiểm tra, giám sát chức năng chia sẻ thông tin trong mạng nội bộ. Tổ chức cấp phát tài nguyên trên máy chủ theo danh mục, thư mục cho từng phòng/ban, đơn vị. Khi thực hiện việc chia sẻ tài nguyên trên máy chủ hoặc trên máy đang sử dụng phải đặt mật khẩu theo quy định tại Điều 13 của Quy định này để bảo vệ thông tin.

8. Hệ thống thông tin phải có cơ chế, giải pháp sao lưu dự phòng dữ liệu ở mức người dùng, mức hệ thống và được lưu trữ tại nơi an toàn nhằm tránh bị ảnh hưởng khi xảy ra sự cố hỏa hoạn, thiên tai, lũ lụt. Đồng thời, thường xuyên kiểm tra dữ liệu dự phòng để đảm bảo tính sẵn sàng phục hồi và toàn vẹn thông tin.

Điều 15. Các biện pháp kỹ thuật đảm bảo an toàn thông tin phần mềm ứng dụng

1. Quản lý toàn bộ các phiên bản mã nguồn của phần mềm ứng dụng. Các phần mềm ứng dụng khi triển khai ra môi trường Internet phải tổ chức mô hình hợp lý, tránh khả năng tấn công chiếm quyền quản trị ứng dụng; cài đặt các hệ thống phòng vệ như tường lửa (firewall), thiết bị phát hiện/phòng chống xâm nhập (IDS/IPS) ở mức phần mềm ứng dụng.

2. Các phần mềm ứng dụng khi đưa vào sử dụng hoặc khi bổ sung các chức năng mới cần tiến hành đánh giá, kiểm định mức độ an toàn thông tin trước khi đưa vào vận hành chính thức nhằm tránh các lỗi mang tính bảo mật.

3. Thiết lập và cấu hình cơ sở dữ liệu bảo đảm an toàn:

a) Luôn cập nhật bản vá lỗi mới nhất cho hệ thống quản trị cơ sở dữ liệu; sử dụng công cụ để đánh giá, tìm kiếm lỗ hổng trên máy chủ cơ sở dữ liệu.

b) Gỡ bỏ các cơ sở dữ liệu không sử dụng.

c) Có các cơ chế sao lưu dữ liệu, tài liệu trong quá trình thay đổi cấu trúc bằng cách xây dựng nhật ký cơ sở dữ liệu với các nội dung như: Nội dung thay đổi, lý do thay đổi, thời gian, vị trí thay đổi.

4. Xây dựng phương án sao lưu, phục hồi các phần mềm ứng dụng, trong đó chú ý việc sao lưu toàn bộ nội dung liên quan của phần mềm ứng dụng, bao gồm: Mã nguồn, cơ sở dữ liệu, dữ liệu phi cấu trúc, đảm bảo khi có sự cố xảy ra có thể kịp thời khắc phục, phục hồi đầy đủ, trả lại trạng thái hoạt động bình thường của phần mềm ứng dụng.

Điều 16. Điều phối, ứng cứu sự cố mạng

1. Ứng cứu sự cố mạng là hoạt động nhằm xử lý, khắc phục sự cố gây mất an toàn thông tin trên mạng. Ứng cứu sự cố mạng trên địa bàn tỉnh do Bộ phận điều phối các hoạt động ứng cứu sự cố mạng Internet trong các cơ quan nhà nước trên địa bàn tỉnh (gọi tắt là "Bộ phận điều phối") thực hiện.

2. Ứng cứu sự cố mạng được thực hiện theo các nguyên tắc sau đây:

a) Nhanh chóng, chính xác, kịp thời, hiệu quả; tuân thủ quy định của pháp luật về điều phối ứng cứu sự cố mạng.

b) Thông tin được trao đổi, cung cấp trong quá trình điều phối, xử lý sự cố phải được đảm bảo bí mật theo yêu cầu của tổ chức, cá nhân gặp sự cố, trừ khi sự cố xảy ra có liên quan tới nhiều đối tượng người dùng khác hoặc có tính chất nghiêm trọng mà Cơ quan điều phối cấp trên có yêu cầu cung cấp để phục vụ cho công tác ứng cứu.

c) Việc trao đổi thông tin trong hoạt động điều phối phải được thực hiện bằng một hoặc nhiều hình thức như: công văn, thư điện tử, điện thoại, fax. Thành viên tiếp nhận thông tin phải chủ động xác thực đối tượng gửi nhằm bảo đảm thông điệp nhận được là tin cậy.

d) Thành viên Bộ phận điều phối có quyền được chia sẻ thông tin, kinh nghiệm, tham gia các hoạt động diễn tập ứng cứu sự cố, tham gia các khóa đào tạo, bồi dưỡng về hoạt động ứng cứu sự cố.

