UBND TỈNH BÌNH DƯƠNG
SỞ TÀI NGUYÊN VÀ MÔI TRƯỜNG

Số: 215 /QĐ-STNMT

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

Bình Dương, ngày 07 tháng 3 năm 2022.

QUYẾT ĐỊNH

Về việc ban hành Quy chế quản lý, vận hành, khai thác, đảm bảo an toàn thông tin các hệ thống thông tin ngành tài nguyên và môi trường thuộc Sở Tài nguyên và Môi trường tỉnh Bình Dương

GIÁM ĐỐC SỞ TÀI NGUYÊN VÀ MÔI TRƯỜNG

Căn cứ Luật An toàn thông tin mạng số 86/2015/QH13 ngày 19/11/2015;

Căn cứ Luật An ninh mạng số 24/2018/QH14 ngày 12/6/2018;

Căn cứ Nghị định 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 Thông tư 03/2017/TT-BTTTT ngày 24/4/2017 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 01/7/2016 của chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Quyết định số 16/2015/QĐ-UBND ngày 27/4/2015 của Ủy ban nhân dân tỉnh Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Sở Tài nguyên và Môi trường tỉnh Bình Dương;

Xét đề nghị của Trung tâm Công nghệ thông tin – Lưu trữ tài nguyên và môi trường tại Tờ trình số 66. /TTr-TTCNTTLT ngày 01. / 3. /2022,

QUYẾT ĐỊNH:

Điều 1: Ban hành kèm theo Quyết định này Quy chế quản lý, vận hành, khai thác, đảm bảo an toàn thông tin các hệ thống thông tin ngành tài nguyên và môi trường thuộc Sở Tài nguyên và Môi trường tỉnh Bình Dương.

Điều 2: Quyết định này có hiệu lực kể từ ngày ký và thay thế Quyết định số 110/QĐ-STNMT ngày 05/02/2016 về việc ban hành Quy chế quản lý sử dụng mạng máy tính nội bộ và hệ thống thư điện tử thuộc Sở Tài nguyên và Môi trường tỉnh Bình Dương.

Điều 3: Chánh Văn phòng, Giám đốc Trung tâm Công nghệ thông tin – Lưu trữ tài nguyên và môi trường, Trưởng các phòng, đơn vị trực thuộc Sở Tài nguyên và Môi trường và cán bộ, viên chức có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Ban Giám đốc;
- Các đơn vị trực thuộc Sở;
- Lưu: VT,TTCNTTLT.

GIÁM ĐỐC

SỞ TÀI NGUYÊN VÀ MÔI TRƯỜNG TỈNH BÌNH DƯƠNG

Ngô Quang Sự

UBND TỈNH BÌNH DƯƠNG
SỞ TÀI NGUYÊN VÀ MÔI TRƯỜNG

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

QUY CHẾ

Quy chế đảm bảo an toàn, an ninh hệ thống thông tin Sở Tài nguyên và Môi trường tỉnh Bình Dương

(Ban hành kèm theo Quyết định số 215 /QĐ-STNMT ngày 07/3 /2022 của Giám đốc Sở Tài nguyên và Môi trường tỉnh Bình Dương)

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, an ninh thông tin mạng trong các hoạt động của Sở Tài nguyên và Môi trường và các đơn vị trực thuộc Sở.

2. Đối tượng áp dụng:

a) Các phòng, đơn vị thuộc Sở Tài nguyên và Môi trường (sau đây gọi là đơn vị trực thuộc Sở) và cán bộ, công chức, viên chức và người lao động thuộc các đơn vị trực thuộc Sở.

b) Cơ quan, tổ chức, cá nhân có kết nối vào hệ thống mạng của Sở Tài nguyên và Môi trường.

c) Cơ quan, tổ chức, cá nhân cung cấp dịch vụ công nghệ thông tin và an toàn thông tin mạng cho các đơn vị trực thuộc Sở.

Điều 2. Giải thích từ ngữ

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

1. *Báo đảm an toàn thông tin mức vật lý* là việc bảo vệ hệ thống hạ tầng kỹ thuật, phần mềm, ứng dụng và cơ sở dữ liệu khỏi các mối nguy hiểm vật lý (như: cháy, nổ; nhiệt độ, độ ẩm ngoài mức cho phép; thiên tai; mất điện; tác động cơ học) có thể gây ảnh hưởng đến hoạt động của hệ thống;

2. *Không gian mạng* là mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, bao gồm mạng viễn thông, mạng internet, hệ thống máy tính, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, là nơi con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian;

3. *Hạ tầng kỹ thuật* là tập hợp các thiết bị tính toán, lưu trữ, thiết bị ngoại vi, thiết bị kết nối mạng, thiết bị phụ trợ, đường truyền, mạng nội bộ, mạng diện rộng;

4. *Trang thông tin điện tử* là trang thông tin hoặc tập hợp trang thông tin trên môi trường mạng phục vụ cho việc cung cấp, trao đổi thông tin;

5. *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.

Điều 3. Nguyên tắc bảo đảm an toàn, an ninh thông tin mạng

1. Bảo đảm an toàn, an ninh thông tin là yêu cầu bắt buộc, thường xuyên, liên tục, có tính xuyên suốt quá trình liên quan đến thông tin và thiết kế, xây dựng, vận hành, nâng cấp, hủy bỏ hệ thống thông tin. Bảo đảm an toàn, an ninh thông tin tuân thủ các nguyên tắc chung quy định tại Điều 4 Luật An toàn thông tin mạng và Điều 4 Nghị định số 85/2016/ND-CP.

