UBND TỈNH QUẢNG TRỊ
SỞ KHOA HỌC VÀ CÔNG NGHỆ

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

Số: 305 /QĐ-SKHCN

Quảng Trị, ngày 01 tháng 11 năm 2016

QUYẾT ĐỊNH

Về việc ban hành Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng CNTT của Sở Khoa học và Công nghệ Quảng Trị

GIÁM ĐỐC SỞ KHOA HỌC VÀ CÔNG NGHỆ QUẢNG TRỊ

Căn cứ Luật Giao dịch điện tử ngày 29/11/2005;

Căn cứ Luật Công nghệ thông tin ngày 29/6/2006;

Căn cứ Nghị định số 63/2007/NĐ-CP ngày 10/4/2007 của Chính phủ về quy định xử phạt vi phạm hành chính trong lĩnh vực công nghệ thông tin;

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

Căn cứ Nghị định số 72/2013/NĐ-CP ngày 15/7/2013 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng;

Căn cứ Chỉ thị số 897/CT-TTg ngày 10/6/2011 của Thủ tướng chính phủ về việc triển khai các hoạt động đảm bảo an toàn thông tin số;

Căn cứ Quyết định số 35/2016/QĐ-UBND ngày 29/8/2016 của UBND tỉnh Quảng Trị 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 nhà nước tỉnh Quảng Trị;

Căn cứ Quyết định số 14/2015/QĐ-UBND ngày 26/6/2015 của UBND tỉnh về việc Ban hành Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Sở Khoa học và Công nghệ Quảng Trị;

Căn cứ Quyết dịnh số 11/QĐ-SKHCN ngày 11/01/2016 của Giám dốc Sở Khoa học và Công nghệ Quảng Trị về việc ban hành Quy chế làm việc Sở Khoa học và Công nghệ Quảng Trị;

Xét đề nghị của Chánh Văn phòng, Giám dốc Trung tâm Thông tin và Thống kê KH&CN,

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 KH&CN Quảng Trị.

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

Điều 3. Chánh Văn phòng Sở, Chánh Thanh tra Sở, Kế toán trưởng Sở, Trưởng các phòng chức năng, đơn vị trực thuộc Sở và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như điều 3;
- UBND tỉnh (b/c);
- Sở TT&TT (b/c);
- GĐ, các PGĐ Sở;
- Lưu: VT, TT&TK.

GIÁM ĐỐC

SỞ KHOA HỌC VÀ CÔNG NGHỆ TỈNH QUẢNG

Trần Ngọc Lân

UBND TỈNH QUẢNG TRỊ
SỞ KHOA HỌC VÀ CÔNG NGHỆ

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 KH&CN tỉnh Quảng Trị

(Ban hành kèm theo Quyết định số 805 /QĐ-SKHCN ngày 01/11/2016 của Sở KH&CN tỉnh Quảng Trị)

Chương I
QUY ĐỊNH CHUNG

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

1. Quy chế này quy định chi tiết nội dung, biện pháp đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin (CNTT) tại cơ quan Sở KH&CN và các đơn vị trực thuộc Sở KH&CN, bao gồm: Công tác quản lý đảm bảo an toàn, an ninh thông tin mạng; việc áp dụng các biện pháp quản lý kỹ thuật, quản lý vận hành đảm bảo an toàn, an ninh thông tin đối với các hệ thống thông tin.

2. Quy chế này áp dụng cho tất cả cán bộ, công chức, viên chức đang làm việc tại Sở KH&CN và các đơn vị trực thuộc Sở KH&CN.

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

1. Bảo vệ toàn diện, ngăn chặn các mối đe dọa, giảm thiểu các rủi ro do môi trường bị gián đoạn, lỗi của con người hoặc máy, các cuộc tấn công có mục đích làm mất an toàn thông tin; bảo dảo an toàn, an ninh thông tin cho các đơn vị trong môi trường mạng.

2. Bảo vệ chống lại hành vi vô tình hay cố ý thay đổi trái phép, phá hủy, làm chậm trễ, trộm cắp, truy cập (khi không được quyền) gây thiệt hại cho hệ thống, dữ liệu, ứng dụng, thiết bị và viễn thông.

