ỦY BAN NHÂN DÂN TỈNH BÀ RỊA - VŨNG TÀU **SỞ Y TẾ**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 672 /QĐ-SYT	*Bà Rịa-Vũng Tàu, ngày 31 tháng 8 năm 2018.*

QUYẾT ĐỊNH
Về việc ban hành Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của ngành Y tế

GIÁM ĐỐC SỞ Y TẾ TỈNH BÀ RỊA-VŨNG TÀU

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 an toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10 tháng 4 năm 2997 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước;

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

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

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 liên tịch số 71/2014/TTLT-BTC-BNV ngày 30/5/2014 của liên Bộ Tài chính và Bộ Nội vụ Quy định hướng dẫn thực hiện Nghị định số 130/2005/NĐ-CP ngày 17/10/2005 của Chính phủ "Quy định chế độ tự chủ, tự chịu trách nhiệm về sử dụng biên chế và kinh phí quản lý hành chính đối với cơ quan Nhà nước";

Theo đề nghị của Trưởng phòng Kế hoạch Tài chính,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước thuộc tỉnh Bà Rịa - Vũng Tàu.

Điều 2. Hiệu lực thi hành

1. Quyết định này có hiệu lực thi hành kể từ ngày ký.

2. Quyết định số 327/QĐ-UBND ngày 31 tháng 01 năm 2013 của Chủ tịch Ủy ban nhân dân tỉnh Bà Rịa - Vũng Tàu ban hành Hướng dẫn đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước tỉnh Bà Rịa - Vũng Tàu hết hiệu lực kể từ ngày Quyết định này có hiệu lực thi hành.

Điều 3. Chánh văn phòng, Trưởng các phòng chức năng, công chức, viên chức, người lao động thuộc ngành Y tế chịu trách nhiệm thi hành quyết định này./.

Nơi nhận:
- Như điều 3;
- UBND tỉnh ;
- Lưu: VT, KHTC.

GIÁM ĐỐC

Phạm Minh An

Digitally signed by
Phạm Minh An
Sở Y tế
Tỉnh Bà Rịa - Vũng Tàu
Bà Rịa - Vũng Tàu, VN

ỦY BAN NHÂN DÂN
TỈNH BÀ RỊA - VŨNG TÀU
SỞ Y TẾ

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

QUY CHẾ

Đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước thuộc tỉnh Bà Rịa - Vũng Tàu

(*Ban hành kèm theo Quyết định số: 672 /QĐ-SYT ngày* 31 *tháng* 8 *năm 2018 của Sở Y tế tỉnh Bà Rịa-Vũng Tàu*)

Chương I
NHỮNG QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng

1. Quy chế này quy định về công tác đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan, đơn ngành Y tế tỉnh Bà Rịa - Vũng Tàu.

2. Quy chế này được áp dụng đối với các cán bộ, công chức, viên chức và người lao động trong các cơ quan, đơn vị nhà nước và đơn vị sự nghiệp trên địa bàn tỉnh Bà Rịa - Vũng Tàu.

Điều 2. Nguyên tắc đảm bảo an toàn thông tin

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

Điều 3. Giải thích từ ngữ

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

2. *Mạng* là môi trường trong đó thông tin được cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông qua mạng viễn thông và mạng máy tính.

3. *Hệ thống thông tin* là tập hợp 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 trên mạng.

4. *Chủ quản hệ thống thông tin* là cơ quan, đơn vị, tổ chức, cá nhân có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin.

5. *Tính tin cậy* là bảo đảm thông tin chỉ có thể được truy cập bởi những người được quyền truy cập.

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

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

8. *Xâm phạm an toàn thông tin mạng* là hành vi truy nhập, sử dụng, tiết lộ, làm gián đoạn, sửa đổi, phá hoại trái phép thông tin, hệ thống thông tin.

9. *Rủi ro an toàn thông tin mạng* là những nhân tố chủ quan hoặc khách quan có khả năng ảnh hưởng tới trạng thái an toàn thông tin mạng.

10. *Phần mềm độc hại* là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay toàn bộ hệ thống thông tin hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong hệ thống thông tin.

11. *Hệ thống lọc phần mềm độc hại* là tập hợp phần cứng, phần mềm được kết nối vào mạng để phát hiện, ngăn chặn, lọc và thống kê phần mềm độc hại.