3. Công tác điều phối ứng cứu sự cố thực hiện theo Quy chế và quy trình cụ thể từ khâu: Thông báo sự cố; tiếp nhận và xử lý thông báo sự cố đến khâu điều phối ứng cứu sự cố.

Điều 17. Phát hiện, ngăn chặn và xử lý phần mềm độc hại

1. Cơ quan, đơn vị quản lý hệ thống thông tin quan trọng triển khai giải pháp, xây dựng hệ thống kỹ thuật nghiệp vụ nhằm phát hiện, ngăn chặn và xử lý kịp thời việc phát tán phần mềm độc hại.

2. Tổ chức cung cấp dịch vụ thư điện tử, truyền đưa, lưu trữ thông tin trực tuyến phải có hệ thống phát hiện và lọc phần mềm độc hại trong thông tin được gửi, nhận hoặc lưu trữ trên hệ thống thông tin của mình và có trách nhiệm báo cáo cho cơ quan có thẩm quyền theo quy định của pháp luật.

3. Doanh nghiệp cung cấp dịch vụ Internet có trách nhiệm ngăn chặn việc phát tán phần mềm độc hại theo yêu cầu của cơ quan chức năng.

Điều 18. Đào tạo, bồi dưỡng kiến thức an toàn thông tin

1. Cơ quan, tổ chức xây dựng kế hoạch tuyển dụng, đào tạo, phân công, cán bộ chuyên trách về CNTT và an toàn thông tin để đảm bảo quản lý, khai thác có hiệu quả và bảo đảm an toàn cho hệ thống thông tin thuộc phạm vi quản lý của cơ quan, tổ chức mình; chịu trách nhiệm tổ chức hoặc cử cán bộ chuyên trách, bán chuyên trách CNTT tham gia các khóa đào tạo, bồi dưỡng, cập nhật kiến thức cơ bản về an toàn thông tin mạng do tỉnh hoặc cấp trên tổ chức.

2. Cán bộ chuyên trách về CNTT tại các cơ quan, đơn vị có hệ thống thông tin phải thường xuyên được đào tạo nâng cao, chuyên sâu về công tác đảm bảo an toàn thông tin, kịp thời cập nhật kiến thức mới về an toàn thông tin; được bố trí, tạo điều kiện làm việc phù hợp, được hưởng lương và phụ cấp ưu đãi theo quy định.

Điều 19. Xây dựng quy chế nội bộ và áp dụng quy trình đảm bảo an toàn thông tin

1. Các cơ quan, đơn vị phải xây dựng quy chế nội bộ và áp dụng quy trình đảm bảo an toàn, an ninh cho hệ thống thông tin nhằm giảm thiểu các nguy cơ

gây ra sự cố mất an toàn thông tin, tạo điều kiện cho việc khắc phục và truy vết trong trường hợp có sự cố xảy ra.

2. Các cơ quan, đơn vị tham khảo các bước cơ bản để xây dựng khung quy trình đảm bảo an toàn thông tin cho hệ thống thông tin tại tiêu chuẩn Quốc tế ISO/IEC 27001.

Chương III
PHÂN CÔNG TRÁCH NHIỆM THỰC HIỆN

Điều 20. Trách nhiệm của các cơ quan, đơn vị

1. Các cơ quan, đơn vị trên địa bàn tỉnh phải ban hành quy định hoặc quy chế về đảm bảo an toàn thông tin trong hoạt động của cơ quan, đơn vị mình.

2. Thủ trưởng các cơ quan, đơn vị có trách nhiệm tuyên truyền, nâng cao nhận thức cho CBCC-VC về các nguy cơ mất an toàn hệ thống thông tin; triển khai thực hiện nghiêm túc Quy định này và các quy định khác có liên quan; chịu trách nhiệm trước UBND tỉnh về công tác đảm bảo an toàn thông tin cho các hệ thống thông tin do cơ quan, đơn vị mình quản lý, vận hành. Thiết lập kênh thông tin trực tuyến để tiếp nhận phản ánh các vấn đề liên quan đến an toàn thông tin.

3. 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 kỹ thuật chuyên trách CNTT trong cơ quan, đơn vị. Đồng thời, thông báo bằng văn bản gửi về Sở Thông tin và Truyền thông, cơ quan cấp trên quản lý trực tiếp nắm biết. Trường hợp không khắc phục được thì phối hợp với Sở Thông tin và Truyền thông hoặc cơ quan quản lý cấp trên để được hướng dẫn, hỗ trợ.

