UBND TỈNH BÌNH ĐỊNH **SỞ LAO ĐỘNG - THƯƠNG BINH VÀ XÃ HỘI**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**
Số: 471 /QĐ-SLĐTBXH	*Bình Định, ngày 31 tháng 12 năm 2019*

QUYẾT ĐỊNH

Ban hành Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của Sở Lao động – Thương binh và Xã hội

GIÁM ĐỐC SỞ LAO ĐỘNG – THƯƠNG BINH VÀ XÃ HỘI

Căn cứ Quyết định số 368/QĐ-UBND ngày 03/02/2016 của UBND tỉnh ban hành Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Sở Lao động - Thương binh và Xã hội và Quyết định số 4435/QĐ-UBND ngày 28/11/2017 của UBND tỉnh về việc sửa đổi, bổ sung Điều 3 Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Sở Lao động - Thương binh và Xã hội ban hành kèm theo Quyết định số 368/QĐ-UBND ngày 03/02/2016 của UBND tỉnh;

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

Căn cứ Chỉ thị số 897/CT-TTg ngày 10/06/2011 của Thủ tướng Chính phủ về việc tăng cường triển khai các hoạt động đảm bảo an toàn thông tin số;

Căn cứ Quyết định số 22/2012/QĐ-UBND ngày 12/7/2012 của UBND tỉnh Bình Định về việc ban hành Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan quản lý hành chính nhà nước tỉnh Bình Định;

Xét đề nghị của Chánh Văn phòng Sở.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của Sở Lao động – Thương binh và Xã hội.

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

Điều 3. Chánh Văn phòng Sở, Trưởng các phòng, đơn vị trực thuộc Sở, công chức, viên chức và người lao động Sở Lao động – Thương binh và Xã hội căn cứ Quyết định thi hành./.

Nơi nhận:
- Như Điều 3;
- Lãnh đạo Sở;
- Lưu: VT, VP.

GIÁM ĐỐC

Nguyễn Mỹ Quang

UBND TỈNH BÌNH ĐỊNH
SỞ LAO ĐỘNG - THƯƠNG BINH VÀ XÃ HỘI

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

QUY CHẾ
Đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của Sở Lao động – Thương binh và Xã hội

(Kèm theo Quyết định số: ... /QĐ-SLĐTBXH ngày ... /12/2019 của Sở Lao động – Thương binh và Xã hội)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi và đối tượng áp dụng

1. Quy chế này quy định về đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin (CNTT) của Sở Lao động – Thương binh và Xã hội (LĐTBXH).

2. Quy chế này được áp dụng đối với các phòng Sở, các đơn vị trực thuộc Sở, công chức, viên chức và người lao động (CCVCNLĐ) Sở LĐTBXH.

Điều 2. Mục đích đảm bảo an toàn, an ninh thông tin

Giảm thiểu được các nguy cơ gây sự cố mất an toàn, an ninh thông tin và đảm bảo an toàn về dữ liệu, các thiết bị công nghệ thông tin trong hoạt động ứng dụng CNTT của Sở LĐTBXH.

Điều 3. Giải thích từ ngữ

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

1. *Virus máy tính:* Là một chương trình hay một đoạn mã có khả năng tự sao chép chính nó từ đối tượng lây nhiễm này sang đối tượng khác với mục đích gây hại cho máy tính.

2. *Firewall:* Là một kỹ thuật được tích hợp vào máy tính và hệ thống mạng để chống lại sự truy cập trái phép nhằm bảo vệ các nguồn thông tin nội bộ cũng như hạn chế sự xâm nhập vào hệ thống của một số đối tượng khác không mong muốn.

3. *Hệ thống thông tin:* là một tập hợp và kết hợp của các phần cứng, phần mềm và các hệ thống mạng truyền thông được xây dựng và sử dụng để thu thập, tái tạo, phân phối và chia sẻ các dữ liệu, thông tin và tri thức nhằm phục vụ hoạt động của cơ quan, đơn vị.