12. *Sự cố an toàn thông tin mạng* là việc thông tin, hệ thống thông tin bị tấn công hoặc gây nguy hại, ảnh hưởng tới tính toàn vẹn, tính tin cậy hoặc tính sẵn sàng (sau đây gọi tắt là sự cố).

13. *Ứng cứu sự cố an toàn thông tin mạng* là hoạt động nhằm xử lý, khắc phục sự cố gây mất an toàn thông tin mạng gồm: theo dõi, thu thập, phân tích, phát hiện, cảnh báo, điều tra, xác minh sự cố, ngăn chặn sự cố, khôi phục dữ liệu và khôi phục hoạt động bình thường của hệ thống thông tin.

14. *Thiết bị di động* là các thiết bị di động cá nhân có kết nối vào mạng nội bộ của cơ quan, đơn vị như máy tính xách tay, máy tính bảng, điện thoại di động, các thiết bị di động khác.

15. *Người dùng* là cán bộ, công chức, viên chức và người lao động của các cơ quan, đơn vị sử dụng máy tính, các thiết bị điện tử để xử lý công việc. Các tổ chức, cá nhân có liên quan tham gia sử dụng các dịch vụ của Trung tâm Dữ liệu tỉnh.

16. *Các cơ quan, đơn vị* là cụm từ viết tắt chỉ các sở, các đơn vị sự nghiệp trực thuộc Sở Y tế.

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

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

Chương II

QUY ĐỊNH VỀ ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 4. Những quy định về đảm bảo an toàn thông tin

1. Các cơ quan, đơn vị phải thường xuyên tổ chức quán triệt các quy định về an toàn thông tin, phổ biến những kiến thức cơ bản về an ninh thông tin cho cán bộ, công chức, viên chức và người lao động, nhằm nâng cao nhận thức về trách nhiệm đảm bảo an toàn thông tin trước khi tham gia sử dụng hệ thống thông tin.

2. Các cơ quan, đơn vị bố trí người làm công tác chuyên trách về công nghệ thông tin phải có chuyên ngành phù hợp và được đào tạo, bồi dưỡng chuyên môn đối với lĩnh vực an toàn, an ninh thông tin.

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

4. Các cơ quan, đơn vị phải xây dựng, ban hành quy chế nội bộ đảm bảo an toàn thông tin và căn cứ các nội dung của tiêu chuẩn TCVN 7562:2005 và TCVN ISO/IEC 27001:2009. Quy chế phải đảm bảo các nội dung sau:

a) Mục tiêu đảm bảo an toàn thông tin cho các hệ thống thông tin của tỉnh;

b) Quy định cụ thể quyền và trách nhiệm của từng đối tượng: lãnh đạo đơn vị, lãnh đạo phòng, cán bộ chuyên trách về công nghệ thông tin, người sử dụng;

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

d) Quy định về an toàn thông tin trên (trong) môi trường mạng nội bộ;

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

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

g) Khen thưởng, kỷ luật;

h) Tổ chức thực hiện.

5. Các cơ quan, đơn vị nâng cấp, xây dựng, triển khai hệ thống thông tin cần triển khai đánh giá các nguy cơ, sự cố an toàn thông tin và xây dựng phương án đối phó, ứng cứu đối với một số tình huống cụ thể theo hướng dẫn tại Phụ lục III của 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 *(sau đây xin gọi tắt là Thông tư số 20/2017/TT-BTTTT)* và tổng hợp báo cáo về Sở Y tế theo định kỳ hàng năm.

6. Trước khi thanh lý hoặc điều chuyển các máy tính, thiết bị lưu trữ, thiết bị công nghệ thông tin không còn nhu cầu sử dụng trong các cơ quan nhà nước, phải dùng các biện pháp kỹ thuật kiểm tra, sao lưu, xóa bỏ vĩnh viễn dữ liệu trong thiết bị lưu trữ, ổ cứng máy tính tránh lộ lọt thông tin; Tuân thủ các quy định, thủ tục quản lý việc các thiết bị công nghệ thông tin lưu trữ thông tin thuộc danh mục bí mật nhà nước tại Thông tư số 33/2015/TT-BCA ngày 20 tháng 7 năm 2015 của Bộ trưởng Bộ Công an hướng dẫn thực hiện một số điều của Nghị định số 33/2002/NĐ-CP ngày 28 tháng 3 năm 2002 của Chính phủ quy định chi tiết thi hành Pháp lệnh bảo vệ bí mật nhà nước và các quy định khác có liên quan.

