UBND TỈNH BÌNH ĐỊNH
SỞ TÀI CHÍNH

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

QUY CHẾ
BẢO ĐẢM AN TOÀN, AN NINH THÔNG TIN MẠNG CỦA SỞ TÀI CHÍNH BÌNH ĐỊNH

(Ban hành kèm theo Quyết định số 369 /QĐ-STC ngày 09 tháng 12 năm 2019 của Giám đốc Sở Tài chính Bình Định)

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 chính Bình Định

2. Đối tượng áp dụng:

a) Cán bộ, công chức và người lao động của Sở Tài chính Bình Định

b) Cơ quan, tổ chức, cá nhân có kết nối vào hệ thống mạng của Sở Tài chính Bình Định.

Điều 2. Giải thích từ ngữ

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

1. "An toàn thông tin mạng" là sự bảo vệ thông tin số và các hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

2. "An ninh thông tin mạng" là việc bảo đảm thông tin trên mạng không gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội, bí mật nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân.

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. "Cổng thông tin điện tử" là điểm truy nhập duy nhất của cơ quan, đơn vị trên môi trường mạng, liên kết, tích hợp các kênh thông tin, các dịch vụ và các ứng dụng mà qua đó người dùng có thể khai thác, sử dụng và cá nhân hóa việc hiển thị thông tin;

6. "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;

7. "Mạng LAN" là hệ thống mạng nội bộ bao gồm mạng dây và mạng không dây.

8. "Dữ liệu nhạy cảm" là dữ liệu có thông tin mật, thông tin lưu hành nội bộ của đơn vị hoặc do đơn vị quản lý, nếu lộ lọt ra ngoài sẽ gây ảnh hưởng xấu đến danh tiếng, tài chính và hoạt động của đơn vị.

9. "Kết nối Internet": Kết nối mạng tới hệ thống mạng Internet nhằm cung cấp khả năng truy cập Internet hoặc cung cấp thông tin, dịch vụ ra Internet.

10. “Phòng chống xâm nhập”: phát hiện, ngăn chặn các hoạt động vào, ra trên hệ thống thông tin được bảo vệ có dấu hiệu gây hại hoặc vi phạm chính sách an toàn mạng.

11. “Truy cập Internet”: Việc tiếp cận, khai thác, sử dụng thông tin, tài liệu, ứng dụng, dịch vụ trên Internet.

12. “Tường lửa”: Hệ thống cho phép hoặc không cho phép thiết lập kết nối mạng giữa thiết bị thuộc vùng mạng này và thiết bị thuộc vùng mạng khác theo chính sách an toàn mạng của đơn vị.

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/NĐ-CP.

2. Cán bộ, công chức và người lao động của Sở Tài chính có trách nhiệm bảo đảm an toàn, an ninh thông tin trong phạm vi xử lý công việc của mình theo quy định Pháp luật.

3. Thông tin mật, thông tin thuộc Danh mục bí mật nhà nước phải được bảo vệ theo quy định của Nhà nước, quy định của Sở Tài chính Bình Định về công tác bảo vệ bí mật nhà nước và các nội dung tương ứng trong Quy chế này.

4. 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 mà không có sự hướng dẫn hoặc đồng ý của đơn vị quản lý hệ thống thông tin; trên cùng một thiết bị thực hiện đồng thời truy cập vào mạng nội bộ và truy cập Internet bằng thiết bị kết nối Internet của cá nhân (modem quay số, USB 3G/4G, điện thoại di động, máy tính bảng, máy tính xách tay).

3. Tự ý thay đổi thông số mạng, 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.

4. Tạo ra, cài đặt, phát tán phần mềm độc hại gây ảnh hưởng đến hoạt động bình thường của hệ thống thông tin.

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.

7. Không được lợi dụng việc sử dụng Internet nhằm mục đích: Chống lại nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam, gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội; kích động bạo lực, đồi trụy, tệ nạn xã hội, mê tín dị đoan; phá hoại thuần phong mỹ tục của dân tộc.

