UBND TỈNH BẮC NINH
SỞ TÀI CHÍNH

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

Số: 156 /QĐ-STC

Bắc Ninh, ngày 22 tháng 9 năm 2023

QUYẾT ĐỊNH
Ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng Công nghệ thông tin của Sở Tài chính Bắc Ninh

GIÁM ĐỐC SỞ TÀI CHÍNH BẮC NINH

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 Luật An ninh mạng ngày 12/6/2018;

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

Căn cứ Nghị định số 142/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về ngăn chặn xung đột thông tin trên mạng;

Căn cứ Quyết định số 21/2019/QĐ-UBND ngày 22/10/2019 của UBND tỉnh về việc ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng Công nghệ thông tin của cơ quan Nhà nước trên địa bàn tỉnh Bắc Ninh;

Căn cứ Quyết định số 1484/QĐ-BTC ngày 27/7/2022 của Bộ Trưởng Bộ Tài chính về việc ban hành Kế hoạch chuyển đổi số của Bộ Tài chính đến năm 2025, định hướng đến năm 2030;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12/8/ 2022 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/72016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Quyết định số 07/2022/QĐ-UBND ngày 18/5/2022 của UBND tỉnh về việc ban hành Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Sở Tài chính tỉnh Bắc Ninh;

Căn cứ Quyết định số 195/QĐ-STC ngày 01/11/2022 của Giám đốc Sở Tài chính về việc phân công thực hiện chức năng, nhiệm vụ; chế độ trách nhiệm và mối quan hệ công tác giữa các phòng, đơn vị thuộc Sở Tài chính tỉnh Bắc Ninh;

Xét đề nghị của Chánh Văn phòng Sở,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng Công nghệ thông tin của Sở Tài chính

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

Điều 3. Chánh Văn phòng, Trưởng các phòng, đơn vị thuộc sở và toàn thể công chức, viên chức, người lao động thuộc Sở Tài chính; các cơ quan, đơn vị, cá nhân đến làm việc tại Sở Tài chính chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như điều 3 (t/h);
- UBND tỉnh (b/c);
- Sở TT&TT (b/c);
- Lãnh đạo Sở;
- Lưu: VT, VP.

GIÁM ĐỐC

Sở Tài chính
Tỉnh Bắc Ninh
22-09-2023 08:26:45 +07:00

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ TÀI CHÍNH
TỈNH BẮC NINH

Nguyễn Kim Thoại

UBND TỈNH BẮC NINH
SỞ TÀI CHÍNH

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

QUY CHẾ
Bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng Công nghệ thông tin của Sở Tài chính Bắc Ninh

(Kèm theo Quyết định số: /QĐ-STC ngày /9/2023 của Sở Tài chính)

Chương I
QUY ĐỊNH CHUNG

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

1. Phạm vi điều chỉnh.

Quy chế này quy định về bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của Sở Tài chính.

2. Đối tượng áp dụng.

Quy chế này được áp dụng đối với Văn phòng Sở, Thanh tra Sở, các phòng, đơn vị và trung tâm thuộc Sở (sau đây gọi tắt là các phòng làm việc); công chức, viên chức và người lao động (gọi tắt là cán bộ) thuộc Sở.

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

1. Mục tiêu bảo đảm an toàn thông tin.

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 hệ thống mạng LAN của Sở Tài chính.

2. Nguyên tắc.

a) Các phòng làm việc tại Sở Tài chính thuộc đối tượng áp dụng Quy chế này có trách nhiệm bảo đảm an toàn thông tin và hệ thống thông tin trong phạm vi xử lý công việc của mình theo quy định của pháp luật, hướng dẫn của cơ quan, đơn vị có thẩm quyền và các quy định tại Quy chế này.

b) Bảo đảm an toàn thông tin là yêu cầu bắt buộc, thường xuyên, liên tục, có tính xuyên suốt quá trình, đồng bộ từ khi thiết kế, xây dựng, vận hành, nâng cấp và huỷ bỏ (dừng hoạt động) hệ thống thông tin.

c) Xử lý sự cố an toàn thông tin mạng phải phù hợp với trách nhiệm, quyền hạn và đảm bảo lợi ích hợp pháp của cơ quan, đơn vị, cá nhân liên quan và theo quy định của pháp luật.

Điều 3. Giải thích từ ngữ.

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

1. *Mạng* được quy định tại Khoản 2 Điều 3 Luật An toàn thông tin mạng. Cụ thể: 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.

2. *An toàn thông tin mạng* được quy định tại Khoản 1 Điều 3 Luật An toàn thông tin mạng. Cụ thể: 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.

