UBND TỈNH HƯNG YÊN
SỞ GIAO THÔNG VẬN TẢI

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

Số: 100 /QĐ-SGTVT

Hưng Yên, ngày 15 tháng 02 năm 2023

QUYẾT ĐỊNH

Về việc ban hành Quy chế đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin của Sở Giao thông vận tải

GIÁM ĐỐC SỞ GIAO THÔNG VẬN TẢI HƯNG YÊN

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 của cơ quan nhà nước; 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 tăng cường triển khai các hoạt động đảm bảo an toàn thông tin số;

Căn cứ Quyết định số 39/2022/QĐ-UBND ngày 29/09/2022 của UBND tỉnh về việc tổ chức lại các phòng chuyên môn, nghiệp vụ và quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Sở Giao thông vận tải;

Căn cứ Quyết định số 05/2016/QĐ-UBND ngày 17/03/2016 của UBND tỉnh Hưng Yên ban hành Quy chế đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Hưng Yên;

Căn cứ Nghị quyết Hội nghị cán bộ, công chức, viên chức, người lao động cơ quan năm 2023;

Theo 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 thuộc lĩnh vực công nghệ thông tin của Sở Giao thông vận tải.

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày ký và thay thế Quyết định số 716/QĐ-SGTVT ngày 26/4/2021 của Sở GTVT về Quy chế đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin của Sở GTVT.

Điều 3. Chánh Văn phòng, Trưởng các phòng chuyên môn, thủ trưởng các đơn vị thuộc Sở, các cơ quan, đơn vị có liên quan và toàn thể công chức và người lao động cơ quan có trách nhiệm thi hành quyết định này./.

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

GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ GIAO THÔNG VẬN TẢI
TỈNH HƯNG YÊN

Trần Minh Hải

UBND TỈNH HƯNG YÊN
SỞ GIAO THÔNG VẬN TẢI

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

QUY CHẾ

Đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin của Sở Giao thông vận tải Hưng Yên

(Ban hành kèm theo Quyết định số 100 /QĐ-SGTVT, ngày 15 /02/2023 của Sở Giao thông vận tải Hưng Yên)

Chương I
NHỮNG QUY ĐỊNH CHUNG

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

1. Quy chế này quy định về nội dung, biện pháp đảm bảo an toàn, an ninh thông tin (sau đây viết tắt là AT-ANTT) trong lĩnh vực ứng dụng công nghệ thông tin (viết tắt là CNTT) phục vụ cho công tác điều hành và quản lý nhà nước của Sở Giao thông vận tải Hưng Yên.

2. Quy chế được áp dụng cho tất cả các phòng, đơn vị trực thuộc và cán bộ, công chức, viên chức, người lao động (sau đây viết tắt là CB, CC, VC, NLĐ) thuộc Sở Giao thông vận tải Hưng Yên.

3. Các tổ chức, cá nhân có hoạt động trao đổi thông tin với Sở Giao thông vận tải (Đối tác tham gia tư vấn, xây dựng, triển khai, hỗ trợ, vận hành, thử nghiệm hệ thống công nghệ thông tin; Cơ quan, tổ chức, cá nhân có kết nối mạng để trao đổi thông tin với các đơn vị thuộc sở Giao thông vận tải).

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

1. Tăng cường khả năng phòng chống nguy cơ tấn công, xâm nhập hệ thống thông tin và ngăn chặn, khắc phục kịp thời các sự cố gây mất an toàn thông tin trên môi trường mạng.

2. Công tác đảm bảo an toàn, bảo mật thông tin trên môi trường mạng là yêu cầu bắt buộc trong quá trình thiết kế, vận hành, nâng cấp và hủy bỏ hạ tầng kỹ thuật, hệ thống thông tin.

3. Thông tin thuộc danh mục bí mật nhà nước trên môi trường máy tính và mạng máy tính phải được bảo vệ theo các quy định của Nhà nước và các nội dung tương ứng trong quy định này.

4. Các hoạt động ứng dụng công nghệ thông tin phải tuân theo nguyên tắc đảm bảo an toàn thông tin được quy định tại Điều 41, Nghị định 64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước.