3. Việc nghiên cứu, ứng dụng và phát triển CNTT của các đơn vị phải bảo đảm tính bảo mật, an toàn, an ninh thông tin, hợp lý và hiệu quả.

Điều 3. Các hành vi bị cấm

1. Cản trở, ngăn chặn, can thiệp trái phép việc truyền tải thông tin, xóa, thay đổi, làm sai lệch thông tin trên mạng, ảnh hưởng tới sự hoạt động bình thường của hệ thống thông tin hoặc khả năng truy cập hợp pháp của người sử dụng tới hệ thống thông tin.

2. Sử dụng trái phép tài khoản, mật khẩu của tổ chức, cá nhân; thông tin riêng, thông tin cá nhân và tài nguyên Internet.

3. Tạo, cài đặt, phát tán thư rác, tin nhắn rác, mã độc; thiết lập hệ thống thông tin lừa đảo, giả mạo.

4. Lợi dụng mạng để truyền bá thông tin, quan điểm, tài liệu, hình ảnh, âm thanh hoặc dạng thông tin khác nhằm thực hiện các hành vi gây lộ thông tin ảnh hưởng đến an toàn, bí mật thông tin của cá nhân, cơ quan và ảnh hưởng đến an ninh quốc gia, trật tự, an toàn xã hội.

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

Điều 4. Về quản lý tài khoản người dùng:

1. Quản trị mạng Sở có trách nhiệm tạo, lập và cung cấp tài khoản truy nhập hệ thống mạng nội bộ, phần mềm Hồ sơ công việc cho cán bộ, công chức, viên chức của Sở.

Đối với công chức, viên chức tiếp nhận mới hoặc luân chuyển, ngừng công tác ở Sở: Quản trị mạng căn cứ quyết định của cơ quan tạo mới hoặc hủy bỏ các tài khoản liên quan cho các cá nhân đó.

2. Cán bộ, công chức, viên chức phải cài đặt mật khẩu cho máy tính cá nhân của mình, có trách nhiệm bảo vệ và bảo mật tài khoản, dữ liệu của mình như: thư công vụ, quản lý hồ sơ công việc, kế toán, cơ sở dữ liệu...; không tự ý xâm nhập các tài khoản khác; đồng thời không cho thông tin tài khoản của mình cho các cá nhân không có liên quan.

- Mật khẩu phải thay đổi thường xuyên hoặc định kỳ 3 tháng 1lần.
- Không dùng một mật khẩu trong nhiều tài khoản.

Điều 5. Về quản lý, sử dụng hệ thống:

1. Đối với thiết bị CNTT: Cán bộ, công chức Sở có trách nhiệm quản lý trang thiết bị CNTT (máy vi tính, máy in, thiết bị ngoại vi,...) được giao, tự quản lý dữ liệu trên máy tính của mình, tự quyết định việc chia sẻ tài nguyên với các máy tính khác theo đúng quy định. Ngoài ra, đối với cơ sở dữ liệu có tính chất "Mật" khi chia sẻ dữ liệu phải có ý kiến của lãnh đạo cơ quan và quản lý, lưu trữ theo quy định.

- Quản trị mạng chịu trách nhiệm kiểm tra, theo dõi, đánh giá hoạt động của máy chủ, máy trạm, các thiết bị mạng và các thiết bị ngoại vi theo đúng tiêu chuẩn kỹ thuật; thực hiện việc sao lưu dữ liệu; ghi nhật ký báo lỗi của mạng, các thiết bị CNTT để thực hiện công tác bảo trì, bảo dưỡng định kỳ, đột xuất, giảm

thiểu tối đa các sự cố kỹ thuật; cung cấp địa chỉ IP mạng và tham số mạng cho người dùng kết nối vào mạng LAN Sở.

- Máy tính và các thiết bị CNTT để nơi an toàn, tránh ảnh hưởng các tác nhân bên ngoài (ánh nắng, mưa...), không để các tài liệu giấy gần máy tính và các thiết bị ngoại vi nhằm tránh cháy nổ xảy ra, thường xuyên vệ sinh cho máy; hàng ngày kiểm tra theo dõi sự hoạt động của máy tính, thiết bị ngoại vi... Khi không sử dụng máy tính nên tắt máy nhằm tiết kiệm điện và phòng, chống các xâm nhập trái phép.