3. *Hệ thống thông tin* được quy định tại Khoản 3 Điều 3 Luật An toàn thông tin mạng. Cụ thể: 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. *Xâm phạm an toàn thông tin mạng* được quy định tại Khoản 6 Điều 3 Luật An toàn thông tin mạng. Cụ thể: 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.

5. *Sự cố an toàn thông tin mạng* được quy định tại Khoản 7 Điều 3 Luật An toàn thông tin mạng. Cụ thể: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.

6. *Rủi ro an toàn thông tin mạng* được quy định tại Khoản 8 Điều3 Luật An toàn thông tin mạng. Cụ thể: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.

7. *Phần mềm độc hại* được quy định tại Khoản 11 Điều 3 Luật An toàn thông tin mạng. Cụ thể: 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.

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

Điều 4. Những hành vi nghiêm cấm.

1. Các hành vi bị nghiêm cấm được quy định tại Điều 7 Luật An toàn thông tin mạng số 86/2015/QH13 ngày 19/11/2015 và Điều 8 Luật An ninh mạng số 24/2018/QH14 ngày 12/6/2018, cụ thể:

- Ngăn chặn việc truyền tải thông tin trên mạng, can thiệp, truy nhập, gây nguy hại, xoá, thay đổi, sao chép và làm sai lệch thông tin trên mạng trái pháp luật.

- Gây ảnh hưởng, cản trở trái pháp luật tới hoạt động bình thường của hệ thống thông tin hoặc tới khả năng truy nhập hệ thống thông tin của người sử dụng.

- Tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng của biện pháp bảo vệ an toàn thông tin mạng của hệ thống thông tin; tấn công, chiếm quyền điều khiển, phá hoại hệ thống thông tin.

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

- Thu thập, sử dụng, phát tán, kinh doanh trái pháp luật thông tin cá nhân của người khác; lợi dụng sơ hở, điểm yếu của hệ thống thông tin để thu thập, khai thác thông tin cá nhân.

- Xâm nhập trái pháp luật bí mật mật mã và thông tin đã mã hóa hợp pháp của cơ quan, tổ chức, cá nhân; tiết lộ thông tin về sản phẩm mật mã dân sự, thông tin về khách hàng sử dụng hợp pháp sản phẩm mật mã dân sự; sử dụng, kinh doanh các sản phẩm mật mã dân sự không rõ nguồn gốc.

2. Tự ý lắp đặt các thiết bị phát sóng Wifi (Access Point) vào mạng máy tính của cơ quan, đơn vị và lắp đặt các thiết bị tiếp sóng Wifi (Wireless card, wireless USB) trên máy tính có kết nối mạng nội bộ để truy cập mạng wifi ngoài khi chưa được phê duyệt của Lãnh đạo Sở.

3. 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.

4. 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.

5. Tự ý tải về, chia sẻ dưới mọi hình thức các dữ liệu, tài liệu, số liệu nội bộ, những văn bản chưa được cấp có thẩm quyền công khai lên mạng internet và các phương tiện thông tin đại chúng khác.

6. Thu thập, sử dụng, phát tán, kinh doanh trái pháp luật thông tin cá nhân của người khác, lợi dụng sơ hở, điểm yếu của hệ thống thông tin để thu thập, khai thác thông tin cá nhân.

Điều 5. Phối hợp với những cơ quan/tổ chức có thẩm quyền.

1. Phân công bộ phận chuyên trách về an toàn thông tin thuộc Văn phòng Sở.

2. Trách nhiệm của bộ phận chuyên trách về an toàn thông tin.

Là đầu mối liên hệ, tiếp nhận, phối hợp với các cơ quan, tổ chức (có thẩm quyền quản lý về an toàn thông tin) trong công tác đảm bảo an toàn thông tin, hỗ trợ điều phối xử lý sự cố an toàn thông tin.

Là đầu mối liên hệ, phối hợp với Sở Thông tin và Truyền thông và các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin phục vụ việc bảo đảm an toàn, an ninh mạng cho Hệ thống Thông tin hỗ trợ quản lý, điều hành ngân sách của tỉnh..

Tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của tổ chức có thẩm quyền.

Làm đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin mạng trong nội bộ Sở.

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

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

Định kỳ hằng năm báo cáo về tình hình an toàn thông tin mạng, gửi về Sở Thông tin và Truyền thông (theo hướng dẫn của Sở Thông tin và Truyền thông).

Chương II
BẢO ĐẢM AN TOÀN THÔNG TIN TRONG QUẢN LÝ VẬN HÀNH HỆ THỐNG

Điều 6. Quản lý an toàn mạng.