2. Các đơn vị trực thuộc Sở có trách nhiệm bảo đảm an toàn, an ninh thông tin mạng của đơn vị mình; bố trí nhân sự chuyên trách chịu trách nhiệm bảo đảm an toàn, an ninh thông tin mạng; xác định rõ quyền hạn, trách nhiệm của Thủ trưởng đơn vị, từng bộ phận, cá nhân trong đơn vị đối với công tác bảo đảm an toàn, an ninh thông tin mạng.

3. Cán bộ, công chức, viên chức và người lao động trong các đơn vị trực thuộc Sở có trách nhiệm bảo đảm an toàn, an ninh thông tin trong phạm vi xử lý công việc của mình theo quy định của Nhà nước và của Sở Tài nguyên và Môi trường.

4. Các nhiệm vụ, dự án ứng dụng công nghệ thông tin phải có nội dung liên quan đến an toàn, an ninh thông tin và phương án bảo đảm an toàn hệ thống thông tin trước khi được phê duyệt.

5. Thông tin mật, thông tin thuộc Danh mục bí mật nhà nước ngành tài nguyên môi trường phải được bảo vệ theo quy định của Nhà nước, quy định của Sở Tài nguyên và Môi trường về công tác bảo vệ bí mật nhà nước và các nội dung tương ứng trong Quy chế này.

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

Điều 4. Các hành vi bị nghiêm cấm

1. Các hành vi bị nghiêm cấm quy định tại Điều 7 Luật An toàn thông tin mạng.

2. Tự ý đấu nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập mạng không dây của cá nhân vào mạng nội bộ; tự ý thay đổi, gỡ bỏ biện pháp an toàn thông tin cài đặt trên thiết bị công nghệ thông tin phục vụ công việc; tự ý thay thế, lắp mới, tráo đổi thành phần của máy tính phục vụ công việc.

3. Tạo ra, cài đặt, phát tán phần mềm độc hại.

4. Cản trở hoạt động cung cấp dịch vụ của hệ thống thông tin; ngăn chặn việc truy nhập đến thông tin của cơ quan, cá nhân khác trên môi trường mạng.

5. Bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã và thông tin của cơ quan, cá nhân khác trên môi trường mạng.

6. Các hành vi khác làm mất an toàn, bí mật thông tin của cơ quan, cá nhân khác được trao đổi, truyền đưa, lưu trữ trên môi trường mạng, mở tập tin trực tiếp trên máy chủ.

Chương II

QUY ĐỊNH BẢO ĐẢM AN TOÀN, AN NINH THÔNG TIN MẠNG

Điều 5. Quản lý trang thiết bị công nghệ thông tin

1. Giao, gắn trách nhiệm cho cá nhân hoặc tập thể quản lý, sử dụng trang thiết bị công nghệ thông tin.

2. Quy định các quy tắc sử dụng, giữ gìn bảo vệ trang thiết bị công nghệ thông tin trong các trường hợp như: mang ra khỏi cơ quan, trang thiết bị công nghệ thông tin liên quan đến dữ liệu nhạy cảm, cài đặt và cấu hình.

3. Trang thiết bị công nghệ thông tin có lưu trữ dữ liệu liên quan đến dữ liệu tài nguyên và môi trường, dữ liệu hồ sơ mật thì khi thay đổi mục đích sử dụng hoặc thanh lý, đơn vị phải thực hiện các biện pháp xóa, tiêu hủy dữ liệu đó đảm bảo không có khả năng phục hồi. Trường hợp không thể tiêu hủy được dữ liệu, đơn vị phải thực hiện tiêu hủy phần lưu trữ dữ liệu trên trang thiết bị công nghệ thông tin đó. Quy trình hủy bỏ thiết bị công nghệ thông tin tại phụ lục IV Quy chế này.

4. Thiết bị tính toán có bộ phận lưu trữ hoặc thiết bị lưu trữ khi mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài hoặc ngừng sử dụng phải tháo bộ phận lưu trữ khỏi thiết bị hoặc xóa thông tin, dữ liệu lưu trữ trên thiết bị (trừ trường hợp để khôi phục dữ liệu).

5. Thực hiện bảo trì, bảo dưỡng hạ tầng kỹ thuật công nghệ thông tin theo Phụ lục II của Quy chế này (bao gồm thiết bị đang hoạt động và thiết bị dự phòng).

Điều 6. Quản lý cán bộ, công chức, viên chức và người lao động

1. Các đơn vị trực thuộc Sở phải xây dựng các yêu cầu, trách nhiệm bảo đảm an toàn, an ninh thông tin đối với từng vị trí công việc. Sau khi tuyển dụng, tiếp nhận nhân sự mới, đơn vị phải có trách nhiệm phổ biến cho nhân sự mới các quy định về bảo đảm an toàn, an ninh thông tin tại đơn vị; đối với các vị trí tiếp xúc, quản lý các thông tin, dữ liệu quan trọng hoặc quản trị các hệ thống thông tin quan trọng, đơn vị phải yêu cầu nhân sự mới cam kết bảo mật thông tin bằng văn bản hoặc cam kết trong hợp đồng làm việc, hợp đồng lao động.

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

3. Xây dựng quy trình cấp mới, quản lý và thu hồi tài khoản, phân quyền truy

cập các hệ thống thông tin và tất cả các tài sản liên quan đến hệ thống thông tin đối với các cá nhân do đơn vị quản lý.

4. Khi cán bộ, công chức, viên chức và người lao động chấm dứt hoặc thay đổi công việc, cơ quan, đơn vị phải:

a) Xác định rõ trách nhiệm của cán bộ, nhân viên và các bên liên quan trong quản lý, sử dụng các tài sản công nghệ thông tin được giao.

b) Lập biên bản bàn giao tài sản công nghệ thông tin.

c) Thay đổi hoặc thu hồi quyền truy cập các hệ thống thông tin.