Điều 5. Quản lý phòng máy chủ

1. Phòng máy chủ của các cơ quan, đơn vị là khu vực hạn chế tiếp cận và được lắp đặt hệ thống camera giám sát. Chỉ những người có trách nhiệm theo quy định của thủ trưởng cơ quan, đơn vị mới được phép vào phòng máy chủ.

2. Các thiết bị mạng quan trọng như hệ thống máy chủ, tường lửa *(firewall)*, thiết bị định tuyến *(router)* và các thiết bị mạng quan trọng khác phục vụ cho phòng máy chủ phải được đặt trong phòng máy chủ và có các biện pháp bảo vệ, ngăn chặn xâm nhập trái phép vào phòng máy chủ.

3. Phòng máy chủ phải đảm bảo an toàn phòng cháy chữa cháy, chống sét, điều hòa nhiệt độ, nguồn điện ổn định và có hệ thống lưu điện đủ công suất và duy trì thời gian hoạt động của các máy chủ tối thiểu 15 *(mười lăm)* phút khi có sự cố mất điện.

4. Những người có trách nhiệm theo quy định của Thủ trưởng cơ quan mới được phép vào phòng máy chủ. Quá trình vào, ra phòng máy chủ phải được ghi nhận đầy đủ vào nhật ký quản lý phòng máy chủ.

5. Bố trí cán bộ, công chức có năng lực chuyên môn về công nghệ thông tin để quản lý, vận hành phòng máy chủ và duy trì chế độ trực phù hợp để đảm bảo an toàn, an ninh thông tin.

Điều 6. Đảm bảo an toàn máy chủ, máy trạm và các thiết bị di động

1. Kiểm soát chặt chẽ việc cài đặt các phần mềm mới lên máy chủ, máy trạm và các thiết bị di động. Các phần mềm được cài đặt trên máy chủ, máy trạm và

các thiết bị di động *(bao gồm hệ điều hành, các phần mềm ứng dụng văn phòng, phần mềm phục vụ công việc, ứng dụng tiện ích khác)* phải được thường xuyên theo dõi, cập nhật bản vá lỗi bảo mật của nhà phát triển; và phải cài đặt các phần mềm phòng, chống mã độc, diệt virus và thường xuyên cập nhật phiên bản mới, đặt lịch quét virus theo định kỳ ít nhất hàng tuần.

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

3. Tất cả các tập tin, thư mục phải được quét mã độc trước khi sao chép, sử dụng.

4. Khi phát hiện ra bất kỳ dấu hiện nào liên quan đến việc bị nhiễm mã độc trên máy tính (*ví dụ: máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống mã độc, mất dữ liệu, các phần mềm và hệ thống mạng hoạt động không ổn định và các dấu hiệu bất thường khác*) người sử dụng phải tắt máy và báo trực tiếp cho bộ phận có trách nhiệm của cơ quan, đơn vị để xử lý.

5. Các đơn vị phải quy định cụ thể về quản lý, vận hành sử dụng máy chủ, quản lý chặt chẽ logfile để ghi nhận thông tin quá trình đăng nhập hệ thống, các thay đổi, cấu hình hệ thống, theo dõi các dịch vụ, sự kiện trong quá trình vận hành máy chủ. Các phần mềm cài đặt trên máy chủ phục vụ công tác chuyên môn, nghiệp vụ, điều hành phải có kế hoạch và được lãnh đạo cơ quan, đơn vị phê duyệt. Chỉ cài đặt trên máy chủ các phần mềm cần thiết, có bản quyền, không được cài đặt các phần mềm bẻ khóa, không rõ nguồn gốc vào máy chủ để phòng lây nhiễm mã độc; tắt các dịch vụ, các port *(cổng)* không sử dụng, chia sẻ tài nguyên trên máy chủ phải được phân quyền khoa học, rõ ràng.

Điều 7. Đảm bảo an toàn hệ thống mạng nội bộ, đăng nhập hệ thống thông tin và kết nối Internet

1. Hệ thống thông tin tại cơ quan, đơn vị phải được triển khai chức năng giám sát truy cập từ bên ngoài vào hệ thống, và từ hệ thống ra môi trường mạng bên ngoài *(ghi log)* để phục vụ cho công tác khắc phục sự cố, điều tra, phân tích và làm rõ các nguy cơ gây mất an toàn thông tin, chức năng giới hạn truy cập website không phù hợp quy định hiện hành và gây nguy hiểm cho hệ thống thông tin.