8. Không được chơi các trò chơi trực tuyến (game online) hoặc các trò chơi khác trên Internet trong giờ làm việc, không được truy cập hoặc tải các trang Website có nội dung đồi trụy, phản động, các chương trình không rõ nguồn gốc, bẻ khóa…

9. Khi sử dụng hệ thống thư điện tử (Email) không được kích chuột vào bất cứ thư điện tử, tệp đính kèm, đường link, thư rác, thư quảng cáo nào không rõ nguồn gốc và không xác định được người gửi.

CHƯƠNG II
QUẢN LÝ, KHAI THÁC, SỬ DỤNG HỆ THỐNG THÔNG TIN

Điều 5. Quản lý, sử dụng thiết bị

1. Thiết bị tin học được trang bị tại các phòng chuyên môn là tài sản của Nhà nước, được quản lý, sử dụng theo quy định của Sở Tài chính và của Nhà nước. Các phòng chuyên môn, công chức và người lao động có trách nhiệm quản lý trang thiết bị tin học được giao.

2. Phòng Tài chính Doanh nghiệp-Tin học chịu trách nhiệm quản trị mạng, trực tiếp quản lý kỹ thuật và duy trì hoạt động của hệ thống thông tin của Sở; là đầu mối kết nối mạng LAN, mạng Internet, mạng dữ liệu chuyên dùng cho các phòng; kiểm tra hiện trạng, đề xuất sửa chữa hoặc mua mới các chủng loại thiết bị CNTT phù hợp, an toàn, bảo mật theo quy định về quản lý, sử dụng tài sản cơ quan.

3. Trang thiết bị công nghệ thông tin có lưu trữ dữ liệu nhạy cảm khi thay đổi mục đích sử dụng hoặc thanh lý… 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 cấu phần lưu trữ dữ liệu trên trang thiết bị công nghệ thông tin đó.

4. Trang thiết bị công nghệ thông tin có bộ phận lưu trữ dữ liệu hoặc thiết bị lưu trữ dữ liệu 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. Quy trình sửa chữa thiết bị tin học: Khi thiết bị tin học bị hư hỏng, người sử dụng lập phiếu, lãnh đạo phòng xác nhận gửi Phòng TCDN-TH kiểm tra và có ý kiến đề xuất gửi Văn phòng Sở (phụ lục 1), Văn phòng Sở báo cáo lãnh đạo Sở xem xét để quyết định sửa chữa hoặc mua mới thay thế.

6. Sử dụng thiết bị tin học: Không sử dụng thiết bị tin học của cơ quan vào việc riêng. Cán bộ sử dụng, vận hành thiết bị phải thực hiện đúng quy trình kỹ thuật, đúng quy định về thao tác. Chấp hành các quy định về bảo quản thiết bị, thường xuyên vệ sinh bên ngoài thiết bị, cần chủ động khắc phục các lỗi nhỏ xuất hiện khi sử dụng thiết bị trong khả năng của mình, trường hợp không tự khắc phục được thì đề nghị Phòng TCDN-TH kiểm tra để có giải pháp khắc phục. Người sử dụng không được tùy tiện mở và làm sai lệch các linh kiện bên trong của thiết bị (kể thêm và bớt linh kiện). Mọi mất mát và hư hỏng do sử dụng sai nguyên tắc thì người sử dụng gây ra phải chịu trách nhiệm cá nhân.

7. Quản lý thiết bị tin học: Thiết bị tin học được giao cho các phòng ban sử dụng, Lãnh đạo phòng thường xuyên kiểm tra và quản lý. Trường hợp mang thiết bị ra khỏi công sở phải có ý kiến chấp thuận của Lãnh đạo phòng, Phòng TCDN-TH và

Văn phòng Sở (phụ lục 2), trừ những thiết bị tin học thường xuyên phải mang ra khỏi cơ quan để trợ giúp các hoạt động nghiệp vụ đặc thù của từng Phòng hay Lãnh đạo Sở. Trường hợp này, lãnh đạo phòng lập danh mục thiết bị có sự thoả thuận của Văn phòng Sở (mỗi năm 1 lần) và tự chịu trách nhiệm quản lý. Thiết bị tin học phải được giao cho cá nhân sử dụng, quản lý. Trường hợp nhiều người sử dụng chung phải phân công một người chịu trách nhiệm quản lý chính. Không được tự ý sử dụng các máy tính do người khác quản lý. Việc điều chuyển thiết bị tin học phải do lãnh đạo Sở quyết định sau khi có ý kiến đề xuất của Văn phòng Sở và Phòng TCDN-TH.