Điều 7. Bảo đảm an toàn hệ thống công nghệ thông tin

1. Bảo đảm an toàn thông tin đối với trung tâm dữ liệu/phòng máy chủ

a) Các thiết bị kết nối mạng, thiết bị bảo mật quan trọng như tường lửa (firewall), thiết bị định tuyến (router), hệ thống máy chủ, hệ thống lưu trữ SAN, NAS, ... phải được đặt trong trung tâm dữ liệu/phòng máy chủ và phải được thiết lập cơ chế bảo vệ, theo dõi phát hiện xâm nhập và biện pháp kiểm soát truy nhập, kết nối vật lý phù hợp với từng khu vực: máy chủ và hệ thống lưu trữ; tủ mạng và đầu nối; thiết bị nguồn điện và dự phòng điện khẩn cấp; vận hành, kiểm soát, quản trị hệ thống. Đơn vị chủ quản trung tâm dữ liệu/phòng máy chủ có trách nhiệm xây dựng nội quy hoặc hướng dẫn làm việc khu vực này.

b) Trung tâm dữ liệu/phòng máy chủ là khu vực hạn chế tiếp cận và được lắp đặt hệ thống camera giám sát. Chỉ những cá nhân có quyền, nhiệm vụ theo quy định của thủ trưởng đơn vị mới được phép vào trung tâm dữ liệu/phòng máy chủ. Quá trình vào, ra phòng máy chủ phải được ghi nhận vào nhật ký quản lý trung tâm dữ liệu/phòng máy chủ theo Phụ lục III (Nhật ký ra/vào phòng máy chủ) Quy chế này.

c) Trung tâm dữ liệu/phòng máy chủ phải được trang bị hệ thống lưu điện đủ công suất và duy trì thời gian hoạt động của các máy chủ ít nhất 15 phút sau khi có sự cố mất điện.

d) Trung tâm dữ liệu/phòng máy chủ phải có hệ thống giám sát nhiệt độ, độ ẩm để đảm bảo môi trường vận hành; hệ thống cảnh báo cháy, hệ thống chữa cháy tự động bằng khí, thiết bị phòng cháy, chữa cháy khẩn cấp; hệ thống cảnh báo hệ thống nguồn điện; hệ thống chống sét lan truyền. Tất cả các cảnh báo này phải được gửi đến các cá nhân có trách nhiệm qua tin nhắn hoặc thư điện tử. Đơn vị phải cử cán bộ thường xuyên giám sát thiết bị, hạ tầng của trung tâm dữ liệu/phòng máy chủ.

e) Phòng máy chủ chỉ được đặt các thiết bị đang hoạt động phục vụ vận hành hệ thống, tuyệt đối không đặt các thiết bị khác: Thiết bị hỏng, thiết bị chờ thanh lý, thanh hủy, tài liệu, vật tư, các vật dụng dễ cháy nổ,…

2. Bảo đảm an toàn thông tin cho phần mềm hệ thống trung tâm dữ liệu/phòng máy chủ:

a) Cài đặt địa chỉ mạng xác định (IP tĩnh).

b) Máy chủ phải được đặt tên trong hệ thống, tên đặt phải có cấu trúc rõ ràng, dễ quản lý.

c) Không được cài đặt các bộ phần mềm/ứng dụng văn phòng như: Microsoft Office, LibreOffice, Apache OpenOffice, … để đọc tập tin trực tiếp trên máy chủ. Chỉ sử dụng các loại trình duyệt mặc định do hệ thống cung cấp. Nghiêm cấm sử dụng máy chủ làm phương tiện cài đặt các ứng dụng trao đổi công việc như: zalo, mail, nghe nhạc, duyệt web.

d) Tháo/gỡ toàn bộ các ứng dụng/phần mềm không cần thiết hoặc không dùng cho việc vận hành dịch vụ, hệ thống.

e) Máy chủ phải luôn bật tính năng tường lửa (firewall).

g) Khi phát hiện hệ thống máy chủ 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 4 bước cơ bản sau:

Bước 1: Ngắt kết nối máy chủ ra khỏi mạng.

Bước 2: Sao chép logfile và toàn bộ dữ liệu của hệ thống ra thiết bị lưu trữ (phục vụ cho công tác phân tích).

Bước 3: Khôi phục hệ thống bằng cách chuyển dữ liệu dự phòng (backup) mới nhất để hệ thống hoạt động.

Bước 4: Thông báo về Trung tâm Công nghệ thông tin – Lưu trữ tài nguyên và môi trường để được hướng dẫn, hỗ trợ.

3. Bảo đảm an toàn thông tin khi sử dụng máy tính

a) Cá nhân chỉ cài đặt phần mềm hợp lệ và thuộc danh mục phần mềm được phép sử dụng do cơ quan có thẩm quyền ban hành trên máy tính được đơn vị cấp cho mình; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm khi chưa có sự đồng ý của bộ phận chuyên trách về công nghệ thông tin; thường xuyên cập nhật phần mềm và hệ điều hành.

b) Cài đặt phần mềm xử lý phần mềm độc hại và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm; khi phát hiện bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại trên máy tính phải tắt máy và báo trực tiếp cho bộ phận chuyên trách về công nghệ thông tin để được xử lý kịp thời.

c) Chỉ truy nhập vào các trang/cổng thông tin điện tử, ứng dụng trực tuyến tin cậy và các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình; có trách nhiệm bảo mật tài khoản truy nhập thông tin, không chia sẻ mật khẩu, thông tin cá nhân với người khác.

