BẢO HIỂM XÃ HỘI VIỆT NAM	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
	Độc lập - Tự do - Hạnh phúc
Số: 967 /QĐ-BHXH	*Hà Nội, ngày 20 tháng 6 năm 2017*

QUYẾT ĐỊNH

Về việc ban hành Quy chế Bảo đảm an toàn thông tin trong ứng dụng công nghệ thông tin của ngành Bảo hiểm xã hội

TỔNG GIÁM ĐỐC BẢO HIỂM XÃ HỘI VIỆT NAM

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

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

Căn cứ Nghị định số 01/2016/NĐ-CP ngày 05/01/2016 của Chính phủ về việc quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bảo hiểm xã hội Việt Nam;

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 166/2016/NĐ-CP ngày 24/12/2016 của Chính phủ quy định về giao dịch điện tử trong lĩnh vực Bảo hiểm xã hội, bảo hiểm y tế và bảo hiểm thất nghiệp;

Xét đề nghị của Giám đốc Trung tâm Công nghệ thông tin,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế Bảo đảm an toàn thông tin trong ứng dụng công nghệ thông tin của ngành Bảo hiểm xã hội.

Điều 2. Quyết định này có hiệu lực thi hành từ ngày ký.

Điều 3. Giám đốc Trung tâm Công nghệ thông tin, Chánh Văn phòng Bảo hiểm xã hội Việt Nam, Thủ trưởng các đơn vị trực thuộc BHXH Việt Nam, Giám đốc Bảo hiểm xã hội các tỉnh, thành phố trực thuộc Trung ương chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Tổng Giám đốc (để b/c);
- Các Phó TGĐ;
- Lưu: VT, CNTT(03).

KT. TỔNG GIÁM ĐỐC
PHÓ TỔNG GIÁM ĐỐC

BẢO HIỂM XÃ HỘI VIỆT NAM

Phạm Lương Sơn

BẢO HIỂM XÃ HỘI VIỆT NAM

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

QUY CHẾ
Bảo đảm an toàn thông tin trong ứng dụng công nghệ thông tin ngành Bảo hiểm xã hội

(Ban hành kèm theo Quyết định số :967../QĐ-BHXH ngày 20...tháng ..6.. năm 2017 của Tổng Giám đốc BHXH Việt Nam)

Chương I
QUY ĐỊNH CHUNG

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

1. Quy chế này quy định về công tác bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin (CNTT) của các đơn vị thuộc hệ thống ngành BHXH (sau đây gọi tắt là đơn vị).

2. Quy chế này được áp dụng đối với các đơn vị, cá nhân trực tiếp tham gia hoặc liên quan đến hoạt động an toàn thông tin mạng trong các đơn vị thuộc hệ thống ngành BHXH.

Điều 2. Mục đích, nguyên tắc bảo đảm an toàn thông tin mạng

1. Việc áp dụng Quy chế này nhằm giảm thiểu được các nguy cơ gây mất an toàn thông tin mạng và bảo đảm an toàn thông tin mạng trong quá trình ứng dụng CNTT trong hoạt động của các đơn vị.

2. Việc bảo đảm an toàn thông tin mạng là yêu cầu bắt buộc và phải được thực hiện thường xuyên, liên tục, hiệu quả trên cơ sở tuân thủ tiêu chuẩn, quy chuẩn, quy định về an toàn thông tin mạng trong quá trình thiết kế, xây dựng, vận hành, nâng cấp, sử dụng và hủy bỏ trong ứng dụng CNTT của Ngành.

3. Các hoạt động an toàn thông tin mạng phải tuân theo Luật An toàn thông tin mạng số 86/2015/QH13 của Quốc hội; Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về việc bảo đảm an toàn hệ thống thông tin theo cấp độ và quy định của pháp luật có liên quan.

4. Thủ trưởng các đơn vị là người chịu trách nhiệm trực tiếp chỉ đạo công tác bảo đảm an toàn thông tin mạng.

5. Các đơn vị bố trí nguồn lực phù hợp với quy mô, điều kiện của mình nhằm thực hiện tốt nhất công tác bảo đảm an toàn thông tin mạng.