Điều 3. Giải thích từ ngữ

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

1. An toàn thông tin: Bao gồm các hoạt động quản lý, nghiệp vụ và kỹ thuật đối với hệ thống thông tin nhằm bảo vệ, khôi phục các hệ thống, các dịch vụ và nội dung thông tin đối với nguy cơ tự nhiên hoặc do con người gây ra. Việc bảo vệ thông tin, tài sản trong hệ thống thông tin nhằm bảo đảm cho các hệ thống thực hiện đúng chức năng, phục vụ đúng đối tượng một cách sẵn sàng, chính xác và tin cậy. An toàn thông tin bao hàm các nội dung bảo vệ và bảo mật thông tin, an toàn dữ liệu, an toàn máy tính và an toàn mạng.

2. An ninh thông tin: 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. Hệ thống mạng LAN: Là hệ thống mạng nội bộ của cơ quan bao gồm hệ thống dây mạng, các thiết bị mạng, các thiết bị tin học được kết nối với nhau thành một hệ thống mạng nội bộ. Các máy tính trong mạng LAN có thể chia sẻ tài nguyên với nhau như: chia sẻ tập tin, máy in, máy quét và một số thiết bị khác.

4. Hacker: Là người có thể viết hay chỉnh sửa phần mềm, phần cứng máy tính bao gồm lập trình, quản trị và bảo mật. Những người này hiểu rõ hoạt động của hệ thống máy tính, mạng máy tính và dùng kiến thức của bản thân để làm thay đổi, chỉnh sửa nó với mục đích xấu. (nên sử dụng định nghĩa mang tính tiếng Việt như tin tặc, tội phạm mạng,…)

5. Hệ thống thông tin: Là tập hợp thiết bị 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 số.

6. Tham số mạng: Là các tham số kỹ thuật được cài đặt trong các thiết bị mạng và thiết bị máy tính để tạo ra các địa chỉ kết nối trong mạng. Các máy tính gửi và nhận thông tin thông qua các địa chỉ kết nối này.

7. Thiết bị lưu trữ ngoài: Là các ổ cứng di động, USB, đĩa CD, DVD, …

Chương II

QUY ĐỊNH ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

Điều 4. Quản lý, sử dụng tài sản CNTT

1. Máy chủ (Server):

a) Máy chủ phải được đặt ở nơi khô, thoáng, hạn chế tiếp cận, chỉ những người có trách nhiệm theo quy định của Lãnh đạo cơ quan mới được phép vào phòng máy chủ;

b) Máy chủ phải có hệ thống lưu điện đủ công suất và duy trì thời gian hoạt động của máy chủ tối thiểu 30 phút khi có sự cố mất điện;

c) Máy chủ phải có cấu hình tối thiểu RAM 8GB, hai ổ đĩa cứng mỗi ổ 1T,...chỉ dùng để cài đặt các phần mềm hệ thống, phần mềm dùng chung, các phần mềm chống virus có bản quyền, cơ sở dữ liệu cần thiết và các phần mềm có bản quyền hỗ trợ việc triển khai hệ thống thông tin, ngoài ra không được cài đặt phần mềm không rõ nguồn gốc, phần mềm không có nhu cầu sử dụng;

d) Tài nguyên trên máy chủ chỉ được chia sẻ theo danh mục, thư mục cho từng phòng/đơn vị và phải sử dụng mật khẩu để bảo vệ thông tin.

e) Tuyệt đối không được sử dụng máy chủ cho việc duyệt web đọc báo, xem tin tức, chơi games,...

f) Dữ liệu của máy chủ phải được sao lưu ít nhất hai tuần một lần.