Chương II
QUY ĐỊNH ĐẢM BẢO AN TOÀN, AN NINH HỆ THỐNG THÔNG TIN

Điều 4. Quản lý các nguồn tài nguyên của hệ thống thông tin

1. Đối với phần mềm

a) Phần mềm đã được cơ quan, đơn vị mua bản quyền nhằm phục vụ cho việc đảm bảo an toàn hệ thống thông tin, yêu cầu tất cả CCVCNLĐ sử dụng máy tính phải cài đặt và thường xuyên cập nhật phiên bản mới theo hướng dẫn của nhà cung cấp.

b) Các phần mềm ứng dụng như: Phần mềm kế toán, tiền lương, phần mềm thu thập, tổng hợp, báo cáo số liệu, phần mềm văn phòng điện tử,... phải đảm bảo tính chính xác của thông tin, không gây ra sự cố mất dữ liệu, đảm bảo hệ thống phần mềm hoạt động liên tục.

2. Đối với dữ liệu

a) Người sử dụng có trách nhiệm tự quản lý dữ liệu lưu trữ trên máy tính phục vụ công tác chuyên môn của mình, định kỳ ít nhất 06 tháng một lần, phải tiến hành lưu trữ, sao chép dữ liệu trong máy tính ra thiết bị lưu trữ như: ổ cứng gắn ngoài, USB,... (dữ liệu trong các máy tính phải tiến hành sao chép để bảo vệ là những dữ liệu chuyên môn phục vụ công tác của cơ quan, đơn vị).

b) Các thiết bị lưu trữ thông tin phải được bảo quản ở nơi an toàn và bảo mật. Các dữ liệu có tính chất quan trọng cần phải được mã hóa nhằm bảo vệ khỏi bị đánh cắp, lộ lọt thông tin.

3. Đối với trang thiết bị

a) Những máy tính có chứa dữ liệu quan trọng cần được bảo vệ như: máy của lãnh đạo Sở, máy tính sử dụng cho công việc kế toán, văn thư, lưu trữ,…phải cài đặt phần mềm diệt virus tin cậy, có bản quyền; đối với các máy tính khác, có thể cài đặt phần mềm diệt virus miễn phí nhưng phải đảm bảo nguồn gốc, có độ tin cậy cao, được cộng đồng công nhận.

b) Các thiết bị gắn ngoài như USB, thẻ nhớ, máy tính xách tay, máy tính bảng, điện thoại di động,…khi cắm vào máy tính hoặc mạng nội bộ, mạng internet, mạng không dây (wifi) của cơ quan, đơn vị phải đảm bảo không có virus hoặc các phần mềm độc hại khác để đảm bảo an toàn cho hệ thống mạng máy tính của cơ quan, đơn vị.

c) Phải bố trí 01 máy tính riêng, không kết nối mạng nội bộ, mạng internet dùng để quản lý, soạn thảo các tài liệu mật theo quy định.

Điều 5. Các biện pháp quản lý vận hành trong công tác đảm bảo an toàn, an ninh thông tin

1. Quản lý, cấp phát tài khoản truy nhập các hệ thống thông tin

a) Quản trị mạng có trách nhiệm tạo lập, sửa đổi và cung cấp thông tin tài khoản truy nhập hệ thống mạng nội bộ, hệ thống văn phòng điện tử (iDesk), hệ thống thư điện tử công vụ,… cho người sử dụng.

b) Đối với người sử dụng tiếp nhận mới hoặc chuyển công tác, nghỉ hưu, nghỉ việc: Quản trị mạng căn cứ quyết định của cơ quan, tạo mới hoặc hủy bỏ các tài khoản có liên quan của cá nhân tương ứng.

c) Thiết lập tài khoản người dùng với quyền thấp nhất, chỉ vừa đủ để phục vụ công việc theo đúng chức năng, nhiệm vụ được giao. Không sử dụng tài khoản có quyền quản trị (Administrator) khi không cần thiết để giảm khả năng lây nhiễm mã độc vào hệ thống. Chỉ sử dụng quyền quản trị khi cài đặt, gỡ bỏ, cấu hình thay đổi thông tin về hệ thống.