4. Bảo đảm an toàn thông tin đối với hệ thống mạng máy tính

a) Hệ thống mạng nội bộ (LAN) phải được thiết kế phân vùng theo chức năng

cơ bản (theo các chính sách an toàn thông tin riêng), bao gồm: vùng mạng người dùng; vùng mạng kết nối hệ thống ra bên ngoài Internet và các mạng khác; vùng mạng máy chủ công cộng; vùng mạng máy chủ nội bộ; vùng mạng máy chủ quản trị. Dữ liệu trao đổi giữa các vùng mạng phải được quản lý, giám sát bởi hệ thống các thiết bị mạng, thiết bị bảo mật.

b) Đơn vị trực thuộc Sở tham gia kết nối, sử dụng hệ thống mạng diện rộng (WAN) của Sở Tài nguyên và Môi trường có trách nhiệm bảo đảm an toàn thông tin đối với hệ thống mạng nội bộ và các thiết bị của mình khi thực hiện kết nối vào mạng diện rộng; Thông báo sự cố hoặc các hành vi phá hoại, xâm nhập về Trung tâm Công nghệ thông tin và Lưu trữ tài nguyên môi trường để xử lý; Định kỳ sao lưu thông tin, dữ liệu dùng chung lưu trữ trên mạng diện rộng; Không được tiết lộ phương thức (tên đăng ký, mật khẩu, tiện ích, tệp hỗ trợ và các cách thức khác) để truy nhập vào hệ thống mạng diện rộng cho tổ chức, cá nhân khác; Không được tìm cách truy nhập dưới bất cứ hình thức nào vào các khu vực không được phép truy nhập.

c) Các hệ thống thông tin phải áp dụng các biện pháp kỹ thuật cần thiết bảo đảm an toàn thông tin trong hoạt động kết nối Internet, tối thiểu đáp ứng các yêu cầu sau: có hệ thống tường lửa và hệ thống bảo vệ truy nhập Internet, đáp ứng nhu cầu kết nối đồng thời, hỗ trợ các công nghệ mạng riêng ảo thông dụng và có phần cứng mã hóa tích hợp để tăng tốc độ mã hóa dữ liệu và có khả năng bảo vệ hệ thống trước các loại tấn công từ chối dịch vụ (DDoS); Lọc bỏ, không cho phép truy nhập các trang tin có nghi ngờ chứa mã độc hoặc các nội dung không phù hợp.

d) Các đường truyền dữ liệu, đường truyền Internet và các hệ thống dây dẫn các mạng LAN, WAN phải được lắp đặt trong ống, máng che đậy kín, hạn chế khả năng tiếp cận trái phép. Ngắt kết nối cổng Ethernet không sử dụng, đặc biệt là ở khu vực làm việc chung của các cơ quan, đơn vị.

e) Việc kết nối giữa máy trạm với các hệ thống thông tin ngành tài nguyên và môi trường thông qua đường truyền mạng số liệu chuyên dùng hoặc đường mạng riêng ảo (VPN/FotiClientVPN).

5. Quản lý tài khoản truy cập

a) Cá nhân sử dụng hệ thống thông tin được cấp và sử dụng tài khoản truy nhập với định danh duy nhất gắn với cá nhân đó. Các hệ thống thông tin dùng chung của Sở sử dụng cơ chế đăng nhập một lần, chung một tài khoản truy nhập và mật khẩu.

b) Trường hợp cá nhân thay đổi vị trí công tác, chuyển công tác, thôi việc hoặc nghỉ hưu, trong vòng không quá 05 ngày làm việc, đơn vị quản lý cá nhân đó phải thông báo cơ quan, đơn vị chủ quản hệ thống thông tin để điều chỉnh, thu hồi, hủy bỏ các quyền sử dụng đối với hệ thống thông tin.

c) Tài khoản quản trị hệ thống (mạng, hệ điều hành, thiết bị kết nối mạng, phần mềm, ứng dụng, cơ sở dữ liệu) phải tách biệt với tài khoản truy nhập của người sử dụng thông thường. Tài khoản hệ thống phải được giao đích danh cá nhân làm công

tác quản trị. Hạn chế dùng chung tài khoản quản trị.

d) Khi có yêu cầu khóa quyền truy cập hệ thống thông tin của tài khoản đang hoạt động, lãnh đạo đơn vị phải yêu cầu bằng văn bản gửi đơn vị chủ quản hệ thống thông tin. Đơn vị chủ quản hệ thống thông tin thực hiện việc khóa quyền truy cập của tài khoản. Đơn vị chủ quản hệ thống thông tin có quyền khóa quyền truy cập của tài khoản trong trường hợp tài khoản đó thực hiện các hành vi tấn công hoặc để xảy ra vấn đề mất an toàn, an ninh thông tin.

6. Bảo đảm an toàn thông tin mức ứng dụng

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

b) Phần mềm, ứng dụng phải đáp ứng các yêu cầu sau: cấu hình phần mềm, ứng dụng để xác thực người sử dụng; giới hạn số lần đăng nhập sai liên tiếp; giới hạn thời gian để chờ đóng phiên kết nối; mã hóa thông tin xác thực trên hệ thống; không khuyến khích việc đăng nhập tự động.

c) Thiết lập, phân quyền truy nhập, quản trị, sử dụng tài nguyên khác nhau của phần mềm, ứng dụng với người sử dụng/nhóm người sử dụng có chức năng, yêu cầu nghiệp vụ khác nhau; tách biệt cổng giao tiếp quản trị phần mềm ứng dụng với cổng giao tiếp cung cấp dịch vụ; đóng các cổng giao tiếp không sử dụng.

d) Chỉ cho phép sử dụng các giao thức mạng có hỗ trợ chức năng mã hóa thông tin như SSH, SSL, VPN hoặc tương đương khi truy nhập, quản trị phần mềm, ứng dụng từ xa trên môi trường mạng; hạn chế truy cập đến mã nguồn của phần mềm, ứng dụng và phải đặt mã nguồn trong môi trường an toàn do bộ phận chuyên trách công nghệ thông tin quản lý.