Các đơn vị phải quy định cụ thể trách nhiệm, quyền hạn người dùng khi truy cập, đăng nhập các hệ thống thông tin, đảm bảo mỗi người dùng khi sử dụng hệ thống thông tin phải được cấp và sử dụng tài khoản truy cập với định danh duy nhất gắn với người dùng đó. Trường hợp sử dụng tài khoản dùng chung cho một nhóm người hay một đơn vị, bộ phận phải có cơ chế xác định các cá nhân có trách nhiệm quản lý tài khoản. Người dùng chỉ được truy cập các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình và có trách nhiệm bảo mật tài khoản truy

cập được cấp.

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

3. Mỗi cán bộ, công chức, viên chức và người lao động chỉ được phép truy cập các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình, có trách nhiệm bảo mật tài khoản truy cập thông tin.

4. Các hệ thống thông tin cần giới hạn số lần đăng nhập sai liên tiếp vào hệ thống *(từ ba đến năm lần)*. Hệ thống tự động khóa tài khoản trong một khoảng thời gian nhất định trước khi tiếp tục cho đăng nhập nếu liên tục đăng nhập sai vượt quá số lần quy định.

5. Tất cả máy chủ, máy trạm phải được thiết lập mật mã truy cập và chế độ tự động bảo vệ màn hình sau 10 *(mười)* phút không sử dụng.

6. Hệ thống mạng nội bộ đơn vị phải được tổ chức theo mô hình Clients/Server và khi kết nối với mạng Internet phải thông qua thiết bị tường lửa kiểm soát *(tường lửa phải được cập nhật dữ liệu hàng năm và đucợ thực hiện sau khi được trang bị),* có phân chia hệ thống mạng nội bộ thành các vùng mạng theo phạm vi truy cập, vô hiệu hóa tất cả các dịch vụ không sử dụng tại từng vùng mạng, thực hiện nguyên tắc chỉ mở các dịch vụ cần thiết khi có yêu cầu.

7. Hệ thống mạng không dây *(wifi)* của các cơ quan, đơn vị phải được đặt mật khẩu *(password)* khi truy cập. Thiết lập phương pháp hạn chế người dùng truy cập mạng không dây, giám sát và điều khiển truy cập mạng không dây.

8. Mạng riêng ảo *(VPN),* các giải pháp truy cập từ xa vào hệ thống thông tin của các cơ quan, đơn vị phải được bảo mật, quản lý kiểm soát các kết nối chặt chẽ, nhất là truy cập có sử dụng chức năng quản trị, phải thiết lập mật mã độ an toàn cao, nhắc nhở khuyến cáo thường xuyên thay đổi mật mã, tăng cường sử dụng mạng riêng ảo, hạn chế truy cập từ xa vào mạng nội bộ từ các điểm truy cập Internet công cộng.

9. Tất cả các tài khoản truy cập vào hệ thống máy chủ, thiết bị mạng, máy tính, các ứng dụng phải được đặt mật khẩu đăng nhập, truy cập hệ thống thông tin có độ phức tạp cao (có độ dài tối thiểu tám ký tự, có ký tự thường, ký tự hoa, ký tự số hoặc ký tự đặc biệt như !, @, #, $, %) và phải được thay đổi ít nhất ba tháng/lần.

10. Các cơ quan, đơn vị cần rà soát tối thiểu ba tháng/lần các tài khoản đăng nhập, đảm bảo các tài khoản và quyền truy cập hệ thống được cấp phát đúng, đủ. Khi người dùng thay đổi vị trí công tác, chuyển công tác, thôi việc hoặc nghỉ hưu thì cơ quan , đơn vị phải kịp thời thu hồi tài khoản đã cấp hoặc thông báo cho Trung tâm công nghệ thông tin và truyền thông trực thuộc Sở Thông tin và

Truyền thông thu hồi tài khoản được cấp *(đối với các hệ thống quản lý tập trung tại Trung tâm Dữ liệu của tỉnh).*

11. Thực hiện các hướng dẫn tại công văn số 3024/BTTTT-VNCERT ngày 01 tháng 9 năm 2016 của Bộ Thông tin và Truyền thông về Hướng dẫn một số giải pháp tăng cường đảm bảo an toàn cho hệ thống thông tin.