2. Quản lý đăng nhập hệ thống

a) Người sử dụng đã được cấp các tài khoản truy nhập vào các hệ thống thông tin của cơ quan phải đổi mật khẩu được cấp ban đầu ngay từ lần truy cập đầu tiên, mật khẩu phải đạt độ an toàn cao (bao gồm số, chữ hoa, chữ thường và ký tự đặc biệt, ví dụ: P@ssw0rd). Không dùng chung một mật khẩu cho nhiều tài khoản, định kỳ 03 đến 06 tháng thay đổi mật khẩu một lần, có trách nhiệm bảo vệ, bảo mật các tài khoản của mình, không cung cấp thông tin tài khoản của mình cho các cá nhân không liên quan, đồng thời không tự ý xâm nhập tài khoản của người khác.

3. Hệ thống mạng nội bộ

a) Hệ thống mạng nội bộ được thiết lập và quản lý theo từng phòng chuyên môn; địa chỉ mạng (IP) của máy tính được hệ thống cấp phát tự động trong dải địa chỉ quy định; tên máy tính được đặt theo tên của người sử dụng.

b) Hệ thống mạng không dây được kết nối với mạng nội bộ thông qua các thiết bị phát sóng (Access Point) và phải được thiết lập các tham số bảo mật theo chuẩn bảo mật mạng không dây an toàn nhất.

c) Hệ thống máy chủ, thiết bị chuyển mạch (switch), tường lửa (firewall), thiết bị định tuyến internet (router), phát sóng,…được đặt cố định, ở nơi an toàn, có nguồn điện cung cấp ổn định. CCVCNLĐ không có nhiệm vụ thì không tự ý đụng vào hoặc truy xuất trái phép.

4. Đối với máy tính, thiết bị lưu trữ

a) CCVCNLĐ phải đặt mật khẩu truy cập vào máy tính của mình, đồng thời cài đặt chế độ tự động khóa màn hình có sử dụng mật khẩu bảo vệ sau một khoảng thời gian nhất định khi không sử dụng máy tính.

b) Sử dụng thiết bị lưu trữ (USB, ổ cứng gắn ngoài,...) an toàn, đúng cách để phòng ngừa virus, phần mềm gián điệp xâm nhập vào máy tính: Tắt bỏ tính năng tự động chạy ứng dụng khi kết nối với thiết bị lưu trữ, không được trực tiếp truy nhập ngay vào thiết bị lưu trữ mà phải quét virus trước.

5. Chống mã độc, virus

Lựa chọn, triển khai các phần mềm chống virus, thư rác trên các máy chủ, máy trạm để phát hiện, loại trừ những đoạn mã độc hại (virus, trojan, worm,…) và hỗ trợ người sử dụng cài đặt. Bật tính năng tự động cập nhật của phần mềm chống virus trên các máy chủ, máy trạm để đảm bảo chương trình luôn có cơ sở dữ liệu nhận dạng virus mới nhất, thiết lập chế độ quét thường xuyên ít nhất là hằng tuần.

6. Lưu trữ, quản lý tài nguyên và chia sẻ thông tin

a) Để đảm bảo an toàn, an ninh thông tin trong việc truyền tải, lưu trữ, sao chép thông tin, người sử dụng nên cân nhắc việc chia sẻ tài nguyên cục bộ trên máy tính đang sử dụng, tuyệt đối không được chia sẻ toàn bộ ổ cứng. Khi thực hiện việc chia sẻ tài nguyên trên máy cục bộ hoặc trên các hệ thống thông tin của cơ quan, đơn vị nên sử dụng mật khẩu để bảo vệ thông tin. Khuyến khích việc truyền tải, chia sẻ thông tin, tài liệu qua phần mềm iDesk hoặc qua hệ thống thư điện tử công vụ.

b) Không lưu trữ dữ liệu trên ổ đĩa cứng cài đặt hệ điều hành (mặc định là ổ C:), việc lưu trữ dữ liệu chỉ thực hiện trên ổ đĩa cứng (D:), (E:),…hoặc trên USB, phòng khi máy tính gặp sự cố thì việc khôi phục hoạt động được nhanh chóng, không ảnh hưởng, thất thoát dữ liệu.