đ) Ghi và lưu giữ bản ghi nhật ký hệ thống của phần mềm, ứng dụng trong khoảng thời gian tối thiểu 03 tháng với những thông tin cơ bản: thời gian, địa chỉ, tài khoản (nếu có), nội dung truy nhập và sử dụng phần mềm, ứng dụng; các lỗi phát sinh trong quá trình hoạt động; thông tin đăng nhập khi quản trị.

e) Phần mềm, ứng dụng cần được kiểm tra phát hiện và khắc phục các điểm yếu về an toàn, an ninh thông tin trước khi đưa vào sử dụng và trong quá trình sử dụng.

f) Thực hiện quy trình kiểm soát cài đặt, cập nhật, vá lỗi bảo mật phần mềm, ứng dụng trên các máy chủ, máy tính cá nhân, thiết bị kết nối mạng đang hoạt động thuộc hệ thống mạng nội bộ.

7. Bảo đảm an toàn thông tin mức dữ liệu

a) Thực hiện bảo vệ thông tin, dữ liệu liên quan đến hoạt động công vụ, thông tin có nội dung quan trọng, nhạy cảm hoặc không phải là thông tin công khai bằng các biện pháp như: thiết lập phương án bảo đảm tính bí mật, nguyên vẹn và khả dụng của thông tin, dữ liệu; mã hóa thông tin, dữ liệu khi lưu trữ trên hệ thống/thiết bị lưu

trữ dữ liệu di động; sử dụng chữ ký số để xác thực và bảo mật thông tin, dữ liệu.

b) Triển khai hệ thống/phương tiện lưu trữ độc lập với hệ thống lưu trữ trên các máy chủ dịch vụ để sao lưu dự phòng; phân loại và quản lý thông tin, dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau; thực hiện sao lưu dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

c) Bố trí máy tính riêng không kết nối mạng, đặt mật khẩu, mã hóa dữ liệu và các biện pháp bảo mật khác bảo đảm an toàn thông tin để soạn thảo, lưu trữ dữ liệu, thông tin và tài liệu quan trọng ở các mức độ mật, tuyệt mật, tối mật.

d) Các đơn vị trực thuộc Sở phải thường xuyên kiểm tra, giám sát các hoạt động chia sẻ, gửi, nhận thông tin, dữ liệu trong hoạt động nội bộ của mình; khuyến cáo việc chia sẻ, gửi, nhận thông tin trên môi trường mạng cần phải sử dụng mật khẩu để bảo vệ thông tin.

đ) Đối với hoạt động trao đổi thông tin, dữ liệu với bên ngoài, đơn vị và cá nhân thực hiện trao đổi thông tin, dữ liệu ra bên ngoài cam kết và có biện pháp bảo mật thông tin, dữ liệu được trao đổi. Giao dịch trực tuyến phải được truyền đầy đủ, đúng địa chỉ, tránh bị sửa đổi, tiết lộ hoặc nhân bản một cách trái phép; sử dụng các cơ chế xác thực mạnh, chữ ký số khi tham gia giao dịch, sử dụng các giao thức truyền thông an toàn.

Điều 8. Bảo đảm an toàn thông tin khi tiếp nhận, phát triển, vận hành và bảo trì hệ thống thông tin

1. Khi thực hiện nâng cấp, mở rộng, thay thế một phần hệ thống thông tin, phải rà soát cấp độ, phương án bảo đảm an toàn của hệ thống thông tin và thực hiện điều chỉnh, bổ sung hoặc thay mới hồ sơ đề xuất cấp độ trong trường hợp cần thiết.

2. Khi tiếp nhận, phát triển, nâng cấp, bảo trì hệ thống thông tin, đơn vị phải tiến hành phân tích, xác định rủi ro có thể xảy ra, đánh giá phạm vi tác động và phải chuẩn bị các biện pháp hạn chế, loại trừ các rủi ro này và yêu cầu các bên cung cấp, thi công, các cá nhân liên quan thực hiện.

3. Trong quá trình vận hành hệ thống thông tin, đơn vị chủ quản hệ thống thông tin cần thực hiện đánh giá, phân loại hệ thống thông tin theo cấp độ; triển khai phương án bảo đảm an toàn hệ thống thông tin đáp ứng yêu cầu cơ bản trong tiêu chuẩn, quy chuẩn kỹ thuật về bảo đảm an toàn hệ thống thông tin theo cấp độ; thường xuyên kiểm tra, giám sát an toàn hệ thống thông tin; tuân thủ quy trình vận hành, quy trình xử lý sự cố đã xây dựng; ghi lại và lưu trữ đầy đủ thông tin nhật ký hệ thống để phục vụ quản lý, kiểm soát thông tin.

4. Đối tác phát triển phần mềm ứng dụng cho các đơn vị trực thuộc Sở có trách nhiệm bảo đảm an toàn thông tin cho công tác phát triển, vận hành, bảo hành, bảo trì phần mềm, ứng dụng, tránh lộ, lọt mã nguồn và dữ liệu, tài liệu thiết kế, quản trị hệ thống mà đối tác đang xử lý ra bên ngoài.

Điều 9. Quy định về kiểm tra, báo cáo định kỳ

1. Hệ thống mạng phải được kiểm tra đánh giá an toàn thông tin định kỳ tối thiểu 1 lần/năm. Kết quả kiểm tra phải đưa vào báo cáo tình hình ứng dụng công nghệ thông tin vào cuối năm.