2. Thiết bị công nghệ thông tin:

a) Thiết bị kết nối vào hệ thống thông tin của cơ quan: Chỉ máy chủ, máy vi tính trang bị (máy trạm) cho CB, CC, VC, NLĐ được cài đặt phần mềm diệt vi rút và các thiết bị phục vụ cho hoạt động chuyên môn mới được kết nối vào hệ thống thông tin của cơ quan.

b) Khi có sự cố xảy ra đối với các thiết bị CNTT: Nếu sự cố nhỏ không phải thay thế hoặc sửa chữa linh kiện thì cán bộ phụ trách CNTT thực hiện xử lý trực tiếp. Nếu có sự cố lớn cần phải thay thế linh kiện để sửa chữa thì người dùng thiết bị CNTT phải làm đề xuất, có xác nhận của Lãnh đạo phòng và gửi về Văn phòng để được sửa chữa, thay thế theo quy định, tuyệt đối không được tự động chuyển cho các tập thể, cá nhân chưa được xác nhận tính an toàn, bảo mật thông tin sửa chữa.

c) Khi sửa chữa, thanh lý các thiết bị công nghệ thông tin: Không mang thiết bị lưu trữ dữ liệu ra khỏi cơ quan, trong trường hợp bắt buộc phải mang thiết bị ra khỏi cơ quan để bảo hành, sửa chữa cần bố trí cán bộ giám sát và có biên bản xác nhận hiện trạng của thiết bị; khi thanh lý tài sản là thiết bị công nghệ thông tin như máy trạm, máy chủ,... không thanh lý ổ cứng và các thiết bị lưu trữ dữ liệu mà phải hủy theo quy định.

d) Khi thu hồi hoặc chuyển giao phần cứng, phần mềm giữa các phòng phải được lập thành biên bản trong đó có chứng kiến và ký xác nhận của lãnh đạo phòng, đơn vị thực hiện việc giao nhận, đại diện Văn phòng và cán bộ chuyên trách công nghệ thông tin của Sở. Việc sao lưu dữ liệu phải được các bên thực hiện trước khi thu hồi hoặc bàn giao và phải được ghi rõ trong nội dung biên bản.

3. Hệ thống mạng LAN:

a) Mạng LAN Sở Giao thông vận tải có tham số mạng riêng do nhà cung cấp cấp phát theo gói mạng sử dụng; được đặt tại Văn phòng Sở do Cán bộ phụ trách CNTT quản lý, vận hành đảm bảo thông suốt; được sử dụng để phục vụ cho công tác quản lý, chỉ đạo, điều hành, phối hợp công tác trong nội bộ cơ quan.

b) Khi tham gia vào mạng LAN: Các CB, CC, VC, NLĐ không được tự ý thay đổi các tham số mạng, nếu tự ý thay đổi tham số mạng thì người thay đổi

phải chịu hoàn toàn trách nhiệm. Trường hợp cần thiết phải thay đổi tham số mạng báo cán bộ phụ trách CNTT của Sở biết để xử lý.

c) Máy tính và các thiết bị CNTT để nơi an toàn, tránh ảnh hưởng của các tác nhân bên ngoài như nắng, mưa,...; không để các tài liệu, vật liệu dễ cháy gần máy tính và các thiết bị CNTT để tránh xảy ra cháy nổ.

4. Hệ thống mạng internet và mạng không dây (Wifi):

a) Mạng Internet phải được trang bị các thiết bị đảm bảo an toàn, an ninh thông tin như: Tường lửa (tường lửa cứng, tường lửa mềm), hệ thống phát hiện truy cập trái phép,...

b) Thay đổi mật khẩu truy cập mạng không dây: khi có yêu cầu của Lãnh đạo Sở nhằm tăng cường công tác bảo mật.

Điều 5. Quản lý tài khoản người dùng

1. Tất cả tài khoản truy cập vào các phần mềm dùng chung như: Phần mềm Quản lý văn bản và điều hành; phần mềm cung cấp dịch vụ công trực tuyến; Cổng thông tin điện tử của cơ quan; các phần mềm nghiệp vụ của các phòng chuyên môn... phải được thiết lập mật khẩu đủ mạnh (mật khẩu có độ dài tối thiểu 8 ký tự, bao gồm: chữ hoa, chữ thường trong bảng chữ cái, số và các ký tự đặc biệt như: @, !, #, ...); phải đổi mật khẩu mặc định ngay sau khi được cấp và thường xuyên thay đổi mật khẩu tối thiểu 6 tháng/lần.