1. Hệ thống mạng phải được thiết kế thống nhất, được quản lý định danh, xác thực đối với tất cả người sử dụng nhằm mục đích quản lý và bảo đảm an toàn và bảo mật.

2. Hệ thống mạng nội bộ (LAN) phải được bảo vệ bằng tường lửa (có thể tích hợp tường lửa trên modem hoặc router) và phân chia hệ thống mạng thành các vùng mạng quản lý theo chính sách an toàn thông tin riêng.

3. 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. Hệ thống mạng không dây phải được bảo vệ bởi mật khẩu an toàn.

Điều 7. Quản lý an toàn máy chủ và ứng dụng.

1. Máy chủ phải được thiết lập chính sách xác thực và kiểm soát truy cập. Các hệ thống thông tin cần có phướng án giới hạn số lần đăng nhập, tự động khóa tài khoản khi liên tục đăng nhập sai vượt quá số lần quy định. Tổ chức theo dõi, giám sát tất cả các phương pháp đăng nhập từ xa, nhất là các trường hợp đăng nhập vào hệ thống với mục đích quản trị.

2. Kiểm tra, giám sát các hoạt động liên quan đến các nơi lưu trữ mật khẩu và cảnh báo khi có những hành động bất thường (Ví dụ: user không có quyền nhưng cố tình truy xuất đến các file lưu mật khẩu…).

Điều 8. Quản lý an toàn dữ liệu.

1. Có cơ chế sao lưu dữ liệu dự phòng, lưu trữ dữ liệu tại nơi an toàn đồng thời thường xuyên kiểm tra để đảm bảo sẵn sàng phục hồi nhằm ngăn ngừa và hạn chế khi sự cố an toàn thông tin mạng xảy ra. Dữ liệu trên máy chủ được sao lưu thông qua hệ thống sao lưu dữ liệu.

2. Định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ và các thông tin, dữ liệu quan trọng khác trên hệ thống theo yêu cầu của đơn vị vận hành.

3. Quyền truy cập phải được phân ra theo từng cấp độ tương ứng với từng nhiệm vụ của nhân viên và phải được phê duyệt từ cấp trên.

Điều 9. Quản lý an toàn người sử dụng đầu cuối.

Chính sách, quy trình quản lý an toàn người sử dụng đầu cuối bao gồm:

1. Việc sử dụng các thiết bị lưu trữ ngoài như ổ cứng di động, các loại thẻ nhớ, thiết bị lưu trữ USB,... phải thường xuyên quét virus trước khi đọc hoặc sao chép dữ liệu.

2. Không sử dụng các máy tính thuộc sở hữu cá nhân (máy xách tay của cá nhân, thiết bị di động) hoặc những thiết bị lưu trữ di động cá nhân vào mục đích kinh doanh của công ty tại nơi làm việc. Hạn chế tối đa việc sử dụng các thiết bị lưu trữ ngoài để sao chép, di chuyển dữ liệu.

3. Các thiết bị đầu cuối khi kết nối phải được quản lý và cập nhật thông tin (tên, chủng loại, địa chỉ MAC, địa chỉ IP). Cần sử dụng cơ chế xác thực và sử dụng giao thức mạng an toàn.

4. Bộ phận chuyên trách về an toàn thông tin phải thường xuyên theo dõi, kiểm tra các lỗ hổng bảo mật và quản lý kết nối, truy cập khi sử dụng thiết bị đầu cuối từ xa, theo dõi cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống đối với các nhân viên đã nghỉ việc, theo dõi cấu hình tối ưu và tăng cường bảo mật (cứng hóa) cho máy tính người sử dụng và thực hiện quy trình trước khi đưa hệ thống vào sử dụng.

Điều 10. Quản lý rủi ro an toàn thông tin mạng.

1. Đơn vị vận hành hệ thống thông tin lập danh sách toàn bộ các thiết bị, phần mềm công nghệ thông tin đang sử dụng trong phạm vi quản lý của chủ quản hệ thống thông tin: nhãn hiệu phần cứng; tên phần mềm và phiên bản (hệ điều hành, cơ sở dữ liệu, ứng dụng, các tiện ích khác).

2. Thiết lập, duy trì kênh tiếp nhận thông tin về lỗ hổng, điểm yếu an toàn thông tin mạng từ các cơ quan, tổ chức có chức năng cảnh báo về an toàn thông tin mạng; các đơn vị cung cấp thiết bị, phần mềm công nghệ thông tin mà đơn vị vận hành đang sử dụng.

Điều 11. Quản lý truy cập.