2. Các chức năng hệ thống phải được giám sát trạng thái hoạt động, thông tin phải được ghi nhận và được ký xác nhận bởi người phụ trách quản lý.

3. Tổng hợp, xây dựng báo cáo trong quá trình duy trì vận hành hệ thống. Định kỳ hàng năm gửi báo cáo về Trung tâm Công nghệ thông tin – Lưu trữ tài nguyên và môi trường để tổng hợp báo cáo lãnh đạo Sở Tài nguyên và Môi trường.

CHƯƠNG III
TRÁCH NHIỆM CỦA CÁC TỔ CHỨC CÓ LIÊN QUAN

Điều 10. Trách nhiệm của thủ trưởng các phòng, đơn vị trực thuộc

1. Tổ chức triển khai thực hiện Quy chế này tại đơn vị và thực hiện các trách nhiệm được giao tại Quy chế này.

2. Xây dựng, triển khai Quy chế bảo đảm an toàn, an ninh thông tin tại đơn vị bảo đảm phù hợp với Quy chế này và các yêu cầu cụ thể của đơn vị.

3. Thực hiện việc quản lý trang thiết bị công nghệ thông tin và cán bộ, công chức, viên chức, người lao động theo Điều 5 và Điều 6 của Quy chế này.

4. Triển khai các giải pháp bảo đảm an toàn thông tin đối với hạ tầng kỹ thuật, hệ thống thông tin và cơ sở dữ liệu được giao quản lý, vận hành. Đảm bảo an toàn, an ninh thông tin cho các hệ thống thông tin, cơ sở dữ liệu dùng chung của Sở.

5. Tạo điều kiện để bồi dưỡng, đào tạo, tăng cường năng lực cho bộ phận chuyên trách/kiêm nhiệm về công nghệ thông tin và cá nhân làm công tác công nghệ thông tin.

Điều 11. Trách nhiệm của Trung tâm Công nghệ thông tin – Lưu trữ tài nguyên và môi trường.

1. Tổ chức phổ biến, triển khai, hướng dẫn và kiểm tra việc thực hiện Quy chế này trong phạm vi Sở Tài nguyên và Môi trường; định kỳ báo cáo Lãnh Sở về thông tin, tình hình thực hiện.

2. Tham mưu triển khai các giải pháp bảo đảm an toàn thông tin đối với hạ tầng kỹ thuật, hệ thống thông tin và cơ sở dữ liệu dùng chung của Sở.

3. Tổ chức truyền thông, nâng cao nhận thức về bảo đảm an toàn thông tin với triển khai ứng dụng công nghệ thông tin.

Điều 12. Trách nhiệm của cá nhân

1. Thủ trưởng đơn vị thuộc đối tượng áp dụng của Quy chế này có trách nhiệm: phổ biến tới từng cán bộ, công chức, viên chức, người lao động của đơn vị; thường

xuyên kiểm tra việc thực hiện Quy chế này tại đơn vị; chịu trách nhiệm trước pháp luật và Lãnh đạo Sở Tài nguyên và Môi trường về các vi phạm, thất thoát thông tin, dữ liệu mật thuộc phạm vi quản lý của đơn vị do không tổ chức, chỉ đạo, kiểm tra cán bộ của đơn vị thực hiện đúng quy định.

2. Cán bộ, công chức, viên chức, người lao động của Sở Tài nguyên và Môi trường, các đơn vị trực thuộc Sở và các đơn vị khác thuộc đối tượng áp dụng của quy định có trách nhiệm: tuân thủ Quy chế; thông báo các vấn đề bất thường liên quan tới an toàn thông tin cho đơn vị, bộ phận chuyên trách về an toàn thông tin mạng của đơn vị; chịu trách nhiệm trước pháp luật và Lãnh đạo đơn vị về các vi phạm, thất thoát dữ liệu mật của ngành tài nguyên môi trường do không tuân thủ Quy chế.

CHƯƠNG IV
TỔ CHỨC THỰC HIỆN

Điều 13. Kinh phí thực hiện

Kinh phí bảo đảm an toàn, an ninh thông tin mạng được chi từ nguồn ngân sách nhà nước theo phân cấp ngân sách nhà nước hiện hành và các nguồn kinh phí hợp pháp khác.

Điều 14. Công tác kiểm tra

1. Các đơn vị trực thuộc phải thường xuyên kiểm tra, theo dõi và đánh giá công tác bảo đảm an toàn, an ninh thông tin mạng tại cơ quan, đơn vị mình, coi đây là nhiệm vụ trọng tâm của đơn vị.

2. Giao Trung tâm Công nghệ thông tin – Lưu trữ tài nguyên và môi trường kiểm tra và báo cáo Lãnh đạo Sở việc thực hiện Quy chế này.

Điều 15. Chế độ báo cáo

1. Báo cáo định kỳ:

a) Báo cáo an toàn thông tin định kỳ hàng năm gồm các nội dung quy định tại khoản 3 Điều 17 Thông tư 03/2017/TT-BTTTT.

b) Báo cáo hoạt động giám sát của chủ quản hệ thống thông tin định kỳ 6 tháng theo mẫu tại Phụ lục II Thông tư 31/2017/TT-BTTTT.

2. Báo cáo đột xuất: Báo cáo về công tác khắc phục mã độc, lỗ hổng, điểm yếu, triển khai cảnh báo an toàn thông tin và các báo cáo đột xuất khác theo yêu cầu của các cơ quan quản lý nhà nước về an toàn thông tin.