Điều 6. Bảo vệ bí mật nhà nước trong ứng dụng công nghệ thông tin

1. Không được sử dụng máy tính có nối mạng nội bộ, mạng internet để soạn thảo văn bản, chuyển giao, lưu trữ thông tin có nội dung bí mật Nhà nước; không cung cấp tin, tài liệu và đưa thông tin bí mật Nhà nước lên trang thông tin điện tử. Nghiêm cấm cài cắm các thiết bị lưu trữ tài liệu có nội dung bí mật Nhà nước vào máy tính nối mạng nội bộ, mạng internet.

2. Không được in, sao chụp tài liệu, vật mang bí mật Nhà nước trên các thiết bị kết nối mạng nội bộ, mạng internet.

3. Khi sửa chữa, khắc phục các sự cố của máy tính dùng để soạn thảo văn bản mật, không được cho phép bất kỳ đơn vị tư nhân hoặc người không có trách nhiệm trực tiếp sửa chữa, xử lý, khắc phục.

4. Trước khi thanh lý các máy tính của cơ quan, đơn vị, quản trị mạng phải dùng các biện pháp xóa bỏ vĩnh viễn dữ liệu trong ổ cứng máy tính.

Điều 7. Xử lý khẩn cấp sự cố về an toàn, an ninh thông tin

Khi phát hiện hệ thống bị tấn công, thông qua các dấu hiệu như: luồng tin tăng lên bất ngờ, nội dung trang chủ bị thay đổi, hệ thống hoạt động rất chậm khác thường, ... cần thực hiện các bước cơ bản sau:

Bước 1: Ngắt kết nối máy chủ ra khỏi mạng nội bộ, mạng internet.

Bước 2: Sao chép toàn bộ dữ liệu của hệ thống ra thiết bị lưu trữ.

Bước 3: Tiến hành quét virus toàn bộ hệ thống.

Bước 4: Khôi phục hệ thống bằng cách chuyển dữ liệu sao lưu mới nhất để hệ thống hoạt động

Trường hợp sự cố nghiêm trọng vượt quá khả năng khắc phục thì báo cáo ngay với lãnh đạo cơ quan, đơn vị để có hướng xử lý tiếp theo.

Chương III
TRÁCH NHIỆM ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

Điều 8. Trách nhiệm của các phòng, đơn vị trực thuộc Sở

1. Các Trưởng phòng, đơn vị trực thuộc Sở chịu trách nhiệm trước Lãnh đạo Sở trong công tác đảm bảo an toàn, an ninh thông tin của phòng, đơn vị mình.

2. Nghiêm chỉnh chấp hành các quy định nội bộ, quy định về an toàn thông tin của cơ quan, đơn vị cũng như các quy định khác của pháp luật; nâng cao ý thức cảnh giác và trách nhiệm đảm bảo an ninh thông tin của cơ quan, đơn vị.

3. Tạo điều kiện cho công chức, viên chức người lao động trong phòng, đơn vị tham gia các chương trình đào tạo về an toàn an ninh thông tin.

Điều 9. Trách nhiệm của CCVCNLĐ Sở LĐTBXH

1. Nghiêm chỉnh chấp hành các quy định của quy chế này cũng như các quy định khác đã được UBND tỉnh và Sở ban hành như: Quy chế đảm bảo an toàn, an ninh thông tin; Quy chế quản lý, sử dụng Hệ thống thư điện tử công vụ, Quy chế quản lý, sử dụng Hệ thống văn phòng điện tử và các quy định khác của pháp luật.

