

Số: 3735/QĐ-BHXH

Hà Nội, ngày 29 tháng 12 năm 2022

QUYẾT ĐỊNH

**BAN HÀNH QUY CHẾ QUẢN LÝ, TRIỂN KHAI, VẬN HÀNH VÀ KHAI
THÁC HỆ THỐNG HẠ TẦNG THÔNG TIN TRONG NGÀNH BẢO HIỂM XÃ
HỘI VIỆT NAM**

TỔNG GIÁM ĐỐC BẢO HIỂM XÃ HỘI VIỆT NAM

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 Nghị định 89/2020/NĐ-CP ngày 04 tháng 8 năm 2020 của Chính phủ 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 tháng 4 năm 2007 của Chính phủ về ứng dụng Công nghệ thông tin trong hoạt động của cơ quan nhà nước;

Căn cứ Quyết định số 749/QĐ-TTg ngày 03 tháng 6 năm 2020 của Thủ tướng Chính phủ phê duyệt Chương trình chuyển đổi số quốc gia đến năm 2025, định hướng năm 2030;

Căn cứ Quyết định số 942/QĐ-TTg ngày 15 tháng 6 năm 2021 của Thủ tướng Chính phủ phê duyệt Chiến lược phát triển Chính phủ điện tử hướng tới Chính phủ số giai đoạn 2021-2025, định hướng đến năm 2030;

Căn cứ Quyết định số 861/QĐ-BHXH ngày 01 tháng 9 năm 2021 của Tổng Giám đốc Bảo hiểm xã hội Việt Nam thành lập Ban chỉ đạo chuyển đổi số ngành Bảo hiểm xã hội Việt Nam;

Căn cứ Quyết định số 345/QĐ-BHXH ngày 09 tháng 4 năm 2021 của Tổng Giám đốc Bảo hiểm xã hội Việt Nam thành lập đội ứng cứu sự cố, bảo đảm an toàn thông tin mạng ngành Bảo hiểm xã hội Việt Nam;

Căn cứ Quyết định số 2358/QĐ-BHXH ngày 19 tháng 9 năm 2022 của Tổng Giám đốc Bảo hiểm xã hội Việt Nam phê duyệt kiến trúc Chính phủ điện tử ngành Bảo hiểm xã hội Việt Nam, phiên bản 2.0;

Theo đề nghị của Giám đốc Trung tâm Công nghệ thông tin.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế quản lý, triển khai, vận hành và khai thác hệ thống hạ tầng thông tin trong ngành Bảo hiểm xã hội Việt Nam.

Điều 2. Quyết định này có hiệu lực từ ngày 01/01/2023 và thay thế Quyết định số 3582/QĐ-BHXH ngày 26 tháng 12 năm 2006 của Tổng Giám đốc Bảo hiểm xã hội Việt Nam ban hành quy định về quản lý hoạt động công nghệ thông tin trong hệ thống Bảo hiểm xã hội Việt Nam.

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 Bảo hiểm xã hội Việt Nam, Giám đốc Bảo hiểm xã hội các tỉnh, thành phố trực thuộc Trung ương và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:

- Như điều 3;
- Tổng Giám đốc;
- Các Phó Tổng Giám đốc;
- Lưu: VT, CNTT.

TỔNG GIÁM ĐỐC

Nguyễn Thế Mạnh



QUY CHẾ

QUẢN LÝ, TRIỂN KHAI, VẬN HÀNH VÀ KHAI THÁC HỆ THỐNG HẠ TẦNG THÔNG TIN TRONG NGÀNH BẢO HIỂM XÃ HỘI VIỆT NAM (Ban hành kèm theo Quyết định số 3735/QĐ-BHXH ngày 29 tháng 12 năm 2022 của Tổng Giám đốc Bảo hiểm xã hội Việt Nam)

Chương I

QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

1. Quy chế này quy định về việc quản lý, triển khai, vận hành và khai thác hệ thống hạ tầng thông tin tại các đơn vị trực thuộc Bảo hiểm xã hội Việt Nam và Bảo hiểm xã hội tỉnh, thành phố (sau đây gọi là Bảo hiểm xã hội tỉnh) trực thuộc trung ương, Bảo hiểm xã hội huyện, quận, thị xã, thành phố (sau đây gọi là Bảo hiểm xã hội huyện) trực thuộc Bảo hiểm xã hội tỉnh (sau đây gọi chung là các đơn vị).

2. Các công chức, viên chức và lao động hợp đồng trực thuộc ngành Bảo hiểm xã hội Việt Nam tham gia khai thác, sử dụng hệ thống hạ tầng thông tin chịu sự điều chỉnh của Quy chế này.

Điều 2. Giải thích từ ngữ và từ viết tắt

1. Giải thích từ ngữ

a) Hệ thống hạ tầng thông tin là tập hợp trang thiết bị (máy chủ, thiết bị lưu trữ, thiết bị mạng, thiết bị bảo mật, máy trạm, máy tính xách tay, các thiết bị đầu cuối), đường truyền dẫn kết nối phục vụ chung hoạt động nghiệp vụ của Ngành.

b) 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.

c) Người dùng là người sử dụng hệ thống hạ tầng thông tin.

d) LAN (Local Area Network): Hệ thống mạng nội bộ được thiết kế để kết nối các máy tính, mạng không dây trong một phạm vi nhỏ.

đ) WAN (Wide Area Network): Hệ thống mạng diện rộng được thiết kế để kết nối, truyền dữ liệu giữa BHXH tỉnh với các BHXH huyện và giữa BHXH tỉnh với BHXH Việt Nam.

e) VPN (Virtual Private Network): Mạng riêng ảo là cấu phần thuộc hạ tầng truyền thông kết nối máy tính của cán bộ BHXH khi đi công tác, làm việc bên ngoài cơ quan vào hệ thống mạng nội bộ của đơn vị qua đường truyền Internet, nhằm phục vụ truy cập vào các hệ thống thông tin để làm việc từ xa.

g) Thiết bị mạng là thiết bị định tuyến, chuyển mạch, proxy, cân bằng tải, tường lửa, tối ưu mạng...

h) Hạ tầng truyền thông là thiết bị mạng, đường truyền dữ liệu phục vụ kết nối mạng LAN, Wifi, WAN, Internet, VPN.

i) Thiết bị công nghệ thông tin là các thiết bị bao gồm máy tính (máy chủ, máy trạm), thiết bị kết nối mạng, thiết bị bảo đảm an toàn thông tin, máy in, máy quét, các thiết bị ngoại vi khác đầu nối trực tiếp vào máy tính qua giao diện kết nối mạng, USB và phần mềm hệ thống, phần mềm ứng dụng, phần mềm tiện ích, phần mềm công cụ được cài đặt trên máy tính.

k) Bộ phận công nghệ thông tin là đơn vị tổ chức thực hiện quản lý, triển khai, vận hành hệ thống hạ tầng thông tin tại các đơn vị trực thuộc BHXH Việt Nam, BHXH tỉnh và BHXH huyện hoặc người thực hiện việc quản lý, triển khai, vận hành hệ thống hạ tầng thông tin trong ngành BHXH Việt Nam theo vị trí việc làm công nghệ thông tin thuộc các đơn vị trực thuộc BHXH Việt Nam, BHXH tỉnh và BHXH huyện.

l) Quản trị viên (chuyên trách hoặc kiêm nhiệm) là người quản trị mạng, quản trị hệ thống, quản trị cơ sở dữ liệu, quản trị phần mềm, quản trị hạ tầng tại các Bộ phận Công nghệ thông tin.

m) Phòng máy chủ là phòng máy chủ tại BHXH tỉnh, các đơn vị trực thuộc BHXH Việt Nam hoặc khu vực đặt các thiết bị mạng tại BHXH huyện.