6. Các đơn vị và cá nhân có trách nhiệm thực hiện đầy đủ, nghiêm túc các quy định của pháp luật, quy định, quy chế của Bảo hiểm xã hội Việt Nam về bảo vệ bí mật nhà nước và bảo đảm an toàn thông tin mạng.

7. Các văn bản thuộc danh mục bí mật nhà nước phải thực hiện trên máy tính riêng, nghiêm cấm sử dụng máy tính có kết nối Internet, mạng nội bộ (LAN) hay các thiết bị thông minh để soạn thảo.

8. Các dữ liệu khi trao đổi với các hệ thống thông tin ngoài ngành phải có kênh truyền dữ liệu riêng và được mã hóa bằng giải pháp do Ban Cơ yếu Chính phủ cung cấp hoặc cơ quan, đơn vị có thẩm quyền của Bộ Thông tin và Truyền thông chấp nhận sử dụng.

9. Khi thực hiện thuê dịch vụ CNTT hoặc sử dụng dịch vụ CNTT do bên thứ ba cung cấp, đơn vị và cá nhân phải quản lý việc sở hữu thông tin, dữ liệu từ dịch vụ đó; yêu cầu nhà cung cấp dịch vụ có trách nhiệm bảo mật thông tin; không để nhà cung cấp dịch vụ truy nhập, sử dụng thông tin, dữ liệu thuộc phạm vi nhà nước quản lý.

Điều 3. Giải thích từ ngữ

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

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 bảo đảm 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. *Sự cố an toàn thông tin mạng* là việc thông tin, hệ thống thông tin bị gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng.

5. *Mã độc* 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.

6. *Nguy cơ mất an toàn thông tin* là những nhân tố bên trong hoặc bên ngoài có khả năng ảnh hưởng tới trạng thái an toàn thông tin.

7. *Đánh giá rủi ro 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.

8. *Quản lý rủi ro an toàn thông tin* là việc thực hiện đánh giá rủi ro an toàn thông tin, xác định yêu cầu bảo vệ thông tin, hệ thống thông tin và áp dụng giải pháp phòng, chống, giảm thiểu thiệt hại khi có sự cố mất an toàn thông tin.

Chương II

QUY ĐỊNH BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 4. Về quản lý cán bộ, công chức, viên chức và người lao động

Các đơn vị phải thường xuyên tổ chức quán triệt các quy định về an toàn thông tin mạng, nhằm nâng cao nhận thức về trách nhiệm bảo đảm an toàn thông tin mạng của từng cá nhân trong đơn vị.

Điều 5. Quản lý hạ tầng thiết bị CNTT

1. Hạ tầng thiết bị CNTT phải được trang bị tường lửa (firewall) để ngăn chặn và phát hiện các xâm nhập trái phép vào mạng nội bộ. Nhật ký hoạt động của thiết bị tường lửa phải được lưu giữ an toàn trong khoảng thời gian nhất định (tối thiểu 03 tháng) để phục vụ công tác khảo sát, điều tra khi có sự cố xảy ra.

2. Các thiết bị quan trọng như tường lửa, thiết bị định tuyến (router), hệ thống máy chủ (server), hệ thống lưu trữ dữ liệu (storage)... phải được đặt trong trung tâm dữ liệu/phòng máy chủ và có các biện pháp bảo vệ, ngăn chặn xâm nhập trái phép vào trung tâm dữ liệu/phòng máy chủ.

3. Trung tâm dữ liệu/phòng máy chủ của các đơn vị (Trung tâm CNTT, Văn phòng BHXH Việt Nam, BHXH các tỉnh, thành phố, BHXH cấp huyện) 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 đơn vị mới được phép ra vào trung tâm dữ liệu/phòng máy chủ.

4. Quá trình vào, ra trung tâm dữ liệu/phòng máy chủ phải được ghi nhận vào nhật ký quản lý trung tâm dữ liệu/phòng máy chủ.