1. Cán bộ thuộc Sở có trách nhiệm:

- Bảo vệ bí mật thông tin tài khoản cá nhân, hoặc tài khoản của cơ quan, đơn vị khi được phân công nắm giữ đồng thời phải thay đổi ngay mật khẩu tài khoản khi mới được cấp và tự chịu trách nhiệm trong việc quản lý, bảo vệ mật khẩu của tài khoản, không được cho người khác sử dụng tài khoản cá nhân hoặc của cơ quan.

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

- Thiết lập mật mã truy cập và chế độ tự động bảo vệ màn hình sau 10 phút không sử dụng cho tất cả hệ thống máy chủ, máy trạm của người sử dụng.

- Hệ thống mạng không dây (Wifi) của các phòng làm việc 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.

- Đặt mật khẩu đăng nhập, truy cập hệ thống thông tin có độ phức tạp cao (có độ dài tối thiểu 8 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 03 tháng/lần cho tất cả các tài khoản truy cập vào hệ thống máy chủ, thiết bị mạng, máy tính, các ứng dụng.

- Thực hiện rà soát tối thiểu 03 tháng/lần các tài khoản đăng nhập, bảo đảm các tài khoản và quyền truy cập hệ thống được cấp phát đúng, đủ.

2. Đối với các hệ thống thông tin:

- Bảo đảm mỗi tài khoản của tổ chức, cá nhân truy cập vào hệ thống thông tin là duy nhất.

- Các hệ thống thông tin cần giới hạn số lần đăng nhập sai liên tiếp vào hệ thống (từ 03 đến 05 lần). Hệ thống tự động khóa tài khoản trong một khoảng thời gian nhất định nếu liên tục đăng nhập sai vượt quá số lần quy định trước khi tiếp tục cho đăng nhập và có phương thức hỗ trợ cấp lại mật khẩu tài khoản.

- Cơ quan vận hành các hệ thống dùng chung sẽ không chịu trách nhiệm về những thiệt hại do phía người dùng không tuân thủ các quy định về bảo vệ bí mật tài khoản dẫn đến thông tin cá nhân bị đánh cắp hay bị sửa đổi, các ứng dụng bị sử dụng mạo danh hay các hậu quả tiêu cực khác.

Điều 12. Phòng chống phần mềm độc hại.

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

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

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

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

5. Các máy tính xách tay, thiết bị di động (điện thoại thông minh, máy tính bảng,...) trước khi kết nối vào mạng LAN nội bộ của cơ quan, đơn vị phải bảo đảm đã được cài chương trình phòng chống phần mềm độc hại và đã được kiểm duyệt về các phần mềm độc hại.

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

7. Máy chủ chỉ được dùng để cài đặt các phần mềm, dịch vụ dùng chung của cơ quan, đơn vị; không cài đặt phần mềm không rõ nguồn gốc, phần mềm phục vụ mục đích cá nhân và mục đích khác, không phục vụ công việc.

8. Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại trên máy trạm như: máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống phần mềm độc hại, tình trạng này lặp đi lặp lại nhiều

lần, ở các vị trí khác nhau; quan trọng nhất là có dấu hiệu mất dữ liệu…, người sử dụng phải tắt máy, ngắt kết nối từ máy tính đến mạng LAN nội bộ, mạng WAN ngành tài chính, mạng truyền số liệu chuyên dùng của tỉnh, mạng Internet,... và báo trực tiếp cho bộ phận có trách nhiệm của Sở để xử lý.

Điều 13. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ.

Quy định, quy trình về Kết thúc vận hành, khai thác, thanh lý, hủy bỏ bao gồm các nội dung sau:

1. Thiết bị CNTT có chứa dữ liệu (máy tính, thiết bị lưu trữ, ...) khi bị hỏng phải được cán bộ vận hành kiểm tra, sửa chữa, khắc phục. Phải có biện pháp kiểm tra, giám sát đảm bảo không để lọt lộ thông tin hay lây nhiễm mã độc đối với máy tính mang ra bên ngoài sửa chữa, bảo hành.

2. Trước khi tiến hành thanh lý/loại bỏ thiết bị công nghệ thông tin cũ, phải áp dụng các biện pháp kỹ thuật xoá bỏ hoàn toàn dữ liệu người dùng đã tạo ra, đảm bảo không thể phục hồi.

3. Các phương tiện và thiết bị CNTT: Máy tính cá nhân (PC), máy tính xách tay, máy chủ, các thiết bị mạng, phương tiện lưu trữ như CD/DVD, thẻ nhớ, ổ cứng phải xóa sạch dữ liệu khi chuyển giao hoặc thay đổi mục đích sử dụng.