2. Từ ngữ viết tắt

a) BHXH: Bảo hiểm xã hội.

b) CNTT: Công nghệ thông tin.

c) ATTT: An toàn thông tin

d) CCVC: Công chức, viên chức và lao động hợp đồng.

đ) SSO (Single Sign On): Đăng nhập một lần.

e) AD (Active Directory): Hệ thống quản lý tập trung dữ liệu người dùng.

Chương II

QUẢN LÝ HỆ THỐNG HẠ TẦNG THÔNG TIN

Điều 3. Yêu cầu về an toàn thông tin

Hệ thống thông tin phải được thường xuyên giám sát, theo dõi bảo đảm các nguyên tắc về ATTT trong hệ thống bao gồm:

1. Tính bí mật: Các thông tin cá nhân của người dùng như thư điện tử, dữ liệu trên thư mục người dùng phải được bảo đảm bí mật. Thông tin cá nhân không thể bị tiếp cận bởi những người không có thẩm quyền.

2. Tính nguyên vẹn: Thông tin chỉ có thể bị sửa đổi, xóa hoặc bổ sung bởi cá nhân chủ sở hữu thông tin.

3. Tính sẵn sàng: Thông tin luôn sẵn sàng đáp ứng nhu cầu sử dụng của người dùng.

4. Tính không thể phủ nhận: Người khởi tạo thông tin không thể phủ nhận trách nhiệm đối với thông tin do mình tạo ra.

5. Tính xác thực: Xác định được nguồn gốc của thông tin.

Điều 4. Quản lý mật khẩu

1. Lãnh đạo Bộ phận CNTT có trách nhiệm tiếp nhận mật khẩu quản trị hệ thống sau khi hệ thống được triển khai lần đầu và bàn giao cho Quản trị viên có biên bản kèm theo.

2. Quản trị viên phải đổi mật khẩu ngay sau khi tiếp nhận và báo cáo lãnh đạo Bộ phận CNTT, lưu vào nơi an toàn (cho vào phong bì, để vào tủ có khóa). Việc đổi mật khẩu quản trị hệ thống phải tuân thủ theo đúng hướng dẫn của BHXH Việt Nam.

3. Mật khẩu tài khoản người dùng phải được giữ bí mật và chỉ bàn giao cho đúng người đăng ký tài khoản đó.

4. Mật khẩu phải đảm bảo độ phức tạp về độ dài, nội dung và thời gian sử dụng:

a) Độ dài của mật khẩu:

- Đối với mật khẩu của người dùng (sử dụng đăng nhập hệ thống, thư điện tử, ứng dụng nghiệp vụ, Internet, máy tính cá nhân): Độ dài tối thiểu là 8 ký tự.

- Đối với mật khẩu quản trị hệ thống (sử dụng cho việc quản trị các hệ thống mạng, bảo mật, máy chủ, thư điện tử, ứng dụng nghiệp vụ): Độ dài tối thiểu là 12 ký tự.

b) Nội dung mật khẩu:

- Nội dung của mật khẩu không bao gồm các từ dễ nhớ như tên, ngày sinh, số điện thoại.

- Nội dung mật khẩu quản trị hệ thống phải bao gồm, kết hợp các loại sau: chữ cái in thường, chữ cái in hoa, ký tự đặc biệt, số.

c) Thời gian sử dụng mật khẩu:

- Đối với mật khẩu của người dùng: thay đổi định kỳ tối thiểu một lần trong 6 tháng.

- Đối với mật khẩu quản trị hệ thống: thay đổi định kỳ tối thiểu một lần trong 3 tháng.

Điều 5. Kiểm soát truy nhập và xác thực người dùng

1. Hệ thống AD

a) Việc quản lý, xác thực được người dùng truy nhập trên hệ thống AD bảo đảm đầy đủ thông tin người dùng hệ thống bao gồm họ tên, chức vụ, đơn vị công tác, số điện thoại.

b) Cấp phát quyền truy cập, sử dụng và khai thác ứng dụng, tài nguyên trên mạng phải bảo đảm chặt chẽ, đúng mục đích sử dụng. Mỗi người dùng chỉ được cấp một tài khoản và được phân quyền đủ để thực hiện nhiệm vụ được phân công.

c) Kiểm tra và loại bỏ kịp thời tài khoản của người dùng đã chuyển công tác, nghỉ hưu, hết hạn sử dụng hoặc không còn làm việc tại đơn vị trên hệ thống và cập nhật trên các tài liệu liên quan.

d) Tạm dừng quyền sử dụng đối với tài khoản của người dùng đã được đăng ký trên hệ thống nhưng không có hoạt động từ 30 ngày trở lên.

đ) Giới hạn số lần cho phép đăng nhập liên tục vào hệ thống là 5 lần. Sau 5 lần không đăng nhập thành công, tài khoản sẽ bị khóa trong 30 phút.

e) Phát hiện và xử lý kịp thời những trường hợp người dùng truy nhập bất hợp pháp hoặc thao tác vượt quá giới hạn được giao.

2. Hệ thống SSO

a) Mỗi cá nhân được cấp một tài khoản hệ thống SSO có định dạng theo nguyên tắc: Tên người dùng (không dấu) + họ (viết tắt) + tên đệm (viết tắt) + @ + tên miền (vss.gov.vn) hoặc tên người dùng (không dấu) + họ (viết tắt) + tên đệm (viết tắt) + @ + tên tỉnh (không dấu, viết liền).tên miền (vss.gov.vn). Trường hợp tài khoản đã tồn tại trong hệ thống thì bổ sung chỉ số (1, 2...) sau phần tên tài khoản (trước ký tự @). Trường hợp đặc biệt phải báo cáo và thực hiện theo sự chỉ đạo của BHXH Việt Nam.

b) Tài khoản hệ thống SSO sử dụng để truy cập phần mềm nghiệp vụ, phần mềm nội bộ và được tích hợp với hộp thư điện tử công vụ của Ngành.

c) Tài khoản cấp phát cho người dùng phải thực hiện theo quy trình và được sự phê duyệt của Giám đốc BHXH tỉnh. Người dùng thực hiện đăng nhập để thay đổi mật khẩu ngay khi được cấp tài khoản.

d) Sau 5 lần không đăng nhập thành công, tài khoản sẽ bị khóa, phải liên hệ Quản trị viên để mở khóa.

đ) Thường xuyên kiểm tra, đánh giá việc sử dụng tài khoản của cá nhân, tổ chức trong công việc. Hằng quý thống kê danh sách cá nhân, tổ chức đang sử dụng tài khoản gửi về Trung tâm CNTT để tổng hợp, rà soát.

Điều 6. Hệ thống mạng nội bộ

1. Hệ thống mạng LAN tại BHXH Việt Nam, BHXH tỉnh, BHXH huyện phải đảm bảo hiệu năng cho các ứng dụng, khả năng sẵn sàng và có các giải pháp để đảm bảo an toàn hệ thống.