2. Có trách nhiệm tự quản lý các thiết bị được giao sử dụng; không tự ý thay đổi tên máy, cấu hình, địa chỉ mạng (IP) và tháo lắp các thiết bị trên máy vi tính; không tự ý liên hệ với cá nhân bên ngoài vào can thiệp các thiết bị máy tính; nâng cao ý thức cảnh giác và trách nhiệm đảm bảo an ninh thông tin tại cơ quan, đơn vị.

3. Các máy tính khi không sử dụng trong thời gian dài (quá 4 giờ làm việc) cần tắt máy hoặc ngưng kết nối mạng, để tránh bị các hacker lợi dụng, sử dụng chức năng điều khiển từ xa dùng máy tính của mình tấn công vào các hệ thống thông tin khác.

4. Hạn chế việc sử dụng chức năng chia sẻ tài nguyên (sharing), khi sử dụng chức năng này nên bật tính năng bảo mật bằng mật khẩu và thực hiện việc thu hồi chức năng này khi đã sử dụng xong.

5. Không được truy cập hoặc tải thông tin từ các Website có đường dẫn lạ, không rõ nguồn gốc, nội dung hoặc các Website độc hại; không tải và cài đặt các phần mềm không rõ nguồn gốc, không liên quan đến công việc chuyên môn. Hạn chế tải những file có dung lượng lớn (trên 300 MB) trong giờ làm việc, sẽ làm ảnh hưởng đến tốc độ đường truyền mạng internet của cơ quan, đơn vị.

6. Không mở các thư điện tử được gửi bởi người lạ, xóa ngay các thư này khỏi hộp thư. Đối với các tập tin đính kèm theo thư điện tử hoặc được tải xuống từ internet, các thiết bị lưu trữ gắn vào hệ thống cần được kiểm tra để phòng chống lây nhiễm virus hoặc phần mềm gián điệp gây mất mát thông tin.

7. Khi phát hiện các nguy cơ mất an toàn hoặc sự cố phải báo cáo ngay cho lãnh đạo phòng, đơn vị, đồng thời thông báo cho quản trị mạng để kịp thời ngăn chặn, xử lý.

8. Tham gia các chương trình đào tạo, hội nghị về an toàn, an ninh thông tin do các cơ quan, đơn vị về an ninh mạng tổ chức.

Điều 10. Trách nhiệm của quản trị mạng

1. Chịu trách nhiệm trước lãnh đạo cơ quan, đơn vị trong công tác bảo vệ an toàn, an ninh các hệ thống thông tin của cơ quan, đơn vị.

2. Thường xuyên theo dõi, xử lý kịp thời các sự cố xảy ra của hệ thống mạng máy tính của cơ quan, đơn vị; tham mưu cho lãnh đạo cơ quan, đơn vị triển khai các biện pháp phòng chống virus, thư rác cho hệ thống máy chủ và máy trạm trong mạng của cơ quan, đơn vị.

3. Quản lý, phân quyền, hủy quyền truy cập hệ thống thông tin, thu hồi lại thông tin liên quan tới tài khoản trong hệ thống thông tin đối với công chức, viên chức, người lao động nghỉ chế độ hoặc chuyển công tác; hướng dẫn người dùng thay đổi mật khẩu cá nhân theo quy định.

4. Thường xuyên sao lưu dữ liệu của máy chủ, thiết bị mạng; kiểm tra dữ liệu sao lưu phảo đảm bảo tính sẵn sàng và toàn vẹn.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 11. Điều khoản thi hành

Trưởng phòng, đơn vị, công chức, viên chức, người lao động có trách nhiệm triển khai thực hiện Quy chế này.

Trong quá trình triển khai thực hiện, nếu có vấn đề còn bất cập thì các phòng chuyên môn nghiệp vụ, đơn vị trực thuộc Sở báo cáo về Sở Lao động - Thương binh và Xã hội (qua Văn phòng Sở) xem xét, điều chỉnh, bổ sung cho phù hợp./.

GIÁM ĐỐC

Nguyễn Mỹ Quang