- Trong quá trình sử dụng các thiết bị CNTT, nếu có sự cố xảy ra, cán bộ, công chức, viên chức lập phiếu yêu cầu sửa chữa, chuyển đến Quản trị mạng. Trong trường hợp xảy ra sự cố lớn phiếu sửa chữa phải được xác nhận của lãnh đạo Sở.

- Các công việc sửa chữa hàng ngày đều được ghi vào nhật ký sửa chữa của Quản trị mạng sau mỗi lần sửa chữa.

2. Hệ thống mạng LAN:

- Cán bộ, công chức, viên chức Sở khi tham gia vào mạng LAN không được tự ý thay đổi các tham số mạng. Trường hợp cần thiết phải thay đổi tham số mạng, hãy báo cho Quản trị mạng để xử lý.

- Quản trị mạng chịu trách nhiệm kiểm tra, theo dõi, đánh giá sự hoạt động của máy chủ, máy trạm, các thiết bị mạng và các thiết bị khác theo đúng tiêu chuẩn kỹ thuật; thực hiện việc sao lưu dữ liệu; ghi nhật ký báo lỗi của mạng, các thiết bị CNTT để thực hiện công tác bảo trì, bảo dưỡng định kỳ, dột xuất, giảm thiểu tối đa các sự cố kỹ thuật; cung cấp địa chỉ IP mạng và tham số mạng cho người dùng kết nối vào mạng LAN Sở.

- Quản trị mạng chịu tránh nhiệm cài đặt hệ thống an ninh mạng theo đúng tiêu chuẩn an toàn bảo mật; cài đặt hệ thống tự động cập nhật mẫu Virus mới và tự động diệt Virus khi phát hiện có Virus xâm nhập máy tính; thường xuyên kiểm tra, quét Virus định kỳ cho tất cả các máy chủ, máy trạm; xử lý, khắc phục kịp thời khi xảy ra sự cố máy tính bị Virus xâm nhập; đảm bảo hệ thống mạng máy tính luôn sạch Virus để đảm bảo máy tính của cán bộ, công chức, viên chức hoạt động tốt.

3. Cơ sở dữ liệu khoa học và công nghệ:

- Các phòng chuyên môn, đơn vị trực thuộc Sở khi quản lý, lưu trữ và cung cấp cơ sở dữ liệu về khoa học và công nghệ phải thực hiện đúng theo quy chế bảo vệ bí mật Nhà nước của Sở Khoa học và Công nghệ.

- Các phòng chuyên môn, đơn vị thuộc Sở hàng năm có kế hoạch giao nộp tài liệu, cơ sở dữ liệu có liên quan của Phòng mình về Văn phòng Sở để bảo quản và lưu trữ.

- Văn phòng Sở tổ chức việc phân loại dữ liệu, thu thập, xử lý và cung cấp cho các tổ chức cá nhân có nhu cầu theo đúng các quy định hiện hành.

4. Sử dụng phần mềm dùng chung của tỉnh:

- Mật khẩu truy cập vào tài khoản cá nhân phải đảm bảo đủ 8 ký tự, bao gồm chữ hoa, chữ thường, ký tự đặc biệt và chữ số; không đặt chế độ ghi nhớ mật khẩu khi sử dụng.

- Khi khai thác, sử dụng các phần mềm dùng chung của tỉnh tại các điểm truy cập internet công cộng, tuyệt đối không đặt chế độ lưu giữ mật khẩu trong trình duyệt.

5. Quản lý và sử dụng thiết bị ký số:

Các cá nhân được trang bị thiết bị ký số phải bảo quản ở chế độ mật, không
giao thiết bị ký số cho người không có thẩm quyền, tuyệt đối không tiết lộ mật khẩu ký số.

Điều 6. Cơ chế sao lưu dữ liệu

1. Phân loại dữ liệu sao lưu:

- Dữ liệu hệ thống: bao gồm các loại thông tin, dữ liệu cài đặt như: cấp phát tài khoản và địa chỉ IP mạng, phân giải tên miền, cung cấp thông tin internet,….