2. Hệ thống mạng LAN phải bảo đảm:

a) Diện tích chỗ làm việc từ 7-10m² có tối thiểu một nút mạng ($\geq 1\text{Gbps}$) cho một người dùng, mỗi phòng làm việc có tối thiểu 01 nút mạng cho máy in. Số lượng nút mạng (không kể số nút mạng cho máy in và các thiết bị mạng khác) trong mỗi phòng bảo đảm dự phòng 10% tổng số người dùng (tối thiểu 01 nút mạng dự phòng) tại thời điểm thiết kế. Các nút mạng phải được lọc qua mô đun chống sét lan truyền theo tiêu chuẩn.

b) Hệ thống mạng hoạt động liên tục, nhanh, ổn định và an toàn, đáp ứng được yêu cầu về thông lượng cho các ứng dụng nghiệp vụ, hệ thống.

c) Có các giải pháp kiểm soát việc truy cập mạng bảo đảm các quy định về ATTT.

d) Tuân thủ các tiêu chuẩn về bấm dây, dán nhãn, chuẩn cáp mạng, cách thức đi dây, đấu nối, phân bổ nút mạng. Dây mạng, dây điện không chồng chéo lên nhau, và phải được bảo vệ khỏi sự phá hoại hoặc can thiệp trái phép. Hạn chế đi dây mạng xuyên qua những khu vực công cộng.

đ) Việc thiết kế lắp đặt phải bảo đảm tính thẩm mỹ, kinh tế, khả năng mở rộng, thuận tiện trong quản lý, sử dụng và khắc phục sự cố.

3. Hệ thống tủ mạng, dây mạng phải được định kỳ bảo trì, tối thiểu một lần trong 6 tháng.

4. Khi lập dự toán xây dựng trụ sở mới của các đơn vị phải bao gồm kinh phí cho việc thiết kế, thi công mạng LAN.

5. Bộ phận CNTT có trách nhiệm xây dựng yêu cầu kỹ thuật mạng LAN làm cơ sở thuê đơn vị tư vấn, thi công thực hiện.

6. Hồ sơ thiết kế kỹ thuật mạng của các đơn vị phải bao gồm: tài liệu khảo sát và phân tích hiện trạng, tài liệu thiết kế chi tiết. Nội dung tài liệu thiết kế chi tiết gồm: mô tả cách thiết kế; dự trù vật tư thiết bị; bản vẽ sơ đồ thiết kế; danh sách nút mạng phân bổ theo phòng; hồ sơ chi tiết của các nút mạng; mô tả phương án thi công.

7. Hồ sơ thiết kế mạng LAN của các đơn vị phải được phê duyệt của cấp có thẩm quyền sau khi có kết quả thẩm định thiết kế kỹ thuật của Trung tâm CNTT.

8. Thời hạn phê duyệt hồ sơ thiết kế mạng LAN của các đơn vị là 10 ngày làm việc kể từ khi nhận được đầy đủ Hồ sơ thiết kế mạng.

9. Bộ phận CNTT có trách nhiệm phối hợp giám sát việc thi công và nghiệm thu kỹ thuật mạng LAN bảo đảm tuân thủ thiết kế đã được phê duyệt.

10. Bộ phận CNTT có trách nhiệm lưu trữ 01 bộ hồ sơ thiết kế mạng, hồ sơ hoàn công, nghiệm thu mạng LAN.

Điều 7. Hệ thống phòng chống mã độc

1. Duy trì, vận hành hệ thống phòng chống mã độc giảm thiểu tối đa tác hại của việc lây lan, tấn công của các loại mã độc và ngăn chặn kịp thời sự bùng nổ mã độc trong hệ thống mạng.

2. Tất cả các máy chủ, máy trạm tại các đơn vị trong toàn Ngành phải được cài đặt phần mềm phòng chống mã độc của Ngành trang bị. Đối với các thiết bị chưa được cập nhật phiên bản mới nhất thì không được kết nối vào mạng. Bộ phận CNTT có trách nhiệm cài đặt, cập nhật phiên bản mới của phần mềm phòng chống mã độc cho toàn bộ người dùng trong cơ quan.

3. Phần mềm phòng chống mã độc phải luôn được cập nhật kịp thời các bản vá, các mẫu mã độc mới và phải được đặt ở chế độ quét thường xuyên, quét khi có kết nối với các thiết bị ngoại vi (usb, ổ cứng cắm ngoài,...).

4. Những máy tính được phát hiện có mã độc phải được tách khỏi mạng và kịp thời xử lý tránh lây nhiễm sang các máy tính khác.

5. BHXH Việt Nam quản lý tập trung và áp dụng các chính sách của hệ thống phòng chống mã độc trong toàn Ngành.

6. Hằng năm, Bộ phận CNTT tổ chức bồi dưỡng, hướng dẫn người dùng phòng chống và xử lý các sự cố liên quan tới mã độc.

Điều 8. An toàn phòng máy chủ

1. Phòng máy chủ phải được bố trí riêng, đặt gần Bộ phận CNTT và không đặt ở tầng một hoặc tầng cao nhất của tòa nhà. Chỉ thiết kế một cửa ra/vào và không có cửa sổ.

2. Có nội quy sử dụng và các biện pháp kỹ thuật, hành chính bảo vệ, kiểm soát ra/vào, ngăn chặn tiếp cận trái phép trang thiết bị, đường truyền mạng.

3. Chỉ được đặt các thiết bị đang hoạt động phục vụ vận hành hệ thống, tuyệt đối không đặt thiết bị khác: thiết bị hỏng, thiết bị chờ thanh lý, chờ hủy, tài liệu, vật tư, vật dụng dễ cháy nổ.

4. Bảo đảm vệ sinh công nghiệp: Môi trường khô ráo, sạch sẽ, không ẩm, không thấm nước, trang thiết bị lắp đặt trên tủ kỹ thuật, không để ánh nắng chiếu rọi trực tiếp. Độ ẩm, nhiệt độ đạt tiêu chuẩn quy định cho các thiết bị.

5. Phòng máy chủ tại BHXH tỉnh, các đơn vị trực thuộc BHXH Việt Nam phải bảo đảm từ 20m² trở lên và trang bị tối thiểu các thành phần sau:

a) Hệ thống phòng cháy, chữa cháy: Báo động bằng đèn còi, có khả năng phát hiện khói ở nồng độ tiêu chuẩn, không bị ảnh hưởng do nhiễu, không bị tê liệt một phần hay toàn bộ do cháy gây ra trước khi phát hiện cháy.

b) Hệ thống điện

- Nguồn điện độc lập với đường điện của tòa nhà từ máy biến áp; cung cấp đủ nguồn cho các thiết bị, tự động ngắt nguồn cấp đầu vào khi có sự cố.

- Nguồn điện dự phòng kết nối đến máy phát điện của tòa nhà bảo đảm cho hệ thống hoạt động trong thời gian nguồn điện chính gặp sự cố.

c) Hệ thống lưu điện: Cung cấp nguồn ra ổn định cho các thiết bị trong phòng máy chủ và các thiết bị mạng đặt phân tán trong tòa nhà.

d) Hệ thống tủ kỹ thuật: Loại tủ Rack, tiêu chuẩn 42U-19 inch, có máng cáp phía trên tủ Rack để bảo đảm an toàn cho hệ thống cáp mạng và thuận lợi trong việc xử lý sự cố.

đ) Hệ thống chống sét

- Dây mạng phải được nối qua thiết bị chống sét.