Điều 8. Đảm bảo an toàn các phần mềm ứng dụng

1. Việc đảm bảo an toàn các phần mềm ứng dụng *(bao gồm: cơ sở dữ liệu)* phải được đưa vào tất cả các giai đoạn đầu tư *(hoặc thuê dịch vụ)* của phần mềm ứng dụng như thiết kế, xây dựng, vận hành, nâng cấp, hủy bỏ.

2. Đối với giai đoạn thiết kế, xây dựng, nâng cấp, hủy bỏ *(hoặc chuẩn bị thuê dịch vụ):* áp dụng các biện pháp quản lý và kỹ thuật đảm bảo các quy trình, kết quả xử lý của phần mềm phải trung thực *(kết quả xử lý không bị can thiệp trái phép),* kiểm soát lỗ hổng bảo mật trong quá trình thiết kế, xây dựng phần mềm, kiểm soát phân quyền người dùng đăng nhập và kiểm soát các rủi ro mất an toàn thông tin khác có thể phát sinh, thực hiện nghiêm túc việc kiểm thử phần mềm trước khi đưa vào khai thác sử dụng.

3. Đối với giai đoạn vận hành: Kiểm tra, giám sát việc tuân thủ các quy định về an toàn thông tin, đảm bảo cập nhật các lỗ hổng bảo mật, áp dụng cơ chế sao lưu dự phòng, đảm bảo an toàn truy cập, đăng nhập hệ thống.

Điều 9. Đảm bảo an toàn thông tin, dữ liệu

1. Thông tin, dữ liệu khi được lưu trữ, khai thác, trao đổi phải được đảm bảo tính toàn vẹn, tính tin cậy, tính sẵn sàng. Thông tin, dữ liệu quan trọng khi được lưu trữ, trao đổi phải áp dụng kỹ thuật mã hóa, thiết lập mật mã, ứng dụng chữ ký số và phải có cơ chế lưu trữ dự phòng.

2. Trong trao đổi thông tin, dữ liệu phục vụ công việc, các cơ quan, đơn vị, cán bộ, công chức, viên chức phải sử dụng hệ thống thông tin do cơ quan, đơn vị có thẩm quyền triển khai như: hệ thống thư điện tử tỉnh (@baria-vungtau.gov.vn) hoặc hệ thống thư điện tử của ngành, lĩnh vực; phần mềm quản lý văn bản và điều hành, hệ thống thông tin họp và giao tiếp trực tuyến *(chat nội bộ).* Hạn chế việc sử dụng các phương tiện trao đổi thông tin dữ liệu, hệ thống thư điện tử, lưu trữ điện tử công cộng, mạng xã hội trên Internet trong hoạt động của cơ quan, đơn vị.

3. Các đơn vị phải lập kế hoạch và thực hiện sao lưu dữ liệu dự phòng định kỳ ít nhất một lần trong tháng các dữ liệu quan trọng, bao gồm: thông tin cấu hình của hệ thống mạng, máy chủ, tập tin ghi nhật ký *(logfile),* cơ sở dữ liệu và các dữ liệu quan trọng được triển khai, lưu trữ *(bao gồm dữ liệu phát sinh trong quá trình vận hành các phần mềm ứng dụng như: các tập tin văn bản, hình ảnh,*

các tập tin dữ liệu khác). Sau khi sao lưu, lưu trữ bản sao lưu bằng thiết bị lưu trữ ngoài *(như: đĩa quang, ổ cứng ngoài, các thiết bị lưu trữ khác)* theo quy định lưu trữ hiện hành, bảo đảm tính sẵn sàng và toàn vẹn nhằm đáp ứng yêu cầu phục hồi dữ liệu, khắc phục hệ thống thông tin cho hoạt động bình thường kịp thời khi có sự cố xảy ra.

Điều 10. Quy trình phối hợp ứng cứu sự cố về an toàn thông tin

Cơ quan, đơn vị khi phát hiện hệ thống có nguy cơ mất an toàn như: hệ thống hoạt động chậm bất thường, không truy cập được hệ thống, nội dung thông tin bị thay đổi không chủ động hoặc các dấu hiệu bất thường khác thì tiến hành quy trình ứng cứu sự cố theo các bước sau:

1. Bước 1: Nếu hệ thống có nguy cơ mất an toàn thông tin thuộc thẩm quyền cơ quan, đơn vị trực tiếp quản lý thì thực hiện tiếp Bước 2. Nếu hệ thống có nguy cơ mất an toàn thông tin thuộc Sở Thông tin và Truyền thông quản lý (các hệ thống được triển khai tập trung tại Trung tâm Dữ liệu tỉnh) thì thực hiện tiếp Bước 3;