5. Trung tâm dữ liệu phải được thiết kế, xây dựng, quản trị vận hành, khai thác theo tiêu chuẩn, quy chuẩn kỹ thuật quy định tại Thông tư 03/2013/TT-BTTTT ngày 22/01/2013 của Bộ Thông tin và Truyền thông quy định áp tiêu chuẩn, quy chuẩn kỹ thuật đối với trung tâm kỹ thuật. Phòng máy chủ phải áp dụng các tiêu chuẩn kỹ thuật về an toàn kỹ thuật nhiệt độ, độ ẩm,... cho các thiết bị; bảo đảm điều kiện hoạt động ổn định cho các hệ thống hỗ trợ như máy điều hòa nhiệt độ, nguồn cấp điện, dây dẫn.

6. Trung tâm dữ liệu/phòng máy chủ phải có hệ thống lưu điện đủ công suất và duy trì thời gian hoạt động của các thiết bị CNTT trong vòng 15 phút.

7. Các thiết bị hạ tầng CNTT quan trọng phải được triển khai có dự phòng, bảo đảm hoạt động khi có sự cố xảy ra.

Điều 6. Bảo đảm an toàn thông tin hệ thống mạng truyền thông

1. Môi trường mạng Internet, khi thiết lập các dịch vụ trên Internet chỉ cung cấp những chức năng, cổng giao tiếp mạng, giao thức và các dịch vụ thiết yếu nhất bảo đảm duy trì hoạt động của hệ thống thông tin.

2. Mạng không dây (WIFI), cần thiết lập các thông số an toàn và định kỳ ít nhất 3 tháng thay đổi mật khẩu truy cập nhằm tăng cường công tác bảo mật.

3. Hệ thống mạng nội bộ (LAN) phải được bảo vệ bằng tường lửa và phân chia hệ thống mạng thành các vùng mạng quản lý theo chính sách an toàn thông tin riêng, phạm vi truy cập, kiểm soát truy cập giữa các vùng mạng, bao gồm: vùng mạng người dùng; vùng mạng truy cập Internet; vùng máy chủ nội bộ; vùng mạng quản trị.

4. Hệ thống mạng diện rộng (WAN), các đơn vị khi thực hiện kết nối tới WAN phải bảo đảm an toàn thông tin đối với hệ thống mạng nội bộ và các thiết bị thuộc phạm vi quản lý.

5. Các hệ thống mạng phải được thiết kế có đầy đủ thiết bị tường lửa, chống truy cập trái phép, lọc Web...; phải được cài đặt, cập nhật, vá lỗi đúng thời hạn để khắc phục các điểm yếu an ninh mạng.

Điều 7. Bảo đảm an toàn thông tin mức ứng dụng và dữ liệu

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

2. Các ứng dụng phải được thực hiện kiểm tra tính hợp lệ của dữ liệu đầu vào và đầu ra để bảo đảm dữ liệu chính xác và phù hợp.

3. Hạn chế truy cập tới mã nguồn ứng dụng (nếu có) và phải đặt mã nguồn trong môi trường an toàn do bộ phận chuyên trách quản lý.

4. Thực hiện kiểm tra phát hiện và khắc phục lỗ hổng bảo mật của ứng dụng trước khi đưa vào sử dụng, trong quá trình sử dụng (theo định kỳ) và sau khi nâng cấp, cập nhật bổ sung tính năng.

5. Theo dõi nắm bắt thông tin về các lỗ hổng bảo mật mới và cập nhật thường xuyên bản vá lỗi về an ninh cho ứng dụng và hệ điều hành.

6. Thiết lập phân quyền truy nhập, quản trị ứng dụng với người sử dụng/nhóm người sử dụng theo đúng yêu cầu nghiệp vụ.

7. Thiết lập các hệ thống tường lửa lớp ứng dụng và CSDL bảo đảm tính bí mật, nguyên vẹn và khả dụng của dữ liệu; giám sát, cảnh báo khi có thay đổi hoặc phát hiện, ngăn chặn các tác động truy nhập, gửi, nhận dữ liệu trái phép.

8. Định kỳ thực hiện sao lưu các CSDL nghiệp vụ sang các hệ thống tủ đĩa dự phòng và thiết bị sao lưu băng từ.