- Thiết bị chống sét, các trang thiết bị phải được nối tiếp đất.

- Dây nối và hồ tiếp đất phải được khảo sát và bố trí hợp lý, bảo đảm an toàn.

e) Hệ thống điều hòa làm mát

- Có hệ thống điều hòa làm mát riêng, không sử dụng chung với hệ thống điều hòa của tòa nhà, có khả năng tự khởi động sau khi đóng điện, có hệ thống dự phòng.

- Bảo đảm nhiệt độ từ 22oC đến 24oC, độ ẩm trung bình 40% đến 55%.

g) Hệ thống camera giám sát và kiểm soát ra/vào

- Giám sát 24/7, theo dõi được từ phòng Lãnh đạo BHXH tỉnh, Bộ phận CNTT, bộ phận bảo vệ.

- Ghi hình và lưu 7 ngày ở chế độ phát hiện chuyển động.

6. Phòng máy chủ tại BHXH huyện phải bảo đảm từ 7m² trở lên và trang bị tối thiểu các thành phần:

- Bình phòng cháy, chữa cháy.
 - Đường điện cấp độc lập với tòa nhà.
 - Điều hòa làm mát bảo đảm nhiệt độ từ 22oC đến 24oC.
 - Hệ thống chống sét và tiếp đất.
 - Tủ Rack tiêu chuẩn 27U-19 inch.
 - Hệ thống lưu điện.
 - Hệ thống camera giám sát và kiểm soát tại vị trí tủ Rack;
7. Các hệ thống phải được định kỳ bảo trì, tối thiểu 6 tháng một lần.

Điều 9. Quản lý thiết bị công nghệ thông tin

1. Bộ phận CNTT cập nhật tình hình sử dụng thiết bị CNTT trên phần mềm quản lý thiết bị CNTT theo quy chế của BHXH Việt Nam ban hành.
2. Thiết bị CNTT phải đặt tên và dán nhãn. Nhãn thiết bị phải bao gồm các nội dung: mã thiết bị, tên thiết bị, tên người dùng được giao quản lý và sử dụng, tên phòng. Mã thiết bị phải được quản lý trên phần mềm quản lý thiết bị CNTT.
3. Thiết bị CNTT dùng chung phải được bàn giao cho lãnh đạo phòng, BHXH huyện. Lãnh đạo phòng, BHXH huyện có trách nhiệm quản lý theo dõi việc sử dụng thiết bị CNTT dùng chung tại đơn vị.
4. Các đơn vị đăng ký nhu cầu mua sắm trang thiết bị CNTT hằng năm theo quy định tiêu chuẩn định mức trên phần mềm quản lý thiết bị CNTT. BHXH Việt Nam phê duyệt, tổ chức mua sắm và bàn giao cho các đơn vị đưa vào sử dụng.
5. Thiết bị hỏng còn bảo hành, các đơn vị yêu cầu nhà cung cấp thực hiện chế độ bảo hành. Thiết bị hỏng đã hết bảo hành, các đơn vị thực hiện phương án sửa chữa.
6. Trường hợp thiết bị hỏng là thiết bị quan trọng (máy chủ, thiết bị mạng) các đơn vị phải báo cáo ngay BHXH Việt Nam để có biện pháp khắc phục kịp thời bảo đảm duy trì hoạt động của hệ thống.
7. Thiết bị CNTT phải được bảo trì định kỳ, tối thiểu một lần trong năm.

Điều 10. Quản lý kết nối, trao đổi dữ liệu với đơn vị bên ngoài

1. Việc kết nối, trao đổi dữ liệu với bên ngoài phải được BHXH Việt Nam phê duyệt và phải đáp ứng các tiêu chuẩn về kết nối mạng, địa chỉ, cách thức truy cập, định dạng dữ liệu.
2. Việc kết nối không được ảnh hưởng đến an ninh và hoạt động của hệ thống mạng của ngành, có các biện pháp phòng chống xâm nhập bất hợp pháp từ bên ngoài.

Điều 11. Quản lý kết nối Internet

1. Hạ tầng kết nối Internet phải có các giải pháp bảo mật như thiết bị tường lửa, phát hiện xâm nhập, phòng chống mã độc đảm bảo hệ thống không bị tấn công xâm nhập, lây lan mã độc từ bên ngoài.
2. Người dùng tại các đơn vị trực thuộc BHXH Việt Nam truy cập Internet thông qua điểm quản lý tập trung Internet tại đơn vị. Người dùng tại BHXH tỉnh, BHXH huyện truy cập Internet thông qua điểm quản lý tập trung Internet tại BHXH tỉnh.

3. Bộ phận CNTT chịu trách nhiệm giám sát, kiểm tra nội dung và băng thông truy cập, ngăn chặn, đề xuất xử lý các hành vi vi phạm.

Điều 12. Quản lý dịch vụ truy cập mạng riêng ảo

1. Cá nhân có nhu cầu kết nối mạng VPN phải đăng ký và cam kết mục đích sử dụng, bảo mật thông tin tài khoản, bảo đảm ATTT bằng văn bản. Thời gian thực hiện cung cấp dịch vụ VPN tối thiểu 01 ngày làm việc sau khi tiếp nhận đầy đủ hồ sơ đăng ký.

2. CCVC được cấp quyền sử dụng dịch vụ VPN có trách nhiệm:

a) Bảo đảm an toàn máy tính kết nối VPN theo quy định.

b) Bảo đảm an toàn, bảo mật thông tin đối tài khoản truy cập VPN.

c) Trường hợp không còn nhu cầu sử dụng hoặc nghi ngờ tài khoản có nguy cơ bị lộ lọt cần thông báo Quản trị viên của đơn vị để khóa tài khoản kịp thời.

3. Lãnh đạo phòng, BHHX huyện xác nhận việc sử dụng tài khoản VPN của các cá nhân đăng ký trình thủ trưởng đơn vị phê duyệt.

Điều 13. Quản lý bản quyền phần mềm

1. Các phần mềm, ứng dụng sử dụng trong các đơn vị phải có bản quyền sử dụng theo đúng quy định của pháp luật và của BHHX Việt Nam.

2. Chỉ được cài đặt và sử dụng các phần mềm mà BHHX Việt Nam đã trang bị hoặc có quyết định triển khai, các đơn vị tự trang bị phần mềm bản quyền phải có văn bản phê duyệt của BHHX Việt Nam, các phần mềm mã nguồn mở, phần mềm miễn phí phải tuân theo quy định của BHHX Việt Nam.

3. Bộ phận CNTT tổ chức quản lý, theo dõi sử dụng các bản quyền phần mềm tại đơn vị.

4. Không phát tán, chia sẻ phần mềm có bản quyền của Ngành ra bên ngoài. Bộ phận CNTT tiếp nhận và chịu trách nhiệm quản lý về kỹ thuật các phần mềm có bản quyền của Ngành tại đơn vị.

Điều 14. Quản lý hồ sơ hệ thống

1. Danh sách các loại hồ sơ lưu trữ:

a) Quy định về quản lý, triển khai, vận hành hệ thống.

b) Quy trình quản lý và vận hành các hệ thống quản lý người dùng, thư điện tử, sao lưu dữ liệu, phòng chống mã độc và đĩa cài đặt.

c) Hồ sơ khảo sát, thiết kế và thuyết minh kỹ thuật của mạng; sơ đồ thiết kế mạng logic, sơ đồ đi dây mạng vật lý, thông số các thiết bị mạng.

d) Bảng thống kê danh sách các nhóm, người dùng trong hệ thống AD, danh sách người dùng tại đơn vị, phiếu đăng ký người dùng, phiếu đề nghị thay đổi thông tin của người dùng.