4. Phối hợp chặt chẽ với cơ quan Công an trong công tác phòng ngừa, đấu tranh, ngăn chặn các hành vi 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.

5. Phối hợp với đoàn kiểm tra 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.

6. Báo cáo UBND tỉnh về tình hình và kết quả thực hiện công tác đảm bảo an toàn thông tin tại cơ quan, đơn vị (thông qua Sở Thông tin và Truyền thông) định kỳ hàng năm (trước ngày 20 tháng 9).

Điều 21. Trách nhiệm Sở Thông tin và Truyền thông

1. Tham mưu UBND tỉnh tổ chức thực hiện các văn bản quy phạm pháp luật, chiến lược, quy hoạch, tiêu chuẩn, quy chuẩn kỹ thuật về an toàn thông tin trên địa bàn tỉnh; chịu trách nhiệm trước UBND tỉnh về việc đảm bảo an toàn thông tin cho các hệ thống thông tin trực tiếp quản lý vận hành.

2. Hàng năm, xây dựng và trình UBND tỉnh phê duyệt kế hoạch, dự toán nguồn kinh phí triển khai thực hiện công tác đảm bảo an toàn thông tin trong hoạt động ứng dụng CNTT của các cơ quan, đơn vị trên địa bàn tỉnh; đánh giá an toàn thông tin cho các hệ thống thông tin trọng điểm của tỉnh.

3. Phối hợp với các cơ quan, đơn vị liên quan thực hiện thanh tra, kiểm tra khi phát hiện có các dấu hiệu, hành vi vi phạm pháp luật về an toàn thông tin. Sở

Thông tin và Truyền thông có trách nhiệm quản lý công tác giám sát an toàn hệ thống thông tin của cơ quan, đơn vị trên địa bàn tỉnh.

4. Xây dựng và triển khai thực hiện các chương trình, kế hoạch đào tạo, bồi dưỡng; hội nghị tuyên truyền, phổ biến pháp luật về an toàn thông tin cho các cơ quan, đơn vị, tổ chức, cá nhân có liên quan trên địa bàn tỉnh.

5. Tham mưu UBND tỉnh quyết định thành lập, ban hành Quy chế hoạt động của Bộ phận điều phối và triển khai thực hiện quy trình điều phối xử lý, ứng cứu sự cố mất an toàn thông tin của Bộ phận điều phối trong cơ quan nhà nước của tỉnh. Tùy theo mức độ sự cố, phối hợp Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) và các đơn vị có liên quan để hướng dẫn xử lý, ứng cứu các sự cố mất an toàn thông tin tại các hệ thống thông tin trên địa bàn tỉnh.

6. Hướng dẫn chuyên môn nghiệp vụ về đảm bảo an toàn thông tin cho hệ thống thông tin của các cơ quan, đơn vị; thường xuyên thông báo đến các cơ quan, đơn vị về nguy cơ gây mất an toàn thông tin do virus, phần mềm gián điệp,... gây ra và hướng dẫn biện pháp phòng ngừa, ngăn chặn kịp thời.

7. Định kỳ và đột xuất báo cáo UBND tỉnh và Bộ thông tin và Truyền thông về tình hình thực hiện công tác đảm bảo an toàn thông tin trong các cơ quan, đơn vị trên địa bàn tỉnh.

Điều 22. Trách nhiệm Công an tỉnh

1. Phối hợp với Sở Thông tin và Truyền thông kiểm tra công tác đảm bảo an toàn an ninh thông tin trong các cơ quan, đơn vị trên địa bàn tỉnh; triển khai công tác bảo đảm an ninh thông tin, phòng, chống tội phạm và các hành vi vi phạm pháp luật khác trong công tác đảm bảo an toàn thông tin; thanh tra, kiểm tra và xử lý vi phạm đối với tổ chức, cá nhân vi phạm quy định về bảo đảm an ninh thông tin trong hoạt động của các cơ quan, đơn vị.

2. Thường xuyên thông báo cho các cơ quan, đơn vị về âm mưu, phương thức, thủ đoạn hoạt động của các thế lực thù địch và tội phạm trên lĩnh vực CNTT nhằm nâng cao ý thức cảnh giác và có biện pháp phòng ngừa, đấu tranh, ngăn chặn kịp thời hoạt động của tội phạm và các thế lực thù địch.

3. Điều tra và xử lý các trường hợp vi phạm về an toàn, an ninh thông tin theo thẩm quyền quy định của pháp luật hiện hành.