3. Trách nhiệm lập, phê duyệt báo cáo

a) Các đơn vị trực thuộc Sở chịu trách nhiệm:

- Lập báo cáo an toàn thông tin theo quy định tại điểm a khoản 1 điều này, gửi Trung tâm Công nghệ thông tin – Lưu trữ tài nguyên và môi trường trước ngày 15

tháng 11 hàng năm.

- Lập báo cáo hoạt động giám sát của chủ quản hệ thống thông tin theo quy định tại điểm b khoản 1 điều này, gửi Trung tâm Công nghệ thông tin – Lưu trữ tài nguyên và môi trường trước ngày 15 tháng 6 và 15 tháng 12 hàng năm.

- Báo cáo đột xuất theo hướng dẫn của Trung tâm Công nghệ thông tin – Lưu trữ tài nguyên và môi trường.

b) Trung tâm Công nghệ thông tin – Lưu trữ tài nguyên và môi trường chịu trách nhiệm tập hợp, tổng hợp báo cáo của các đơn vị, trình Sở phê duyệt, gửi các cơ quan quản lý nhà nước về an toàn thông tin.

Điều 16. Khen thưởng, kỷ luật

1. Trung tâm Công nghệ thông tin – Lưu trữ tài nguyên và môi trường phối hợp Văn phòng Sở tiến hành kiểm tra, đánh giá, xếp loại an toàn thông tin, trên cơ sở đó tham mưu, đề xuất Lãnh đạo Sở khen thưởng phòng, đơn vị và cá nhân thực hiện tốt Quy chế này hằng năm theo quy định.

2. Cơ quan, 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 Sở thì phải chịu trách nhiệm về những thiệt hại gây ra theo quy định của pháp luật.

3. Việc giải quyết khiếu nại, tố cáo và tranh chấp được thực hiện theo quy định liên quan của pháp luật.

Điều 17. Điều khoản thi hành

Trong quá trình thực hiện Quy chế này, nếu có phát sinh khó khăn, vướng mắc, các đơn vị phản ánh về Sở Tài nguyên và Môi trường thông qua Trung tâm Công nghệ thông tin – Lưu trữ tài nguyên và môi trường để tổng hợp, báo cáo Lãnh đạo Sở Tài nguyên và Môi trường xem xét sửa đổi, bổ sung Quy chế cho phù hợp./.

GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ TÀI NGUYÊN VÀ MÔI TRƯỜNG
TỈNH BÌNH DƯƠNG

Ngô Quang Sự

Phụ lục I

SỞ TÀI NGUYÊN VÀ MÔI TRƯỜNG
BÌNH DƯƠNG
<TÊN PHÒNG, ĐƠN VỊ>

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

Bình Dương, ngày tháng năm .....

PHIẾU ĐỀ NGHỊ
Về việc khắc phục sự cố máy tính, mạng

I. Phần đề nghị

Họ tên: .....

Phòng, đơn vị: .....

Mô tả sự cố: .....

.....

Đề nghị Trung tâm Công nghệ thông tin – Lưu trữ tài nguyên và môi trường cử người kiểm tra, hỗ trợ khắc phục sự cố.

Ngày .....tháng.....năm.....

Trưởng phòng, đơn vị

Ngày .....tháng.....năm .....

Người đề nghị

II. Phân công

Họ tên người được phân công: .....

Nội dung phân công: .....

Ngày..... tháng..... năm.....

Người phân công

III. Khắc phục sự cố

Phân loại sự cố: ☐ Mạng ☐ Thiết bị do phòng ban, đơn vị sử dụng

☐ Máy chủ ☐ Thiết bị thuộc tài sản riêng của đơn vị

Nguyên nhân: .....

Hướng khắc phục: .....

Thời gian hoàn thành: .....

Hồ sơ đính kèm: .....