9. Sử dụng chữ ký số và các giao thức truyền tin an toàn khi thực hiện giao dịch điện tử với người dân và đơn vị sử dụng lao động.

Điều 8. Phòng chống mã độc

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

2. Các cán bộ, công chức, viên chức và người lao động trong đơn vị phải được hướng dẫn về phòng chống mã độc, các rủi ro do mã độc gây ra; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm trên máy trạm khi chưa có sự đồng ý của người có thẩm quyền theo quy định của đơn vị.

3. 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.

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

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

Điều 9. Quản lý nhật ký trong quá trình vận hành các hệ thống thông tin

1. Các đơn vị có quản lý trung tâm dữ liệu/phòng máy chủ phải thực hiện việc ghi nhật ký (log) của toàn bộ hệ thống thông tin nhằm bảo đảm các sự kiện quan trọng xảy ra trên hệ thống được ghi nhận và lưu giữ.

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

3. Các sự kiện tối thiểu cần phải được ghi nhật ký gồm: quá trình đăng nhập 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 thực hiện việc theo dõi bản ghi nhật ký của hệ thống và các sự kiện khác có liên quan để đánh giá, báo cáo các rủi ro và mức độ nghiêm trọng các rủi ro đó.

Điều 10. Quản lý truy cập

1. Các quy định về quản lý truy cập vào hệ thống thông tin của đơn vị phải được quy định chi tiết và tổ chức thực hiện nghiêm túc, phù hợp với các quy định của pháp luật về an toàn thông tin mạng.

2. Cá nhân sử dụng hệ thống thông tin được cấp và sử dụng tài khoản truy nhập duy nhất gắn với cá nhân đó và chịu trách nhiệm bảo mật thông tin tài khoản của mình.

3. Hủy tài khoản, quyền truy cập các hệ thống thông tin, thu hồi lại tất cả các tài sản liên quan tới hệ thống thông tin (chữ ký số, thẻ nhận dạng, thư mục

lưu trữ, thư điện tử, máy vi tính, ...) đối với các cá nhân nghỉ việc, chuyển công tác.

4. Tài khoản quản trị của người quản trị hệ thống thông tin (mạng, hệ điều hành, thiết bị kết nối mạng, phần mềm, ứng dụng, cơ sở dữ liệu) phải cấp phát và quản lý thông qua hệ thống quản lý mật khẩu đặc quyền của BHXH Việt Nam.

5. 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.

6. Các hệ thống thông tin cần giới hạn số lần đăng nhập sai liên tiếp vào hệ thống. Hệ thống tự động khoá 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.

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 10 phút không sử dụng.

8. Mạng không dây trong nội bộ đơn vị phải đặt mật khẩu truy cập và chỉ cho phép truy cập Internet.

9. Mật khẩu đăng nhập vào các hệ thống thông tin quan trọng phải có độ phức tạp cao (có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự số và ký tự đặc biệt như !, @, #, $, %,...) và phải được thay đổi ít nhất 3 tháng/lần.

Điều 11. Quản lý sự cố an toàn thông tin mạng

1. Phân loại mức độ nghiêm trọng của các sự cố an toàn thông tin mạng, bao gồm:

a) Thấp: sự cố gây ảnh hưởng cá nhân và không làm gián đoạn hay đình trệ hoạt động chính của đơn vị;

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

c) Cao: sự cố làm cho thiết bị, phần mềm hay hệ thống không thể sử dụng được và gây ảnh hưởng đến một trong các hoạt động chính của đơn vị;

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

2. Khi có sự cố hoặc nguy cơ mất an toàn thông tin mạng thì lãnh đạo đơn vị phải chỉ đạo kịp thời để khắc phục và hạn chế thiệt hại, báo cáo bằng văn bản cho đơn vị cấp trên trực tiếp quản lý.

3. 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 báo cáo ngay cho đơn vị cấp trên quản lý trực tiếp và Trung tâm CNTT - BHXH Việt Nam để được hướng dẫn, hỗ trợ.