Chương III
TỔ CHỨC BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 14. Đảm bảo an toàn hệ thống mạng máy tính, kết nối Internet

1. Quản lý hệ thống mạng nội bộ: Mạng nội bộ của Sở phải được tổ chức theo mô hình Clients/Server; mạng nội bộ khi kết nối với mạng Internet phải thông qua thiết bị tường lửa (Firewall) kiểm soát, 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.

2. Quản lý hệ thống mạng không dây (Wifi): Khi thiết lập mạng không dây có kết nối vào mạng nội bộ phải thiết lập các thông số cần thiết như định danh, mật mã, mã hóa dữ liệu, có thay đổi mật mã định kỳ.

3. Quản lý truy cập từ xa vào mạng nội bộ: Đối với việc truy cập từ xa vào mạng nội bộ phải được theo dõi, quản lý chặt chẽ, nhất là truy cập có sử dụng chức năng quản trị, phải thiết lập mật mã độ an toàn cao, thường xuyên thay đổi mật mã, hạn chế truy cập từ xa vào mạng nội bộ từ các điểm truy cập Internet công cộng.

Điều 15. Quản lý, khai thác, sử dụng cơ sở dữ liệu và phần mềm.

1. Văn phòng Sở có trách nhiệm cài đặt, quản lý các phần mềm hệ thống và phần mềm ứng dụng trong hệ thống mạng máy tính tại Sở; Nghiên cứu, đề xuất, nâng cấp công nghệ, phần mềm theo định hướng quản lý nhà nước của ngành và tuân theo quy định của Nhà nước.

2. Các phòng, đơn vị trực thuộc Sở và toàn thể cán bộ có trách nhiệm phối hợp với Văn phòng Sở trong quá trình triển khai, khai thác và sử dụng các phần mềm đã được cài đặt.

Điều 16. Trách nhiệm của người dùng.

1. 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 mạng trong phạm vi trách nhiệm và quyền hạn được giao.

2. Khi tham gia vận hành mạng LAN của Sở phải nghiêm chỉnh chấp hành chế độ bảo mật, an toàn, an ninh thông tin đồng thời chịu trách nhiệm đối với các thông tin mà mình cung cấp. Mỗi cán bộ 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 vào các trang thông tin điện tử 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; không cho phép bất cứ hành vi nào gây tổn hại đến dịch vụ, gây hư hỏng thiết bị mạng; không cung cấp thông tin không trung thực để công bố trên mạng; sử dụng mạng để thâm nhập vào các mạng máy tính khi chưa được phép; không đưa các thông tin có nội dung "**MẬT**", "**TỐI MẬT**" và "**TUYỆT MẬT**" lên hệ thống máy tính có kết nối mạng Internet.

3. Trong trao đổi thông tin, dữ liệu phục vụ công việc, các cơ quan, đơn vị, cán bộ phải sử dụng hệ thống thông tin do cơ quan, đơn vị có thẩm quyền triển khai như: Hệ thống thư điện tử của tỉnh (hovaten.stc@bacninh.gov.vn) hoặc hệ thống thư điện tử của Bộ Tài chính; Hệ thống quản lý văn bản và điều hành. Không sử dụng các trang mạng xã hội, các dịch vụ thư điện tử công cộng,… để trao đổi thông tin quan trọng liên quan đến công việc chuyên môn của cơ quan.

4. Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo với bộ phận chuyên trách công nghệ thông tin của Sở để kịp thời ngăn chặn và xử lý.

5. Tham gia các chương trình đào tạo, hội nghị về an toàn thông tin mạng do các cơ quan, đơn vị chuyên trách an toàn thông tin mạng hoặc Sở Thông tin và Truyền thông tổ chức.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 17. Điều khoản thi hành.

1. Giao cho Trưởng các phòng, đơn vị có trách nhiệm triển khai, quán triệt và đôn đốc thực hiện nghiêm túc nội dung quy chế này đến toàn thể cán bộ. Trường hợp cán bộ thuộc phòng vi phạm Trưởng phòng có trách nhiệm báo cáo lãnh đạo Sở (qua Văn phòng Sở) để làm căn cứ đánh giá xếp loại cán bộ hàng năm.

2. Giao Văn phòng Sở tổng hợp báo cáo kết quả thực hiện theo quy định.

3. Trong quá trình thực hiện, nếu có vấn đề phát sinh hoặc khó khăn, vướng mắc cần phản ánh kịp thời về Văn phòng Sở để tổng hợp báo cáo Giám đốc Sở xem xét quyết định điều chỉnh, bổ sung cho phù hợp./.