Ngày .....tháng.....năm..... *Ngày .....tháng.....năm.....*

Xác nhận của phòng, đơn vị **Người thực hiện**

Phụ lục II

QUY TRÌNH BẢO TRÌ, BẢO DƯỠNG HỆ THỐNG THÔNG TIN

1. Sơ đồ quy trình bảo trì, bảo dưỡng hệ thống thông tin

	Tên Bước công việc		Mô tả
Bước 1	- Lập kế hoạch bảo dưỡng - Thông báo cho các bộ phận liên quan về lịch bảo dưỡng định kỳ	⟷	- Hệ thống danh sách và ghi chép thời gian bảo trì theo quy định của nhà sản xuất - Lên kế hoạch bảo dưỡng định kỳ (Thời gian, tên thiết bị, vịt trí đặt thiết bị, máy móc, nội dung bảo trì, đơn vị bảo trì, người giám sát)
Bước 2	Vệ sinh các thiết bị	⟷	- Ngắt điện của thiết bị - Dùng chổi quét nhỏ, làm sạch bụi bẩn tại tất cả các vị trí trong tủ điện
Bước 3	Kiểm tra các kết nối của các thiết bị ngoại vi, kết nối nguồn, kết nối mạng, kết nối hệ thống của các thiết bị;	⟷	- Dùng bút thử điện kiểm tra tín hiệu dây cáp điện - Dùng hợp kiểm tra tín hiệu mạng kiểm tra tín hiệu dây cáp mạng
Bước 4	Kiểm tra môi trường hoạt động, độ ẩm, nhiệt độ, hệ thống làm mát của hệ thống	⟷	Kiểm tra trạng thái điều hòa hoặc thiết bị tản nhiệt có đang hoạt động hay không, nhiệt độ trong phòng có phù hợp để đảm bảo thiết bị trong tình trạng hoạt động tốt nhất
Bước 5	Lấy bản ghi nhật ký hệ thống hoạt động (log dữ liệu), kiểm tra các đèn cảnh báo	⟷	- Thực hiện xuất nhật ký ra tập tin, lưu trữ vào thiết bị - Kiểm tra tín hiệu thông qua đèn trạng thái, xử lý các vấn đề phát sinh nếu không làm ảnh hưởng hệ thống.
Bước 6	Chạy các chương trình kiểm tra hiệu năng máy tính, máy chủ về trạng thái hoạt động của thiết bị	⟷	- Thực hiện kiểm tra công suất hoạt động của CPU, RAM, HDD - Ghi nhận dung lượng sử dụng so với tài nguyên sẵn có
Bước 7	Kiểm tra danh mục các phần mềm được phép chạy trên máy chủ và loại bỏ các phần mềm không được phép trên máy tính, máy chủ	⟷	Kiểm tra trạng thái điều hòa hoặc thiết bị tản nhiệt có đang hoạt động hay không, nhiệt độ trong phòng có phù hợp để đảm bảo thiết bị trong tình trạng hoạt động tốt nhất
Bước 8	Kiểm tra toàn bộ hệ thống và ghi nhận hiện trạng phục vụ cho các kỳ bảo dưỡng tiếp theo	⟷	- Tổng hợp số liệu và ghi chép vào sổ theo dõi - Báo cáo tình hình bảo trì, bảo dưỡng với lãnh đạo đơn vị
Bước 9	Thay thế/sửa chữa các thiết bị hỏng hóc phát sinh trong giai đoạn bảo dưỡng	⟷	Từ số liệu báo cáo tổng hợp thực hiện thay thế thiết bị đã bị hư hỏng
Bước 10	Nhật ký bảo dưỡng, thay thế Báo cáo bảo dưỡng, thay thế	⟷	Lưu trữ

2. Diễn giải Quy trình bảo trì, bảo dưỡng hệ thống thông tin

2.1. Các bước thực hiện:

Bước 1: Lập kế hoạch bảo dưỡng, thông báo cho các bộ phân liên quan về lịch bảo dưỡng định kỳ;

Bước 2: Vệ sinh các thiết bị;

Bước 3: Kiểm tra các kết nối của các thiết bị ngoại vi, kết nối nguồn, kết nối mạng, kết nối hệ thống của các thiết bị;

Bước 4: Kiểm tra môi trường hoạt động, độ ẩm, nhiệt độ, hệ thống làm mát của hệ thống;

Bước 5: Lấy bản ghi nhật ký hệ thống hoạt động (log dữ liệu), kiểm tra các đèn cảnh báo;

Bước 6: Chạy các chương trình kiểm tra hiệu năng máy tính, máy chủ về trạng thái hoạt động của thiết bị;

Bước 7: Kiểm tra danh mục các phần mềm được phép chạy trên máy chủ và loại bỏ các phần mềm không được phép trên máy tính, máy chủ;

Bước 8: Kiểm tra toàn bộ hệ thống và ghi nhận hiện trạng phục vụ cho các kỳ bảo dưỡng tiếp theo;

Bước 9: Thay thế/sửa chữa các thiết bị hỏng hóc phát sinh trong giai đoạn bảo dưỡng.

2.2. Sản phẩm

Nhật ký bảo dưỡng, thay thế.

Báo cáo bảo dưỡng, thay thế.

Phụ lục III

NHẬT KÝ RA/VÀO PHÒNG MÁY CHỦ

TT	Họ tên người ra/vào	Thời gian ra/vào	Nội dung làm việc	Ký tên	Cán bộ quản trị Ký xác nhận (Ghi rõ họ tên)
	Nguyễn Văn A	Ngày: …/…/…. Từ: …. Đến: …			
1	Nguyễn Văn A	Ngày: 20/01/2021 Từ: 8h30 Đến: 16h30	Bàn giao thiết bị máy chủ: - 4 ổ cứng - 16 cây RAM hiện SAMSUNG		
..					

Phụ lục IV

QUY TRÌNH HỦY BỎ THIẾT BỊ CÔNG NGHỆ THÔNG TIN

Trách nhiệm	Nội dung quy trình	Mô tả, biểu mẫu
Lãnh đạo đơn vị	Quy định trách nhiệm quản lý thiết bị CNTT	- Lãnh đạo phòng, đơn vị phân công trách nhiệm quản lý thiết bị CNTT của đơn vị cho cá nhân cụ thể. - Quy định thời gian kiểm tra, đánh giá, và ghi chép hoạt động của thiết bị. - Tiếp nhận bàn giao sổ sách và số lượng thiết bị CNTT từ đơn vị cung cấp hoặc cán bộ quản lý thiết bị trước đó bao gồm: Số lượng, tình trạng, vị trí, người sử dụng
Cán bộ quản lý tài sản của đơn vị	Quản lý, lập danh sách thiết bị cần	- Quản lý và theo dõi hồ sơ lưu trữ đối với từng thiết bị - Lập danh sách thiết bị CNTT cần hủy báo về bộ phận CNTT
Bộ phận CNTT	Đánh giá thực trạng thiết bị, lập biên bản xác định hư	- Xác định thực trạng thiết bị: Cấu hình thiết bị, thời gian sử dụng, tình trạng hỏng hóc. - Kiểm tra tình trạng máy, nếu không còn khả năng sửa chữa hoặc nâng cấp thì kiểm tra các bộ phận của máy còn sử dụng được lập biên bản thu hồi các bị để tái sử dụng.
Cán bộ quản lý tài sản của đơn vị	Thông báo cho phòng	- Làm công văn thông báo danh sách thiết bị cần hủy kèm các biên bản thu hồi các thiết bị để tái sử dụng