- Dữ liệu các ứng dụng dùng chung được cài đặt trên máy chủ như: Quản lý hộp thư điện tử, đường truyền số liệu, phần mềm dùng chung…

- Các dữ liệu khác cài đặt trên máy tính cá nhân như: số liệu quản lý thu chi kế toán, quản lý hồ sơ một cửa, công văn đi, công văn đến,…do các CBCCVC các phòng thuộc, đơn vị thuộc Sở soạn thảo, tạo lập trên các máy trạm trong mạng nội bộ của Sở.

- Các hệ thống thông tin KH&CN, hệ thống CSDL KH&CN, CSDL các nhiệm vụ KH&CN,.... được lưu trữ ở Trung tâm Thông tin và Thống kê KH&CN.

2. Quy định thiết bị sao lưu:

- Đối với dữ liệu hệ thống: Sử dụng chức năng sao lưu dự phòng của các ứng dụng, kết hợp với sử dụng thiết bị lưu trữ tập trung ở Trung tâm Thông tin và Thống kê KH&CN.

- Đối với các dữ liệu khác: Các dữ liệu cần lưu trữ, các phòng, đơn vị thuộc Sở chép lên ổ đĩa mạng của máy chủ để sao lưu tập trung của đơn vị mình.

Ngoài ra, căn cứ vào các mức độ quan trọng của dữ liệu, các phòng, đơn vị thuộc Sở sử dụng các thiết bị gắn ngoài (ổ cứng di động, USB, đĩa CD, DVD...) nhằm lưu trữ dữ liệu an toàn, bảo mật.

3. Định kỳ sao lưu: Tùy vào mức độ qui định thời hạn mỗi loại thông tin, dữ liệu cần sao lưu.

- Đối với dữ liệu hệ thống: Sao lưu định kỳ: 3 tháng /lần

- Đối với các hệ thống thông tin: Sao lưu thường xuyên và phải xây dựng quy chế sử dụng hệ thống.

- Đối với các dữ liệu khác: sao lưu khi có thay đổi thông tin

4. Quy định về khôi phục dữ liệu đã sao lưu:

- Khi cần khôi phục lại dữ liệu đã sao lưu, các phòng trực thuộc Sở báo cho Quản trị mạng biết, xem xét thực hiện khôi phục dữ liệu.

- Thời kỳ dữ liệu yêu cầu khôi phục phải phù hợp với quy định tại khoản 3 điều này.

Điều 7. Giải quyết và khắc phục sự cố về an toàn, an ninh thông tin

1. Đối với cán bộ, công chức:

- Quản lý chặt chẽ việc di chuyển các trang thiết bị CNTT (máy chủ, máy trạm, thiết bị ngoại vi) của Sở.

- Thông tin báo cáo kịp thời cho Quản trị mạng và Văn phòng Sở khi phát hiện các sự cố gây mất an toàn, an ninh thông tin trong hệ thống mạng Sở.

- Xử lý khẩn cấp: khi phát hiện hệ thống bị tấn công, thông qua các dấu hiệu khác thường như: hệ thống máy vi tính hoạt động chậm khác thường, nội dung bị thay đổi,...cần thực hiện các bước sau:

+ Ngắt kết nối máy vi tính ra khỏi mạng LAN, Internet.

+ Sao chép toàn bộ dữ liệu của hệ thống ra thiết bị lưu ngoài (CD, USB, ổ cứng di động,...).

+ Khôi phục hệ thống bằng cách chuyển dữ liệu backup (sao lưu) mới nhất để hệ thống hoạt động ổn định.

2. Đối với cán bộ Quản trị mạng:

- Quản lý chặt chẽ việc di chuyển các trang thiết bị CNTT (máy chủ, máy

trạm, thiết bị ngoại vi) của Sở.

- Hướng dẫn người dùng các biện pháp kỹ thuật giải quyết và khắc phục sự cố; Trong trường hợp sự cố xảy ra ngoài khả năng giải quyết, kịp thời báo cáo với Lãnh đạo Sở; đồng thời phối hợp với cơ quan chuyên môn (Sở Thông tin và Truyền thông, Công An Tỉnh...) hướng dẫn khắc phục.

- Quản lý chặt chẽ trong việc sử dụng và thanh lý tài sản các trang thiết bị CNTT lưu trữ các thông tin thuộc danh mục bí mật nhà nước. Các thiết bị lưu trữ không sử dụng tiếp cho công việc (thanh lý, cho, tặng) phải được xóa, hủy nội dung bảo đảm không phục hồi dược dữ liệu.