đ) Bảng thống kê danh sách thiết bị tại đơn vị. Danh sách các thiết bị hỏng, sửa chữa, bảo hành. Biên bản bàn giao thiết bị cho người dùng. Hồ sơ, tài liệu triển khai hệ thống của BHHX Việt Nam.

e) Danh sách mật khẩu quản trị hệ thống.

- g) Tài liệu, biên bản kiểm tra, đánh giá của đơn vị.
- h) Báo cáo quản trị hệ thống, nhật ký quản trị, hỗ trợ, xử lý các sự cố, thay đổi trong hệ thống, nhật ký vào/ra phòng máy chủ, dữ liệu ghi hình hoạt động tại phòng máy chủ.

2. Hồ sơ của hệ thống CNTT được lưu bằng văn bản, tập tin bản mềm trên máy tính đã được mã hóa, đặt mật khẩu và phải được cập nhật khi có sự thay đổi.

Điều 15. Hỗ trợ và xử lý sự cố về hệ thống

1. Bộ phận CNTT tổ chức một đầu mối hỗ trợ (số điện thoại, hộp thư điện tử) tiếp nhận yêu cầu hỗ trợ người dùng tại đơn vị; thông báo cho các đơn vị trực thuộc các thông tin từ BHXH Việt Nam hoặc các kế hoạch nhiệm vụ ứng dụng CNTT, ATTT.

2. Khi phát hiện có sự cố, Bộ phận CNTT thực hiện các biện pháp cô lập và xác định nguyên nhân xảy ra sự cố theo nguyên tắc hạn chế tối đa ảnh hưởng tới hoạt động của hệ thống CNTT; đồng thời phải thông báo cho người dùng và các bộ phận liên quan về tình hình sự cố. Sau khi khắc phục sự cố, Bộ phận CNTT thông báo cho các bộ phận liên quan.

3. Tùy thuộc vào mức độ ảnh hưởng của các sự cố, Bộ phận CNTT đánh giá và phân loại theo 3 mức: sự cố đặc biệt nghiêm trọng, sự cố nghiêm trọng, sự cố thông thường.

4. Đối với các sự cố thông thường (các sự cố liên quan đến máy tính xách tay, máy trạm, máy in, các sự cố không gây ảnh hưởng đến hoạt động của nội bộ đơn vị và người tham gia BHXH, BHYT, BHTN), Bộ phận CNTT nhanh chóng xử lý sự cố. Trường hợp không xử lý được thông báo với đầu mối hỗ trợ cấp trên để phối hợp giải quyết.

5. Đối với các sự cố nghiêm trọng (các sự cố liên quan đến thiết bị mạng, thiết bị bảo mật, máy chủ, đường truyền dữ liệu, cơ sở dữ liệu, các sự cố gây ảnh hưởng trực tiếp và làm ngưng trệ đến toàn bộ hoạt động của đơn vị); sự cố đặc biệt nghiêm trọng (các sự cố liên quan đến thiết bị mạng, thiết bị bảo mật, máy chủ, đường truyền dữ liệu, cơ sở dữ liệu, các sự cố gây ảnh hưởng trực tiếp và làm ngưng trệ đến toàn bộ hoạt động của Ngành) ngay sau khi phát hiện sự cố, Bộ phận CNTT cần đánh giá ảnh hưởng của sự cố và báo cáo về BHXH Việt Nam để được hướng dẫn xử lý.

6. Bộ phận CNTT tại Trung ương (Trung tâm CNTT) là đầu mối hỗ trợ cao nhất có trách nhiệm hỗ trợ xử lý sự cố cho các đơn vị trong toàn Ngành. Bộ phận CNTT tại BHXH tỉnh có trách nhiệm hỗ trợ BHXH huyện khắc phục các sự cố. Bộ phận CNTT tại BHXH tỉnh phải báo cáo Trung tâm CNTT, Bộ phận CNTT tại BHXH huyện phải báo cáo BHXH tỉnh về các sự cố tại đơn vị.

7. Yêu cầu đối với việc xử lý sự cố cần tuân thủ các nguyên tắc

- a) Các dữ liệu quan trọng phải được sao lưu trước khi thực hiện xử lý sự cố.
- b) Bảo đảm tuyệt đối an toàn cho người và thiết bị hệ thống.
- c) Ghi nhật ký sự cố kỹ thuật phát sinh tại chỗ.
- d) Thông báo thời gian dự kiến khắc phục xong sự cố.

Điều 16. Kiểm tra bảo trì hệ thống hạ tầng thông tin

1. Bộ phận CNTT tổ chức kiểm tra việc tuân thủ các quy định về quản lý, triển khai, vận hành, khai thác sử dụng hệ thống hạ tầng thông tin tại đơn vị theo các quy định tại Quy chế này tối thiểu mỗi năm một lần.

2. Hằng năm, Bộ phận CNTT xây dựng kế hoạch tổ chức kiểm tra công tác quản lý, triển khai, vận hành, khai thác sử dụng hệ thống hạ tầng thông tin tại các đơn vị trực thuộc.

3. Các nội dung kiểm tra:

a) Việc bảo đảm điều kiện môi trường cho thiết bị, nguồn cấp, thiết bị vận hành an toàn, sạch sẽ.

b) Tình hình sử dụng thiết bị CNTT, sử dụng ứng dụng hệ thống của ngành.

c) Hoạt động của hệ thống máy chủ, máy trạm, các dịch vụ (Cập nhật các bản vá, bản sửa lỗi, dung lượng ổ cứng, hiệu năng sử dụng...).

d) Tình hình phòng chống mã độc, đánh giá hiệu quả (khả năng phát hiện và diệt) của các phần mềm phòng chống mã độc.

đ) Kiểm tra công tác sao lưu, lưu trữ, phục hồi dữ liệu.

e) Công tác cập nhật, lưu trữ hồ sơ: ghi nhật ký, cập nhật thống kê, tổng hợp thiết bị, báo cáo,...

g) Việc tuân thủ các quy định khác nêu tại quy chế này.

4. Các vấn đề phát hiện sau khi kiểm tra phải được tổng hợp, đánh giá phân tích mức độ ảnh hưởng với hoạt động của hệ thống và lập kế hoạch khắc phục xử lý.

5. Bộ phận CNTT thực hiện bảo trì thường xuyên, bảo đảm hệ thống CNTT hoạt động liên tục, ổn định và an toàn.

6. Toàn bộ quá trình bảo trì phải được ghi sổ nhật ký, cập nhật các thay đổi của hệ thống hạ tầng thông tin trong những lần sửa chữa, nâng cấp, thay thế hoặc lắp đặt mới.

7. Các thiết bị CNTT phải được thường xuyên theo dõi và xử lý kịp thời các hư hỏng, biểu hiện mất ổn định hoặc quá tải. Cập nhật kịp thời các bản vá lỗi, lỗ hổng về an ninh.

8. Hằng năm trước ngày 5/12, Các đơn vị báo cáo BHXH Việt Nam bằng văn bản toàn bộ tình hình quản lý, triển khai, vận hành, khai thác sử dụng hệ thống hạ tầng thông tin theo quy định của ngành.