Điều 6. Quản lý, khai thác mạng máy tính và internet

1. Nguyên tắc quản lý: Các phòng chuyên môn, công chức và người lao động thuộc Sở khi tham gia vào hệ thống mạng (LAN, internet, dữ liệu chuyên dùng) không được tự ý lắp đặt các thiết bị như: Switch, Hub, modem wifi… trường hợp cần lắp đặt phải được sự đồng ý của Giám đốc Sở và thông báo cho cán bộ quản trị mạng kiểm tra, cấu hình thiết bị (nếu cần) để đảm bảo an toàn bảo mật thông tin, dữ liệu và hệ thống mạng.

2. Vận hành mạng máy tính:

a) Phòng TCDN-Tin học chủ trì vận hành mạng LAN, có trách nhiệm phân công cán bộ quản trị mạng để thống nhất vận hành và hướng dẫn nghiệp vụ cho các phòng sử dụng, khai thác mạng LAN, mạng Internet và mạng dữ liệu chuyên dùng.

b) Các phòng chuyên môn, công chức và người lao động thuộc Sở được phép truy cập mạng máy tính của Sở sẽ được cấp tài khoản người dùng (Account) để truy cập và phải chịu trách nhiệm bảo đảm bí mật của tài khoản được cấp; được bộ phận quản trị mạng phân quyền khai thác cơ sở dữ liệu, dịch vụ trên mạng theo chức năng, nhiệm vụ của mình và chỉ có quyền sử dụng những thông tin mà máy chủ đã phân quyền.

c) Hàng ngày, công chức và người lao động thường xuyên truy cập vào mạng máy tính để khai thác thông tin phục vụ công tác; thực hiện việc gửi, nhận, trao đổi, xử lý văn bản, giấy tờ hành chính thông qua mạng máy tính, các phần mềm chuyên ngành, phần mềm dùng chung và có trách nhiệm với nhiệm vụ của mình.

d) Khi khai thác sử dụng các tài nguyên trên mạng (*phần mềm, cơ sở dữ liệu và các thông tin khác*) lãnh đạo, công chức và người lao động phải theo đúng trách nhiệm, quyền hạn, chức năng, nhiệm vụ được phân công; không được tự ý di chuyển đường cáp, các thiết bị phần cứng, cài đặt phần mềm, khai thác thông tin không thuộc phạm vi xử lý của mình.

đ) Công chức và người lao động thuộc Sở không được sử dụng mạng máy tính, mạng Internet của Sở để khai thác, lưu trữ các dữ liệu, thông tin như các trò chơi, các chương trình giải trí không lành mạnh, các trang web có nội dung xấu.

Điều 7. Quản lý, khai thác, sử dụng dữ liệu và phần mềm

1. Phòng TCDN-TH chịu 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 chuyên môn trực thuộc Sở và toàn thể công chức và người lao động có trách nhiệm phối hợp với Phòng TCDN-TH trong quá trình triển khai, khai thác và sử dụng phần mềm.

3. Cán bộ công chức và người lao động phải chủ động sao lưu dữ liệu cá nhân của mình bằng các phương tiện lưu trữ (USB, drive, điện toán đám mây..). Trong trường hợp dữ liệu lớn, quan trọng thì đề nghị Phòng TCDN-TH hỗ trợ sao lưu trên hệ thống mạng, máy chủ của cơ quan.

CHƯƠNG III
AN TOÀN, AN NINH HỆ THỐNG THÔNG TIN

Điều 8. Bảo đảm an toàn thông tin đối với Phòng máy chủ

1. 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.