2. CB, CC, VC, NLĐ phải cài đặt mật khẩu cho máy tính cá nhân của mình, có trách nhiệm bảo vệ và bảo mật tài khoản, dữ liệu cá nhân, của phòng và của cơ quan; không tự ý xâm nhập các tài khoản của người khác để sử dụng, không cung cấp thông tin tài khoản của cá nhân, cơ quan cho tổ chức, cá nhân không có liên quan.

3. Hủy tài khoản, quyền truy cập hệ thống thông tin, thu hồi lại tất cả các dữ liệu lưu trữ trong hệ thống thông tin đối với CB, CC, VC, NLĐ đã nghỉ hưu, chuyển công tác, chấm dứt hợp đồng lao động.

4. Không đặt chế độ ghi nhớ tài khoản sử dụng; đăng xuất khỏi tài khoản khi không sử dụng.

Điều 6. Đảm bảo an toàn dữ liệu

1. Cán bộ chuyên trách CNTT thực hiện sao lưu dữ liệu ít nhất hai tuần một lần *(khuyến khích sao lưu 1 tuần 1 lần hoặc 1 tuần 2 lần)* đối với máy chủ của cơ quan để đảm bảo an toàn và thuận tiện cho quá trình phục hồi khi xảy ra sự cố.

2. Đối với dữ liệu quan trọng: Các CB, CC, VC, NLĐ tự sao chép dữ liệu của mình khi có thay đổi thông tin vào các thiết bị lưu trữ ngoài để đảm bảo dữ liệu được lưu ít nhất ở hai nơi, đề phòng ổ đĩa cứng của máy tính bị hỏng (được lưu trữ nơi an toàn để phòng để đảm bảo khả năng khôi phục dữ liệu khi ổ cứng máy tính hỏng hoặc do vi rút, phần mềm độc hại tấn công, xâm nhập trái phép phá hoại dữ liệu).

3. Trước khi sử dụng thiết bị lưu trữ ngoài để kết nối với máy tính hoặc hệ thống mạng nội bộ phải được quét vi rút trước khi đọc hoặc sao chép dữ liệu.

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

1. Đối với CB, CC, NLĐ:

a) Thông báo kịp thời cho cán bộ chuyên trách về công nghệ thông tin của cơ quan, đơn vị khi phát hiện các sự cố gây mất an toàn, an ninh thông tin trong quá trình tham gia vào hệ thống thông tin của cơ quan, đơn vị.

b) Phối hợp tích cực trong suốt quá trình giải quyết và khắc phục sự cố.

2. Đối với cán bộ chuyên trách về CNTT:

a) Xử lý khẩn cấp: Khi phát hiện hệ thống bị tấn công, thông qua các dấu hiệu như luồng tin tăng lên bất ngờ, nội dung bị thay đổi, hệ thống hoạt động bất thường cần thực hiện các bước cơ bản sau:

Bước 1: Ngắt kết nối máy chủ ra khỏi mạng LAN, internet;

Bước 2: Sao chép toàn bộ dữ liệu của hệ thống ra thiết bị lưu trữ ngoài (USB, ổ cứng di động, …);

Bước 3: Khôi phục lại hệ thống bằng cách chuyển dữ liệu backup (sao lưu) mới nhất để hệ thống hoạt động trở lại bình thường.

Lập biên bản ghi nhận sự cố gây ra mất an toàn, an ninh thông tin đối với hệ thống thông tin của cơ quan, đơn vị. Đồng thời, thu thập các chứng cứ, dấu vết và nguyên nhân gây ra sự cố (nếu có) sau đó báo cáo sự cố và kết quả khắc phục sự cố cho Chánh Văn phòng Sở.

b. Trong trường hợp xảy ra sự cố nghiêm trọng ngoài khả năng giải quyết của cơ quan, đơn vị phải báo cáo khẩn cấp bằng điện thoại, gửi thư điện tử cho Trung tâm Công nghệ thông tin và Truyền thông thuộc Sở Thông tin và Truyền thông để được hỗ trợ, hướng dẫn và phối hợp khắc phục sự cố.

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 Sở Giao thông vận tải.