Chương III

CÔNG TÁC TRIỂN KHAI, VẬN HÀNH

Điều 17. Công tác triển khai, vận hành hạ tầng mạng

1. Kiểm tra theo dõi hoạt động các thiết bị mạng, hạ tầng truyền thông tại các đơn vị.

2. Lắp đặt, bổ sung các thiết bị mạng, nút mạng đáp ứng nhu cầu phát sinh tại các đơn vị.

3. Lưu trữ và cập nhật các thông tin mới, thông tin thay đổi vào hồ sơ quản trị mạng.

4. Định kỳ thay đổi mật khẩu quản trị hệ thống mạng theo khoản 4 Điều 4 Quy chế này.

5. Triển khai bảo trì, đánh giá hiện trạng hệ thống mạng tại đơn vị để lập kế hoạch nâng cấp hệ thống mạng hằng năm.

6. Yêu cầu với Quản trị viên tại các đơn vị

a) Hằng ngày:

- Kiểm tra tình trạng của các thiết bị mạng (bao gồm thiết bị điều khiển mạng LAN không dây (wireless LAN controller), điểm truy cập (access point)) vào đầu giờ làm việc buổi sáng.

- Theo dõi hoạt động của các thiết bị mạng, hạ tầng truyền thông của đơn vị.

- Theo dõi tình trạng hoạt động của các điểm truy cập, kiểm tra đồng bộ cơ sở dữ liệu giữa các máy chủ xác thực, số lượng người dùng đang kết nối hệ thống mạng không dây.

- Tiếp nhận các yêu cầu hỗ trợ hạ tầng mạng từ người dùng và đầu mối hỗ trợ.

- Hỗ trợ hoặc xử lý sự cố về mạng, trong trường hợp không tự khắc phục được phải báo cáo Lãnh đạo đơn vị và đầu mối hỗ trợ cấp trên để phối hợp với các đơn vị liên quan xử lý.

- Ghi nhật ký vận hành.

b) Hằng tuần:

- Kiểm tra chất lượng hạ tầng truyền thông.

- Kiểm tra kết nối của các thiết bị trong hệ thống mạng.

- Kiểm tra tình trạng và môi trường hoạt động của các thiết bị, hệ thống mạng đặt tại phòng máy chủ và tại các tầng của tòa nhà.

- Kiểm tra tình trạng dây mạng, nguồn cấp cho thiết bị.

c) Hằng tháng: Báo cáo Lãnh đạo đơn vị và Trung tâm CNTT về tình trạng hoạt động của hạ tầng mạng; các vấn đề cần khắc phục, chỉnh sửa hoặc các đề xuất, kiến nghị.

Điều 18. Công tác triển khai, vận hành hệ thống phòng chống mã độc

1. Tổ chức cài đặt phần mềm phòng chống mã độc của ngành cho toàn bộ máy chủ, máy trạm, máy tính xách tay tại đơn vị.

2. Cập nhật các mẫu mã độc mới và bản vá của phần mềm phòng chống mã độc của ngành cho các máy chủ, máy trạm, máy tính xách tay.

3. Cập nhật thường xuyên cơ sở dữ liệu về mẫu mã độc mới và bản vá cho các phần mềm quản trị mã độc.

4. Tiếp nhận và thực hiện các yêu cầu của BHXH Việt Nam về việc phòng chống mã độc.

5. Định kỳ thay đổi mật khẩu quản trị hệ thống phòng chống mã độc theo khoản 4 Điều 4 Quy chế này.

6. Hướng dẫn, kiểm tra, hỗ trợ, đơn đốc đơn vị trực thuộc cập nhật mẫu mã độc cho máy trạm.

7. Triển khai rà soát, kiểm tra, nâng cấp hệ thống phòng chống mã độc hằng năm.

8. Yêu cầu đối với Quản trị viên tại các đơn vị

a) Hằng ngày:

- Kiểm tra hoạt động các dịch vụ của hệ thống phòng chống mã độc. Cập nhật mẫu mã độc và bản vá mới nhất cho các phần mềm phòng chống mã độc của ngành. Kiểm tra tình trạng kết nối các phần mềm phòng chống mã độc trên máy chủ, máy trạm, máy tính xách tay đến máy chủ quản trị mã độc và xử lý các trường hợp không kết nối được. Kiểm tra tình trạng nhiễm mã độc, mã nguồn độc hại của các máy chủ, máy trạm, máy tính xách tay cài phần mềm phòng chống mã độc vào đầu giờ làm việc mỗi buổi sáng.

- Khắc phục và xử lý các trường hợp nhiễm mã độc. Đối với trường hợp nặng thì cách ly ra khỏi mạng.

- Tiếp nhận các yêu cầu hỗ trợ liên quan đến phòng chống mã độc từ người dùng và đầu mối hỗ trợ.

- Hỗ trợ hoặc xử lý sự cố về mã độc, trong trường hợp không tự xử lý được phải báo cáo BHXH Việt Nam và phối hợp với các đơn vị liên quan xử lý.

- Ghi nhật ký vận hành.

b) Hằng tuần:

- Kiểm tra kết quả quét mã độc đối với toàn bộ máy trạm cài phần mềm phòng chống mã độc.

- Xóa các tập tin bị nhiễm mã độc trong thư mục lưu giữ.

- Kiểm tra lịch quét mã độc trên các máy chủ, máy trạm.

c) Hằng tháng: Báo cáo Lãnh đạo đơn vị và Trung tâm CNTT về tình trạng mã độc, phần mềm độc hại của các máy chủ, máy trạm, máy tính xách tay; các vấn đề cần khắc phục, chỉnh sửa hoặc các đề xuất, kiến nghị.

Điều 19. Công tác triển khai, vận hành hệ thống an toàn thông tin mạng

1. Thiết lập đầy đủ các chế độ kiểm soát ATTT mạng. Sử dụng các công cụ được trang bị, dò tìm và phát hiện kịp thời các điểm yếu và các truy nhập bất hợp pháp vào hệ thống mạng. Thường xuyên xem xét, phát hiện những kết nối, trang thiết bị, phần mềm cài đặt bất hợp pháp vào mạng.

2. Hướng dẫn, hỗ trợ người dùng bảo vệ tài khoản, tài nguyên trên mạng và giải quyết kịp thời những sự cố truy nhập mạng.

3. Kiểm tra và ngắt kết nối ra khỏi mạng những máy tính của người dùng không tuân thủ các quy định về an ninh mạng.

4. Thường xuyên thực hiện cập nhật các bản sửa lỗi và bản vá cho hệ điều hành trên các máy chủ, máy trạm theo yêu cầu của BHXH Việt Nam.

5. Tạo các chính sách ATTT mạng (Policy), cấu hình dải địa chỉ cho từng vùng trong/ngoài (Internal, External) và thực hiện tất các dịch vụ không sử dụng theo yêu cầu của BHXH Việt Nam.

6. Phân quyền cho người dùng theo các trang Web được phép truy cập hoặc theo thời gian sử dụng Internet.

7. Định kỳ thay đổi mật khẩu quản trị ATTT mạng theo khoản 4 Điều 4 Quy chế này.