2. Bước 2: Tiến hành xử lý sự cố theo quy chế nội bộ của cơ quan, đơn vị. Nếu sự cố được khắc phục thì lập biên bản ghi nhận và kết thúc quy trình phối hợp xử lý sự cố. Khi sự cố vượt quá khả năng xử lý của cơ quan, lập biên bản ghi nhận và thực hiện tiếp Bước 3;

3. Bước 3: Báo sự cố đến Sở Thông tin và Truyền thông theo mẫu số 03 của Thông tư số 20/2017/TT-BTTTT và thực hiện tiếp Bước 4;

4. Bước 4: Phối hợp với Sở Thông tin và Truyền thông và các cơ quan,tổ chức có liên quan để tiến hành khắc phục sự cố và thực hiện tiếp Bước 5;

5. Bước 5: Lập biên bản ghi nhận và kết thúc quy trình phối hợp xử lý sự cố theo mẫu số 04 của Thông tư số 20/2017/TT-BTTTT.

Điều 11. Các hành vi bị nghiêm cấm

Các hành vi bị nghiêm cấm theo quy định tại Điều 12 và khoản 2 Điều 72 của Luật Công nghệ thông tin mạng và các quy định khác có liên quan.

Chương III

TRÁCH NHIỆM VỀ ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 12. Trách nhiệm của các cơ quan, đơn vị chủ quản hệ thống thông tin

1. Thủ trưởng các cơ quan, đơn vị có trách nhiệm chỉ đạo thực hiện tuyên truyền nâng cao nhận thức cho cán bộ công chức viên chức và người lao động; và

chịu trách nhiệm trước Ủy ban nhân dân tỉnh trong công tác đảm bảo an toàn thông tin đối với hệ thống thông tin của cơ quan, đơn vị mình.

2. Thực hiện xác định cấp độ an toàn hệ thống thông tin theo quy định tại Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về đảm bảo an toàn hệ thống thông tin theo cấp độ.

3. Trong phạm vi quản lý của mình, thủ trưởng các cơ quan, đơn vị có trách nhiệm:

a) Thực hiện và chỉ đạo thực hiện Chương II của Quy chế này;

b) Thực hiện và chỉ đạo cán bộ, công chức viên chức và người lao động thuộc thẩm quyền quản lý thực hiện nghiêm túc Quy chế này;

c) Tạo điều kiện thuận lợi cho cán bộ, công chức, viên chức chuyên trách về công nghệ thông tin được đào tạo, bồi dưỡng chuyên môn trong lĩnh vực an toàn thông tin;

d) Quan tâm đầu tư các thiệt bị phần cứng, phần mềm liên quan đến công tác đảm bảo an toàn thông tin;

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

e) Cung cấp đầy đủ các thông tin, không che giấu thông tin sự cố; Tạo điều kiện thuận lợi cho các cơ quan chức năng trong công tác điều tra, làm rõ nguyên nhân gây ra sự cố, lực lượng kỹ thuật tham gia khắc phục sự cố phải thực hiện theo đúng hướng dẫn chuyên môn của cơ quan chức năng.

Điều 13. Trách nhiệm của Sở Y tế

1. Phối hợp thực hiện với Sở Thông tin và Truyền thông

a) Triển khai ác chính sách, văn bản chỉ đạo, kế hoạch nhằm đảm bảo an toàn thông tin mạng trên địa bàn tỉnh;

b) Tham gia tập huấn đội ngũ cán bộ chuyên trách về an toàn thông tin có trình độ đáp ứng yêu cầu theo quy định;

c) Tham gia đoàn kiểm tra về đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin trong các cơ quan, đơn vị nhà nước trên địa bàn tỉnh *(nếu có);*

3. Thực hiện nhiệm vụ cảnh báo về các nguy cơ, sự cố gây mất an toàn thông tin.

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

5. Phối hợp với Sở Thông tin và Truyền thông, Công an tỉnh, Bộ Chỉ huy Quân sự tỉnh và các cơ quan, đơn vị có liên quan tổ chức đoàn kiểm tra về an toàn thông tin để kịp thời phát hiện xử lý các hành vi vi phạm theo thẩm quyền.