2. Phòng máy chủ là khu vực hạn chế tiếp cận chỉ những cá nhân có quyền, nhiệm vụ theo quy định của thủ trưởng đơn vị mới được phép vào Phòng máy chủ. Việc vào, ra phòng máy chủ phải được kiểm soát bằng thiết bị bảo vệ (quẹt thẻ, vân tay, sinh trắc học,…).

3. 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 khi có sự cố mất điện.

4. Phòng máy chủ phải có hệ thống làm mát điều hòa không khí, 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. Các hệ thống này phải được thiết lập chế độ cảnh báo phù hợp. Phòng TCDN-TH thường xuyên giám sát thiết bị, hạ tầng của phòng máy chủ.

5. Hệ thống máy chủ phải có tính năng sẵn sàng cao, cơ chế dự phòng linh hoạt để đảm bảo hoạt động liên tục. Máy chủ phải được thiết lập chính sách xác thực; Kiểm soát truy cập; Thực hiện biện pháp phòng chống xâm nhập; Phòng chống phần mềm độc hại và xử lý dữ liệu trên máy chủ khi chuyển giao. Phần mềm hệ điều hành cài lên máy chủ ưu tiên là phần mềm hệ điều hành có bản quyền hoặc là phần mềm mã nguồn mở được sử dụng rộng rãi trong nước và quốc tế. Có tài liệu liệt kê, cài đặt với những phần mềm hệ thống cài trong máy chủ.

6. Các máy chủ đều được cài đặt phần mềm Antivirus bản quyền (BKAV Endpoint) phòng chống mã độc và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm. Tiến hành kiểm tra, dò quét, xử lý phần mềm độc hại cho các phần mềm trước khi cài đặt trên máy chủ.

7. Thiết lập hệ thống máy chủ chỉ cho phép sử dụng các kết nối mạng an toàn https khi truy cập, quản trị ứng dụng từ xa, có phương án giới hạn địa chỉ IP được phép truy cập, quản trị ứng dụng từ xa tùy tình hình thực tế. Quản lý phân quyền truy cập, quản trị, sử dụng tài nguyên khác nhau của ứng dụng với người sử dụng/nhóm người sử dụng có chức năng, yêu cầu nghiệp vụ khác nhau. Giới hạn số lượng các kết nối đồng thời (kết nối khởi tạo và đã thiết lập) đối với các ứng dụng, dịch vụ

do máy chủ cung cấp tùy tình hình cụ thể đảm bảo tính sẵn sàng của ứng dụng, dịch vụ cung cấp trong trường hợp bị tấn công từ chối dịch vụ.

Điều 9. Phòng chống virus máy tính, bảo mật cơ sở dữ liệu và an ninh mạng

1. Bảo mật số liệu:

a) Công chức và người lao động phải có trách nhiệm bảo mật số liệu nghiệp vụ trên máy tính.

b) Việc chia sẻ dữ liệu trên mạng do bộ phận quản trị mạng thực hiện theo quyết định của Giám đốc Sở và theo phân cấp sử dụng tài nguyên mạng.

2. Bảo mật truy cập: Các chương trình ứng dụng, phân chia sử dụng trên máy tính phải được đặt mật khẩu, mã khoá bảo mật.

3. Bảo mật hệ thống mạng và truyền tin:

a) Mạng và đường truyền được áp dụng các chế độ bảo mật cần thiết, chống xâm nhập bất hợp pháp.

b) Bộ phận quản trị mạng có trách nhiệm thường xuyên theo dõi, kiểm tra phát hiện kịp thời các hoạt động xâm nhập và có biện pháp xử lý kịp thời.

4. An toàn trong sử dụng: Khi không làm việc với máy vi tính trong thời gian dài, công chức và người lao động thuộc Sở phải tắt máy tính hoặc đặt chế độ bảo vệ để đảm bảo an toàn cho dữ liệu của cá nhân.