8. Triển khai rà soát, kiểm tra, nâng cấp hệ thống ATTT mạng hằng năm.

9. Yêu cầu đối với Quản trị viên

a) Hằng ngày:

- Kiểm tra hoạt động của các hệ thống ATTT mạng: các thiết bị tường lửa; thiết bị kiểm soát truy cập mạng vào đầu giờ làm việc buổi sáng.

- Theo dõi các kết nối ra ngoài Internet, nội dung các trang Web truy cập.

- Theo dõi thông tin truy cập hệ thống (log) để kịp thời ngăn chặn các truy cập bất hợp pháp.

- Tiếp nhận các yêu cầu hỗ trợ liên quan đến sự cố ATTT từ người dùng và đầu mối hỗ trợ.

- Hỗ trợ hoặc xử lý sự cố về ATTT, trong trường hợp không tự xử lý được phải báo cáo BHXH Việt Nam và phối hợp với các đơn vị liên quan xử lý.

- Ghi nhật ký quản trị.

b) Hằng tuần:

- Kiểm tra, cập nhật các bản vá sửa lỗi cho các máy chủ, máy trạm.

- Kiểm tra các cảnh báo từ hệ thống phát hiện các mối nguy hại trong hệ thống.

- Kiểm tra các dải địa chỉ trong các vùng được tạo và các chính sách ATTT đối với các dải địa chỉ.

c) Hằng tháng: Báo cáo Lãnh đạo đơn vị và Trung tâm CNTT về tình hình bảo đảm ATTT mạng; các vấn đề cần khắc phục, chỉnh sửa hoặc các đề xuất, kiến nghị.

Điều 20. Công tác triển khai, vận hành phòng máy chủ

1. Theo dõi môi trường hoạt động phòng máy chủ 24/7.

2. Định kỳ 6 tháng/lần bảo trì các thiết bị bảo đảm an toàn phòng máy chủ.

3. Cấu hình các thông số hệ thống lưu điện, các cảm biến (Sensor).

4. Yêu cầu đối với Quản trị viên

a) Hằng ngày:

- Thực hiện theo dõi hoạt động hệ thống điện cấp cho phòng máy chủ (hệ thống tủ điện trung tâm, hệ thống lưu điện); hệ thống điều hòa không khí, hệ thống camera

giám sát, hệ thống phòng cháy chữa cháy, hệ thống chống sét, tiếp đất đường điện, đường mạng, hệ thống làm mát cho tủ máy chủ, thiết bị mạng (Rack).

- Kiểm soát thiết bị và con người vào ra phòng máy chủ.
- Theo dõi các log và các thư điện tử cảnh báo của hệ thống an toàn phòng máy chủ.
- Ghi nhật ký phòng máy chủ, nhật ký ra vào phòng máy chủ thông qua hệ thống camera giám sát và nhật ký vận hành.

b) Hằng tuần:

- Thực hiện kiểm tra hệ thống điện cấp cho phòng máy chủ (hệ thống tủ điện trung tâm, hệ thống lưu điện); hệ thống điều hòa không khí, hệ thống camera giám sát, hệ thống phòng cháy, chữa cháy; độ ẩm, cấp điện, các đầu đầu nối, cửa ra vào, cửa sổ, khóa cửa; hệ thống chống sét, tiếp đất đường điện, đường mạng; bảng hướng dẫn cho từng loại thiết bị, vị trí của các thiết bị trong phòng máy chủ; hệ thống làm mát cho tủ máy chủ, thiết bị mạng.

c) Hằng tháng:

- Thực hiện vệ sinh môi trường phòng máy chủ và các thiết bị trong phòng máy chủ.
- Kiểm tra các thiết bị máy chủ, thiết bị mạng, bảo mật, lưu trữ trong phòng máy chủ.
- Báo cáo Lãnh đạo đơn vị về tình hình hoạt động của phòng máy chủ.

Điều 21. Công tác triển khai, vận hành thiết bị công nghệ thông tin

1. Kiểm tra, đánh giá hiệu quả khai thác sử dụng thiết bị CNTT báo cáo Lãnh đạo đơn vị và BHXH Việt Nam (Trung tâm CNTT).
2. Tổ chức tiếp nhận, cài đặt, lắp đặt thiết bị tại đơn vị và bàn giao bằng văn bản cho người dùng.
3. Thu hồi thiết bị của người dùng không sử dụng và nhập kho.
4. Tiếp nhận thiết bị hỏng từ người dùng, gửi bảo hành, theo dõi đơn đốc thời gian bảo hành, bàn giao cho các bộ phận liên quan sau khi bảo hành xong. Đánh giá chất lượng bảo hành của các đơn vị cung cấp thiết bị.
5. Theo dõi các trường hợp hỏng hóc và quá trình sửa chữa khắc phục. Kiểm tra thiết bị sau bảo hành.
6. Xóa toàn bộ dữ liệu nghiệp vụ và dữ liệu người dùng trên thiết bị máy chủ, máy trạm, lưu trữ trước khi điều chuyển thiết bị từ đơn vị này sang đơn vị khác hoặc khi thanh lý tài sản.

Chương IV

KHAI THÁC, SỬ DỤNG HỆ THỐNG HẠ TẦNG THÔNG TIN

Điều 22. Khai thác, sử dụng thiết bị công nghệ thông tin

1. Người dùng tại các đơn vị có trách nhiệm tiếp nhận và quản lý các thiết bị CNTT được cấp (máy tính để bàn, máy tính xách tay, máy tính bảng, bàn phím, chuột, ổ DVD, thiết bị lưu điện, máy in,...). Lãnh đạo phòng, BHXH huyện tiếp nhận các thiết bị CNTT dùng chung của đơn vị và bàn giao cho một viên chức chịu trách nhiệm quản lý.

2. Người dùng mang thiết bị CNTT (đặc biệt là máy tính xách tay) ra ngoài cơ quan chỉ sử dụng phục vụ công việc của Ngành, không được làm việc riêng của cá nhân; không tự ý tháo lắp, thay đổi các thành phần của thiết bị CNTT được cơ quan trang bị.

3. Người dùng sử dụng máy tính xách tay đi công tác, hội họp, thanh tra, kiểm tra phải đăng ký thời gian sử dụng và được sự đồng ý của lãnh đạo phòng, BHXH huyện, đồng thời phải tự lưu, bảo quản dữ liệu của mình trước khi bàn giao lại cho người khác sử dụng.

4. Người dùng phải bàn giao lại thiết bị CNTT cho đơn vị cũ khi chuyển vị trí công tác mới, nghỉ hưu. Đối với máy trạm/máy tính bảng được cấp cho cá nhân thực hiện điều chuyển theo vị trí công tác mới trong cùng đơn vị trực thuộc BHXH Việt Nam, BHXH tỉnh và phải bảo đảm tiêu chuẩn, định mức của BHXH Việt Nam.

5. Người dùng phải chịu trách nhiệm bồi thường trong trường hợp thiết bị CNTT bị mất hoặc hỏng do lỗi của người dùng.

6. Máy tính phải được cài đặt và cấu hình các phần mềm theo quy định của BHXH Việt Nam và kết nối với hệ thống AD. Người dùng lưu dữ liệu vào ổ đĩa khác với ổ đĩa của hệ điều hành Windows.

7. Người dùng phải sử dụng tài khoản được cấp để đăng nhập vào máy tính. Không đăng nhập máy tính bằng tài khoản quản trị, ngoại trừ các Quản trị viên. Giữ bí mật về mật khẩu tài khoản cá nhân và định kỳ thay đổi mật khẩu theo khoản 4 Điều 4 Quy chế này. Bộ phận CNTT quản lý mật khẩu quản trị máy trạm, mật khẩu cấu hình phần cứng máy tính (BIOS), không cung cấp cho người dùng.