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

Điều 8. Trách nhiệm của Lãnh đạo Sở

1. Lãnh đạo Sở có trách nhiệm toàn diện trước UBND tỉnh trong công tác bảo vệ an toàn hệ thống thông tin của đơn vị.

2. Phân công cán bộ Quản trị mạng dảm bảo, an toàn thông tin trước khi tiến hành các hoạt động quản lý, vận hành hệ thống thông tin.

3. Quan tâm đầu tư các thiết bị phần cứng, phần mềm liên quan đến công tác đảm bảo an toàn thông tin. Đào tạo, tuyển dụng nguồn nhân lực có kiến thức, trình độ về CNTT.

4. Khi có sự cố hoặc nguy cơ mất an toàn thông tin, kịp thời cử cán bộ phối hợp chặt chẽ với cơ quan chuyên môn trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn, an ninh thông tin.

Điều 9. Trách nhiệm của Trung tâm Thông tin và Thống kế KH&CN:

- Thực hiện hướng dẫn các phòng, đơn vị trực thuộc và CBCCVC, NLĐ cơ quan thực hiện các giải pháp bảo mật, an toàn thông tin, phòng chống vi rút máy tính, thư rác và thư giả mạo.

- Hàng năm, lập kế hoạch ứng dụng CNTT, kế hoạch an toàn và an ninh thông tin trình Sở KH&CN phê duyệt để thực hiện.

- Xây dựng quy chế quản lý các hệ thống thông tin, CSDL về KH&CN tỉnh Quảng Trị.

- Kịp thời tham mưu cho Sở những quy định, hướng dẫn có liên quan đến công tác an toàn, an ninh thông tin do cơ quan chuyên môn cấp trên, UBND Tỉnh ban hành.

- Chủ trì, phối hợp với Văn phòng Sở báo cáo định kỳ, dọt xuất về tình hình an toàn, an ninh thông tin của cơ quan khi có yêu cầu.

- Phân công cán bộ có trình độ chuyên môn phụ trách công tác đảm bảo an toàn, an ninh thông tin của cơ quan.

- Đảm bảo an toàn, an ninh thông tin đối với các máy tính quản trị Website của Sở, các máy tính lưu trữ cơ sở dữ liệu. Có kế hoạch trang bị thiết bị, phần mềm an toàn, an ninh thông tin đảm bảo hoạt động ổn định và an toàn.

Điều 10. Đối với trách nhiệm của quản trị mạng

1. Quản lý chặt chẽ việc di chuyển các trang thiết bị CNTT (máy chủ, máy trạm, thiết bị ngoại vi), hệ thống mạng, thực hiện các báo cáo định kỳ về tình trạng hoạt động toàn hệ thống mạng, đề nghị hướng giải quyết khi có sự cố.

2. Thực hiện cấp phát, thu hồi, cập nhật và quản lý tất cả các tài khoản truy cập vào hệ thống thông tin của Sở; hướng dẫn người dùng thay đổi mật khẩu cá nhân theo quy định.

3. Tham mưu chuyên môn và vận hành an toàn hệ thống thông tin của đơn vị, triển khai các biện pháp bảo đảm an toàn, an ninh thông tin cho tất cả cán bộ, công chức, viên chức trong đơn vị mình.

4. Quản lý, theo dõi các hoạt động thường xuyên và định kỳ như vận hành, sửa chữa hệ thống máy chủ, máy trạm, các thiết bị khác...; xử lý các yêu cầu về thay đổi tài khoản sử dụng mạng của các phòng chức năng Sở.

5. Sao lưu dữ liệu tại nơi an toàn, kiểm ra dữ liệu sao lưu phải đảm bảo tính sẵn sàng và toàn vẹn.

6. Thực hiện việc đánh giá, báo cáo các rủi ro về mức độ nghiêm trọng có thể xảy ra do sự truy cập và sử dụng trái phép, thay đổi hoặc phá hủy thông tin và hệ thống thông tin.

Điều 11. Đối với cán bộ, công chức, viên chức và người lao động

1. Nghiêm chỉnh chấp hành các quy định của Quy chế này và các quy định khác của pháp luật có liên quan đến việc đảm bảo, an ninh thông tin.