5. Phòng, chống virus: Công chức và người lao động thuộc Sở có trách nhiệm tuân thủ các biện pháp phòng và chống virus cho máy tính, đảm bảo an toàn dữ liệu thuộc cá nhân quản lý.

a) Các máy tính trạng bị cho CBCC đều được cài đặt phần mềm Antivirus bản quyền (BKAV Endpoint) phòng chống mã độc và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm. Người sử dụng máy tính phải tự sao lưu dữ liệu và quét, diệt virus cho máy tính mình quản lý.

b) Mọi dữ liệu từ các thiết bị lưu trữ bên ngoài (USB, đĩa mềm, đĩa CD…) đều phải được quét, diệt virus trước khi đưa vào máy tính.

c) Những máy tính phát hiện có virus phải được tách khỏi mạng về mặt vật lý để tránh tình trạng lây nhiễm sang các máy tính khác. 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 quản trị mạng để được xử lý kịp thời

d) Không truy cập vào các trang web, các link liên kết không rõ ràng; không click vào các link, tải về các file tài liệu từ các địa chỉ thư không nắm rõ thông tin, địa chỉ người gửi.

e) 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 quản trị mạng

f) 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.

CHƯƠNG VI
TỔ CHỨC THỰC HIỆN

Điều 10. Điều khoản thi hành

1. Cán bộ, công chức và người lao động tại các phòng chuyên môn trực thuộc Sở có trách nhiệm thực hiện nghiêm túc Quy chế này.

2. Mọi hành vi vi phạm các điều khoản trong Quy chế, tùy theo tính chất, mức độ sẽ bị xử lý kỷ luật, xử phạt vi phạm hành chính, bồi thường vật chất, khắc phục hậu quả hoặc truy cứu trách nhiệm hình sự theo quy định của pháp luật hiện hành.

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

GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ TÀI CHÍNH
TỈNH BÌNH ĐỊNH

Ký bởi: Sở Tài chính
Ngày ký: 09-12-2019 09:57:20 +07:00

Lê Hoàng Nghi

Phụ lục 1:

BIỂU MẪU KHẮC PHỤC SỰ CỐ CÔNG NGHỆ THÔNG TIN

Họ tên người đề nghị: …… ……

Phòng: …….……..……..

Số hiệu thiết bị ……...

I. NỘI DUNG SỰ CỐ *(đánh dấu vào ô thích hợp và mô tả sự cố gặp phải)*:

□ Phần cứng □ Phần mềm □ Máy in □ Mạng □ Khác

…….....

…….....

Quy Nhơn, ngày……/……/20…

Người đề nghị **Lãnh đạo Phòng**

(Ký, ghi rõ họ tên) (Ký, ghi rõ họ tên)

II. KHẢO SÁT HIỆN TRẠNG: …….……

…….....

***Nguyên nhân*:.....**

Thiết bị/phần mềm/HTTT: Còn bảo hành □ Hết bảo hành □

Quy Nhơn, ngày……/……/20…

Phòng TCDN-TH

III. KHẮC PHỤC SỰ CỐ:

1. Phòng Tin học (hoặc cùng đơn vị phối hợp**) : Khắc phục sự cố tại chỗ**

Kết quả …..……...…..:…….....

……

2. Đề nghị sửa chữa hoặc thay thế thiết bị *(nếu có)*

……

……

……

3. Tổng thời gian khắc phục sự cố: ……..

Quy Nhơn, ngày……/……/20…

Văn Phòng Sở **Phòng TCDN-TH** **LÃNH ĐẠO SỞ**

(Ký, ghi rõ họ tên) (Ký, ghi rõ họ tên) (Ký, ghi rõ họ tên)

Phụ lục 2:

BIỂU MẪU QUẢN LÝ THIẾT BỊ TIN HỌC

(Trường hợp mang thiết bị ra khỏi cơ quan)

Tên thiết bị tin học:……..

Người sử dụng: ……

Phòng: ……..

Cấu hình thiết bị: ……

……..

Hiện trạng thiết bị trước khi mang ra khỏi cơ quan: ……

……...

Lý do: ……..

Thời gian: Từ ngày (mang đi)…….....đến ngày (hoàn trả)…….

VĂN PHÒNG SỞ **PHÒNG**……

- Ngày mang đi: ……..
- Ngày hoàn trả: .....

Xác nhận

PHÒNG TCND -TH

- Ngày mang đi: ……..
- Ngày hoàn trả: .....

Xác nhận