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

5. Cơ quan chuyên trách bảo vệ an ninh quốc gia thuộc Công an tỉnh khi phát hiện các thông tin, tài liệu, dữ liệu, đồ vật liên quan đến hoạt động xâm phạm an ninh quốc gia theo quy định phải thực hiện các quy định sau đây:

a) Yêu cầu tổ chức, cá nhân cung cấp các thông tin, dữ liệu, số liệu, tài liệu, đồ vật liên quan.

b) Thực hiện theo thẩm quyền các biện pháp thu giữ, sao chép thông tin, dữ liệu, số liệu, tài liệu, đồ vật, một phần hoặc toàn bộ hệ thống thiết bị liên quan.

c) Ngăn cản việc truy nhập hệ thống thiết bị, mạng lưới và sử dụng dịch vụ.

d) Thực hiện các nhiệm vụ, quyền hạn khác theo quy định của pháp luật.

Điều 23. Trách nhiệm Sở Tài chính

Chủ trì phối hợp với Sở Thông tin và Truyền thông hướng dẫn các cơ quan, đơn vị lập dự toán, quản lý, sử dụng và quyết toán kinh phí ngân sách nhà nước hàng năm trong dự toán được giao để thực hiện nhiệm vụ chuyên môn về bảo đảm an toàn, an ninh thông tin.

Điều 24. Trách nhiệm Sở Kế hoạch và Đầu tư

Ưu tiên bố trí nguồn kinh phí đầu tư để thực hiện các nhiệm vụ, dự án liên quan đến công tác bảo đảm an toàn, an ninh thông tin.

Điều 25. Trách nhiệm của cán bộ, công chức, viên chức, người lao động

1. Cán bộ chuyên trách CNTT có trách nhiệm tham mưu thủ trưởng cơ quan, đơn vị:

a) Triển khai thực hiện các biện pháp quản lý vận hành kỹ thuật cho hệ thống thông tin của cơ quan, đơn vị mình;

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

c) Tham gia các chương trình đào tạo, hội nghị về an toàn thông tin do tỉnh hoặc các đơn vị chuyên môn tổ chức;

d) Xác định các chương trình, phần mềm cần thiết để cài đặt trên các máy tính cá nhân trong cơ quan phục vụ công việc của từng nhóm người dùng (văn thư, cán bộ chuyên môn, kế toán,...) và thực hiện cài đặt các phần mềm này theo đúng quy định.

2. Cán bộ, công chức, viên chức, người lao động có trách nhiệm:

a) Chấp hành nghiêm các quy định của tỉnh, cơ quan, đơn vị về công tác đảm bảo an toàn thông tin và các quy định pháp luật khác có liên quan; nâng cao ý thức cảnh giác và có trách nhiệm trong công tác đảm bảo an toàn thông tin tại cơ quan, đơn vị.

b) Khi phát hiện sự cố mất an toàn thông tin phải báo cáo ngay với lãnh đạo trực tiếp và bộ phận hoặc cán bộ chuyên trách CNTT để kịp thời ngăn chặn, xử lý.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 26. Khen thưởng, xử lý vi phạm

1. Hàng năm, Sở Thông tin và Truyền thông dựa trên hoạt động kiểm tra việc triển khai thực hiện công tác đảm bảo an toàn thông tin của các cơ quan, đơn vị trên địa bàn tỉnh, tham mưu, đề xuất UBND tỉnh xem xét khen thưởng các cơ quan, đơn vị, tổ chức, cá nhân thực hiện tốt công tác đảm bảo an toàn thông tin cho hệ thống thông tin của các cơ quan, đơn vị và của tỉnh.

2. Tổ chức, cá nhân có hành vi vi phạm các quy định về an toàn cơ sở hạ tầng và an ninh thông tin trong hoạt động của cơ quan nhà nước thì tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật theo trách nhiệm, xử phạt vi phạm

hành chính hoặc truy cứu trách nhiệm hình sự. Nếu gây thiệt hại thì phải bồi thường theo quy định hiện hành của pháp luật.

Điều 27. Điều khoản thi hành

1. Giao Sở Thông tin và Truyền thông chủ trì, phối hợp với các cơ quan, đơn vị có liên quan hướng dẫn, theo dõi, đôn đốc, kiểm tra việc triển khai thực hiện Quy định này.

2. Trong quá trình thực hiện, nếu có vướng mắc, đề nghị cơ quan, tổ chức, cá nhân có liên quan phản ánh về Sở Thông tin và Truyền thông để tổng hợp trình UBND tỉnh xem xét, giải quyết./.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Đỗ Hữu Lâm