8. Thường xuyên quét mã độc trên máy tính kết nối vào mạng. Hằng tuần, người dùng được cấp máy tính xách tay phải kết nối vào mạng LAN để cập nhật cho phần mềm phòng chống mã độc. Kiểm tra và diệt mã độc trên các thiết bị ngoại vi, thiết bị có khả năng lưu trữ dữ liệu ngay khi cắm vào máy tính.

9. Sử dụng bộ phong chữ tiếng Việt Unicode (UTF-8) thống nhất trong Ngành BHXH Việt Nam. Không được phép cài đặt thêm ứng dụng ngoài danh sách ứng dụng triển khai của BHXH Việt Nam được cung cấp bộ cài đặt trên hệ thống của Ngành. Trường hợp đặc biệt phải được sự đồng ý của Bộ phận CNTT và Bộ phận CNTT có trách nhiệm cài đặt. Không tự ý gỡ bỏ các ứng dụng đã được BHXH Việt Nam và Bộ phận CNTT cài đặt sẵn. Không thay đổi tên máy trạm, thông số kỹ thuật mà Bộ phận CNTT đã cài đặt. Người dùng phải thoát khỏi hệ thống (logout) ngay khi rời khỏi vị trí làm việc. Phải tắt máy tính, hệ thống lưu điện và các thiết bị khác trước khi rời cơ quan.

10. Không cho người ngoài Ngành, cơ quan mượn hoặc sử dụng máy tính để tránh thất thoát, lộ lọt thông tin, dữ liệu.

11. Không cố ý sao chép, sửa đổi, phá hoại các tập tin và dữ liệu trên máy tính không thuộc phạm vi quản lý.

12. Không dò tìm mật khẩu của người khác.
13. Nghiêm cấm chơi các trò chơi điện tử trên hệ thống máy tính do Ngành trang bị.
14. Khi thiết bị CNTT bị hỏng hóc phải báo ngay cho đầu mối hỗ trợ để được xử lý.
15. Người dùng phải có ý thức giữ gìn, bảo quản cẩn thận các thiết bị CNTT; hằng tháng vệ sinh các thiết bị CNTT được cấp; không để các vật dụng cá nhân lên máy tính.
16. Người dùng không mang thiết bị CNTT cá nhân bên ngoài kết nối trực tiếp vào mạng LAN của Ngành khi chưa đăng ký sử dụng với Bộ phận CNTT và bảo đảm an toàn tối thiểu cho thiết bị máy tính.

Điều 23. Khai thác, sử dụng mạng máy tính

1. Chỉ đọc tin tức trên mạng Internet ngoài giờ hành chính.
2. Có trách nhiệm bảo vệ hệ thống mạng (LAN, WAN, Internet, VPN, WiFi) của đơn vị, cảnh giác với những mặt trái của Internet. Chịu trách nhiệm trước pháp luật nếu bao che hoặc cho người khác sử dụng trang thiết bị, mật khẩu của mình để thực hiện các hành vi phạm pháp.
3. Chịu sự kiểm tra, giám sát của đơn vị và các cơ quan chức năng của Nhà nước đối với các thông tin gửi lên hệ thống mạng và chịu trách nhiệm về các thông tin đó.
4. Không truy cập vào những trang Web không lành mạnh gây ảnh hưởng đến an ninh, chính trị, xã hội.
5. Không gây cản trở, phá hoại hoạt động của mạng máy tính, làm ảnh hưởng đến các hệ thống thông tin khác, hoặc xâm phạm đến quyền lợi, danh dự của cá nhân khác.
6. Không sử dụng thiết bị truy cập Internet khác tại đơn vị. Không sử dụng các công cụ, phần mềm và các biện pháp kỹ thuật dưới mọi hình thức nhằm chiếm dụng băng thông đường truyền, gây tắc nghẽn mạng.
7. Không sử dụng các phần mềm điều khiển từ xa truy cập đến máy tính trong cơ quan ngoài giờ hành chính.

Chương V

TỔ CHỨC THỰC HIỆN

Điều 24. Trách nhiệm của các đơn vị trực thuộc Bảo hiểm xã hội Việt Nam, Bảo hiểm xã hội tỉnh và Bảo hiểm xã hội huyện

1. Thực hiện công tác quản lý, triển khai, vận hành hệ thống hạ tầng thông tin tại đơn vị bảo đảm hệ thống hoạt động an toàn theo Quy chế này.
2. Bố trí các nguồn lực cần thiết để thực hiện việc quản lý, triển khai, vận hành, giám sát, bảo đảm ATTT và xử lý các sự cố trong hoạt động ứng dụng CNTT.

3. Kiến nghị BHXH Việt Nam bồi dưỡng kiến thức CNTT, ATTT cho CCVC quản lý, triển khai, vận hành hệ thống hạ tầng thông tin đáp ứng yêu cầu thực hiện các hoạt động nghiệp vụ.

4. Chỉ đạo, đôn đốc, hỗ trợ, kiểm tra các đơn vị trực thuộc trong quá trình quản lý, triển khai, vận hành, khai thác, sử dụng hệ thống hạ tầng thông tin.

5. Tuân thủ và thực hiện các quy định về CNTT, ATTT và các quy định nêu trong Quy chế này.

Điều 25. Trách nhiệm của Trung tâm Công nghệ thông tin

1. Hướng dẫn, hỗ trợ các đơn vị triển khai, thực hiện các quy định trong Quy chế này.

2. Phối hợp các đơn vị liên quan tổ chức các khóa bồi dưỡng cập nhật kiến thức về CNTT cho viên chức CNTT tại các đơn vị phù hợp với yêu cầu công việc được phân công.

3. Hướng dẫn các biểu mẫu báo cáo theo Quy chế: nhật ký vận hành, báo cáo về tình trạng hoạt động của hạ tầng mạng, báo cáo quản lý thiết bị CNTT, báo cáo tình hình bảo đảm ATTT... tại các đơn vị.

4. Cung cấp bộ cài đặt trên hệ thống của Ngành các phần mềm ứng dụng văn phòng thường xuyên được sử dụng như trình duyệt Web, giải nén...

Điều 26. Tổ chức thực hiện

1. Thủ trưởng các đơn vị chịu trách nhiệm thi hành Quy chế này và có trách nhiệm quán triệt, chỉ đạo và giám sát CCVC thuộc đơn vị mình thực hiện nghiêm chỉnh các nội dung Quy chế này.

2. Đội Ứng cứu sự cố ATTT Ngành thực hiện ứng cứu sự cố của các hệ thống hạ tầng thông tin tại các đơn vị theo sự điều phối của BHXH Việt Nam.

3. Trong quá trình tổ chức thực hiện, nếu có khó khăn vướng mắc, các đơn vị cần phản ánh kịp thời về BHXH Việt Nam (qua Trung tâm CNTT) xem xét sửa đổi, bổ sung Quy chế cho phù hợp.

4. Đơn vị, CCVC tại các đơn vị vi phạm Quy chế này thì tùy theo tính chất, mức độ vi phạm bị xử lý kỷ luật hoặc các hình thức xử lý khác theo quy định của pháp luật và của BHXH Việt Nam./.