Điều 12. Các hành vi bị nghiêm cấm

1. Tạo ra, cài đặt, phát tán thư rác, tin nhắn rác, vi rút máy tính, phần mềm độc hại trái pháp luật; thiết lập hệ thống thông tin giả mạo, lừa đảo.

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

3. Cản trở trái pháp luật, gây ảnh hưởng tới sự hoạt động bình thường của hệ thống thông tin hoặc cản trở trái pháp luật, gây ảnh hưởng tới khả năng truy nhập hợp pháp của người sử dụng tới hệ thống thông tin;

4. Bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã và thông tin của đơn vị, cá nhân khác trên môi trường mạng.

5. Tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng của biện pháp bảo vệ an toàn thông tin cho hệ thống thông tin; lợi dụng sơ hở, điểm yếu của hệ thống thông tin, tấn công, chiếm quyền điều khiển trái phép đối với hệ thống thông tin;

6. Lợi dụng mạng để truyền bá thông tin, quan điểm, thực hiện các hành vi gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, lợi ích quốc gia trên mạng; phá hại khối đại đoàn kết toàn dân; tuyên truyền chiến tranh xâm lược, khủng bố; gây hận thù, mâu thuẫn giữa các dân tộc, sắc tộc, tôn giáo và bài ngoại;

7. Lợi dụng mạng để truyền bá trái phép tài liệu, hình ảnh, âm thanh hoặc dạng thông tin khác nhằm kích động bạo lực, dâm ô, đồi trụy, tội ác, tệ nạn xã hội, mê tín dị đoan, phá hoại thuần phong, mỹ tục của dân tộc; bôi nhọ, gây thù hận, xâm hại tới quyền và lợi ích hợp pháp của tổ chức, cá nhân;

8. Các hành vi khác bị nghiêm cấm theo quy định của pháp luật.

Chương III

TRÁCH NHIỆM BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 13. Trách nhiệm của cán bộ, công chức, viên chức và người lao động trong các đơn vị

1. Trách nhiệm của cán bộ, công chức, viên chức phụ trách an toàn thông tin mạng:

a) Chịu trách nhiệm bảo đảm an toàn thông tin mạng của đơn vị;

b) Tham mưu lãnh đạo đơn vị ban hành các quy định, quy trình nội bộ, triển khai các giải pháp kỹ thuật bảo đảm an toàn thông tin;

c) Thực hiện việc giám sát, đánh giá, báo cáo thủ trưởng đơn vị các rủi ro mất an toàn thông tin và mức độ nghiêm trọng của các rủi ro đó;

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

2. Trách nhiệm của cán bộ, công chức, viên chức trong các đơn vị:

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

b) Mỗi cán bộ, công chức, viên chức và người lao động phải có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng; không tự ý thay đổi, tháo lắp các thiết bị trên máy tính; không được truy cập các trang web không rõ về nội dung; không tải và cài đặt các phần mềm không rõ nguồn gốc, không liên quan đến công việc chuyên môn; không nhấp chuột vào các đường dẫn lạ không rõ về nội dung;

c) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin phải báo cáo ngay với cấp trên và bộ phận chuyên trách CNTT của đơn vị để kịp thời ngăn chặn và xử lý;

d) Tham gia các chương trình đào tạo, hội nghị về an toàn thông tin mạng do Bảo hiểm xã hội Việt nam hoặc các đơn vị chuyên môn về an toàn thông tin trên địa bàn tổ chức.

Điều 14. Trách nhiệm của các đơn vị

1. Thủ trưởng các đơn vị có trách nhiệm tổ chức thực hiện các quy định tại Quy chế này và chịu trách nhiệm trước BHXH Việt Nam trong công tác bảo đảm an toàn thông tin mạng của đơn vị mình.

2. Phân công một 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.

3. 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 xảy ra một cách kịp thời, nhanh chóng và đạt hiệu quả.

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

5. Định kỳ hằng quý, các đơn vị (Văn phòng BHXH Việt Nam; các đơn vị sự nghiệp trực thuộc BHXH Việt Nam; BHXH các tỉnh, thành phố) lập báo cáo về tình hình an toàn thông tin mạng và gửi về Trung tâm CNTT – BHXH Việt Nam.