6. Tổng hợp báo cáo về tình hình an toàn thông tin cho Ủy ban nhân tỉnh và các cơ quan, đơn vị có liên quan theo yêu cầu.

7. Duy trì hoạt động Tổ chuyên trách về an toàn, an ninh thông tin mạng ngành Y tế tỉnh BRVT, báo cáo các trường hợp xảy ra sự cố an toán an ninh mạng theo quy định.

Điều 17. Trách nhiệm của cán bộ công chức, viên chức và người lao động

1. Trách nhiệm của cán bộ chuyên trách công nghệ thông tin, an toàn thông tin tại cơ quan, đơn vị:

a) Chịu trách nhiệm triển khai các biện pháp quản lý vận hành, quản lý kỹ thuật và tham mưu xây dựng các quy định về đảm bảo an toàn thông tin cho toàn bộ hệ thống thông tin của cơ quan, đơn vị mình theo đung nội dung của Hướng dẫn này;

b) Chủ động phối hợp với cán bộ, công chức, viên chức và người lao động của cơ quan, đơn vị mình trong việc kiểm tra, phát hiện và khắc phục sự cố về an toàn thông tin;

c) Tuân thủ hướng dẫn kỹ thuật của các cơ quan, đơn vị chức năng trong quá trình khắc phục sự cố về an toàn thông tin;

d) Thường xuyên cập nhật, nâng cao kiến thức, trình độ chuyên môn đáp ứng yêu cầu đảm bảo an toàn thông tin của đơn vị; Tổ chức tuyên truyền, hướng dẫn các hướng dẫn kỹ thuật của cơ quan, đơn vị chức năng trong cảnh báo, phát hiện sự cố an toàn thông tin đến toàn thể cán bộ, công chức, viên chức và người lao động.

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

a) Nghiêm túc thực hiện các nội quy, quy định, quy trình nội bộ về đảm bảo an toàn thông tin của cơ quan, đơn vị mình cũng như các quy định khác của pháp luật về an toàn thông tin;

b) Khi phát hiện hoặc nghi ngờ các nguy cơ hoặc sự cố mất an toàn thông tin phải kịp thời báo cáo cho cán bộ chuyên trách công nghệ thông tin, an toàn thông tin của cơ quan, đơn vị mình để kịp thời ngăn chặn và xử lý;

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

d) Nghiêm cấm các hành vi làm mất, lộ lọt, phá hoại hệ thống thông tin của cơ quan, đơn vị mình.

Chương IV

TỔ CHỨC THỰC HIỆN

Điều 18. Tổ chức thực hiện

1. Lãnh đạo các cơ quan, đơn vị tổ chức triển khai thực hiện nghiêm Quy chế này, các Quy định, Hướng dẫn về an toàn thông tin mạng của các cơ quan cấp trên và các quy chế quy định cụ thể về an toàn thông tin của từng hệ thống thông tin *(Hệ thống thư điện tử công vụ, Hệ thống phần mềm văn phòng điện tử và các hệ thống thông tin khác).*

2. Trong điều kiện cụ thể, từng đơn vị có thể dựa trên nội dung của Quy chế này xây dựng Quy chế đảm bảo an toàn thông tin áp dụng cho cơ quan, đơn vị mình.

3. Trong quá trình thực hiện, khi có khó khăn, vướng mắc, phát sinh cần sửa đổi, bổ sung, điều chỉnh đề nghị các đơn vị kịp thời báo cáo về Sở Y tế tổng hợp gửi Sở thông tin và Truyền thông xem xét, trình Ủy ban nhân dân tỉnh có ý kiến chỉ đạo.

Điều 19. Khen thưởng, xử lý vi phạm

1. Hàng năm, Sở Thông tin và Truyền thông sẽ dựa trên đánh giá mức độ ứng dụng công nghệ thông tin tại các sở ban ngành; huyện, thành phố có các hình thức khen thưởng theo quy định; hoặc khen thưởng đột xuất đối với cá nhân, tổ chức kịp thời phát hiện, ngăn chặn các cuộc tấn công mạng có quy mô lớn trong phạm vi toàn tỉnh hoặc hơn.

2.Tổ chức, cá nhân có hành vi vi phạm Quy chế này tùy theo tính chất, mức độ vi phạm sẽ bị xử lý kỷ luật theo trách nhiệm, xử phạt hành chính, bồi thường thiệt hại hoặc truy tố trách nhiệm hình sự theo quy định của pháp luật./.

GIÁM ĐỐC