2. Các máy tính khi không sử dụng trong thời gian dài (quá 2 giờ làm việc) cần tắt máy hoặc đặt mật khẩu và thiết lập chế độ tự động bảo vệ màn hình sau 10 phút không sử dụng, 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.

3. Các cán bộ, công chức, viên chức có trách nhiệm tự quản lý các thiết bị CNTT được giao sử dụng; không tự ý thay đổi và tháo lắp các thiết bị trên máy vi tính khi chưa có sự đồng ý của quản trị mạng; không tự ý liên hệ với cá nhân bên ngoài vào can thiệp các thiết bị máy tính.

4. Sử dụng chức năng mã hóa ở mức hệ điều hành bảo đảm các dữ liệu

nhạy cảm như tài khoản, mật khẩu, các tập tin văn bản,... được mã hóa trước khi truyền trên môi trường mạng. Các tập tin gửi đính kèm bởi thư điện tử hoặc được tải xuống từ Internet hay 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.

5. Không được truy cập hoặc tải thông tin từ các trang Website độc hại, không được cài dặt các chương trình không rõ nguồn gốc...

6. Cấm các hành vi tạo, cài dặt, phát tán phần mềm độc hại, virus máy tính; xâm nhập trái phép, chiếm quyền điều khiển hệ thống thông tin, sửa đổi, xóa, làm sai lệch thông tin trên mạng, tạo lập công cụ tấn công mạng.

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

8. Cấm lợi dụng mạng và các trang mạng xã hội để truyền bá thông tin, văn hóa độc hại, đồi trụy, kích động, chống phá, xuyên tạc các chủ trương, đường lối của Đảng, chính sách pháp luật của Nhà nước.

9. Không được sử dụng thiết bị (máy tính để bàn, máy tính xách tay, máy tính bảng, điện thoại thông minh...) có kết nối mạng để soạn thảo văn bản, lưu trữ, in, sao chụp thông tin, tài liệu có nội dung thuộc bí mật nhà nước; không cung cấp thông tin, tài liệu và đưa thông tin bí mật nhà nước trên mạng.

10.Không bật các thiết bị kết nối mạng trong các cuộc họp có nội dung bí mật nhà nước.

11. Khi sử dụng các thiết bị lưu trữ dữ liệu di động để lưu thông tin thuộc danh mục bí mật nhà nước phải có trách nhiệm bảo vệ các thiết bị này và thông tin trên thiết bị, tránh làm mất, lộ thông tin. Nghiêm cấm việc bán, cho mượn, giao người không có trách nhiệm sử dụng thiết bị có lưu giữ bí mật nhà nước.

Chương IV
KHEN THƯỞNG, XỬ LÝ VI PHẠM

Điều 12. Khen thưởng

Các phòng chuyên môn, đơn vị trực thuộc; cán bộ, công chức, viên chức và người lao động thực hiện tốt Quy chế này đem lại hiệu quả thiết thực sẽ được xem xét đánh giá khen thưởng.

Điều 13. Xử lý vi phạm

Các phòng chuyên môn, đơn vị trực thuộc; cán bộ, công chức, viên chức có hành vi vi phạm quy chế này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật theo trách nhiệm, xử phạt hành chính hoặc bị truy cứu trách nhiệm

hình sự. Nếu gây thiệt hại thì phải bồi thường theo quy định của pháp luật hiện hành.

Chương V
TỔ CHỨC THỰC HIỆN

Điều 14. Trách nhiệm thi hành

Chánh Văn phòng Sở, Chánh Thanh tra Sở, Kế toán trưởng Sở, Trưởng các phòng chuyên môn, đơn vị sự nghiệp thuộc Sở có trách nhiệm tổ chức thực hiện Quy chế này. Trong quá trình thực hiện, nếu có những vấn đề vướng mắc, phát sinh cần bổ sung, sửa đổi. Đề nghị các đơn vị báo cáo về Văn phòng Sở để kịp thời sửa đổi, bổ sung cho phù hợp.

Quy chế này được phổ biến đến tất cả các phòng, đơn vị trực thuộc và toàn thể CBCCVC, NLĐ của cơ quan, đơn vị./.

GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ KHOA HỌC VÀ CÔNG NGHỆ
TỈNH QUẢNG TRỊ

Trần Ngọc Lân