Điều 15. Trách nhiệm của Trung tâm CNTT

1. Tham mưu cho Tổng Giám đốc BHXH Việt Nam về việc quản lý an toàn thông tin trong hoạt động ứng dụng CNTT của Ngành.

2. Xây dựng kế hoạch triển khai công tác bảo đảm an toàn thông tin phục vụ cho việc vận hành các hệ thống thông tin được BHXH Việt Nam giao quản lý.

3. Chủ trì, phối hợp với các đơn vị liên quan tổ chức kiểm tra theo định kỳ hoặc đột xuất; kịp thời phát hiện và kiến nghị cấp thẩm quyền xử lý theo quy định của quy chế này và của pháp luật hiện hành đối với các đơn vị, cá nhân có các dấu hiệu, hành vi vi phạm an toàn thông tin mạng trên phạm vi toàn Ngành.

4. Hàng năm xây dựng và triển khai các chương trình đào tạo chuyên sâu về an ninh thông tin mạng cho lực lượng bảo đảm an toàn thông tin mạng của các đơn vị.

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

6. Hướng dẫn, giám sát các đơn vị trong toàn Ngành thực hiện việc bảo đảm an toàn, an ninh cho hệ thống thông tin theo quy định của Nhà nước.

7. Là đầu mối với các cơ quan chức năng, đơn vị chuyên môn trong và ngoài Ngành định kỳ rà soát, đánh giá và xác định các sự cố an toàn thông tin, các rủi ro an toàn thông tin có thể xảy ra với từng thành phần hệ thống thông tin của Ngành. Trên cơ sở đó, xây dựng và trình Lãnh đạo Ngành phê duyệt các phương án ứng cứu, xử lý sự cố phù hợp với các rủi ro an toàn thông tin có thể xảy ra.

8. Là đầu mối với các cơ quan chức năng, đơn vị chuyên môn trong và ngoài Ngành chuẩn bị sẵn sàng các biện pháp, phương tiện kỹ thuật để phục vụ cho triển khai các phương án ứng cứu đã được xây dựng.

9. Xây dựng và ban hành các hướng dẫn, quy trình xử lý sự cố an toàn thông tin đối với từng đối tượng người sử dụng cụ thể trong hệ thống thông tin theo hướng dẫn của các cơ quan chuyên môn về an toàn thông tin quốc gia.

10. Tổng hợp và báo cáo về tình hình an toàn, an ninh thông tin cho BHXH Việt Nam.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 16. Khen thưởng và xử lý vi phạm

1. Hàng năm, Trung tâm CNTT dựa trên các điều tra, báo cáo công tác an ninh thông tin mạng của các đơn vị để xác lập bảng xếp hạng an toàn thông tin mạng, trên cơ sở đó đề xuất BHXH Việt Nam xem xét khen thưởng theo quy định hiện hành.

2. Các đơn vị hoặc cá nhân vi phạm Quy chế này, tùy theo tính chất, mức độ vi phạm có thể bị xử lý hành chính, xử lý kỷ luật hoặc các hình thức xử lý khác theo quy định hiện hành; nếu vi phạm gây thiệt hại lớn đến tài nguyên thông tin của Ngành thì phải chịu trách nhiệm về những thiệt hại gây ra theo quy định của pháp luật.

Điều 17. Điều khoản thi hành

1. Thủ trưởng các đơn vị trực thuộc BHXH Việt Nam, Giám đốc BHXH các tỉnh, thành phố chịu trách nhiệm tổ chức triển khai thực hiện Qùy chế tại đơn vị mình.

2. Trong quá trình thực hiện Quy chế này, nếu có vướng mắc, đơn vị, cá nhân phản ánh về Trung tâm CNTT để tổng hợp, báo cáo BHXH Việt Nam xem xét, sửa đổi, bổ sung Quy chế cho phù hợp./.

KT. TỔNG GIÁM ĐỐC
PHÓ TỔNG GIÁM ĐỐC

BẢO HIỂM XÃ HỘI VIỆT NAM

Phạm Lương Sơn