2. Phân công cán bộ phụ trách CNTT đảm 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.

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

5. Chỉ đạo các phòng, đơn vị trực thuộc tăng cường công tác đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng CNTT và khuyến cáo các đơn vị trang bị phần mềm diệt vi rút có bản quyền cài đặt cho máy tính ở cơ quan, đơn vị.

Điều 9. Trách nhiệm của Văn phòng

1. Tham mưu Lãnh đạo Sở về công tác đảm bảo an toàn, an ninh thông tin và chịu trách nhiệm trong việc đảm bảo an toàn, an ninh thông tin cho các hệ thống thông tin của cơ quan.

2. Hàng năm xây dựng kế hoạch, tổng hợp kinh phí để triển khai công tác an toàn, an ninh thông tin trong hoạt động ứng dụng CNTT của Sở.

3. Thường xuyên tuyên truyền đến các phòng, đơn vị thuộc Sở các thông tin, biện pháp phòng ngừa, ngăn chặn các nguy cơ mất an toàn, an ninh thông tin do vi rút, phần mềm gián điệp,…mà các cơ quan chức năng hướng dẫn.

4. Phối hợp với các cơ quan chức năng quản lý, kiểm soát, phòng ngừa, đấu tranh, ngăn chặn các loại tội phạm lợi dụng hệ thống thông tin xâm hại đến an ninh chính trị, trật tự an toàn xã hội.

Điều 10. Trách nhiệm của các đơn vị trực thuộc

1. Tổ chức triển khai thực hiện quy định này tới toàn thể cán bộ, viên chức, người lao động (là đối tượng người dùng) tại đơn vị.

2. Chủ động đầu tư các thiết bị phần cứng, phần mềm liên quan đến công tác đảm bảo an toàn, an ninh thông tin; chỉ đạo triển khai các hoạt động ứng phó khẩn cấp khi có sự cố tấn công về các nội dung liên quan xảy ra tại đơn vị; thực hiện các yêu cầu, hướng dẫn về an toàn thông tin của Sở Giao thông vận tải và các cơ quan Nhà nước có thẩm quyền; chịu sự kiểm tra các quy định về đảm bảo an toàn, anh ninh thông tin của Sở GTVT và các đơn vị chuyên ngành công nghệ thông tin trên địa bàn tỉnh.

3. Thủ trưởng đơn vị chịu trách nhiệm trước pháp luật và Lãnh đạo Sở về các vi phạm làm 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, viên chức, người lao động của đơn vị thực hiện quy định về an toàn, anh ninh thông tin.

4. Hàng năm báo cáo về Sở (qua Văn phòng) tình hình công tác đảm bảo an toàn thông tin, phản ánh các vướng mắc, phát sinh trong quá trình triển khai, thực hiện về công tác an toàn, an ninh thông tin trên môi trường máy tính và mạng máy tính của đơn vị.

Điều 11. Trách nhiệm của CB, CC, VC, NLĐ

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 toàn, an ninh thông tin; nâng cao ý thức cảnh giác và trách nhiệm, đảm bảo an toàn, an ninh thông tin tại Ban.

2. Khi phát hiện sự cố gây mất an toàn, an ninh thông tin phải báo ngay cho lãnh đạo phòng, đơn vị và cán bộ chuyên trách công nghệ thông tin để kịp thời ngăn chặn, xử lý.

3. Tự quản lý, bảo quản thiết bị CNTT mà mình được giao sử dụng; không tự ý thay đổi, tháo lắp các thiết bị trên máy tính, các máy tính khi không sử dụng trong thời gian dài (quá 2 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 của Ban.

4. Không truy cập vào những trang web có nội dung không lành mạnh, không mở những thư điện tử không rõ địa chỉ người gửi; 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.

5. Tích cực phối hợp với cán bộ chuyên trách công nghệ thông tin và các cơ quan, đơn vị, tổ chức có liên quan trong điều tra làm rõ các nguyên nhân gây ra sự cố mất an toàn, an ninh thông tin của cơ quan, đơn vị.

6. Cung cấp mật khẩu Wifi cho tổ chức, cá nhân, doanh nghiệp đến liên hệ công tác tại Sở khi tổ chức, cá nhân, doanh nghiệp có yêu cầu và phải đảm bảo theo quy định tại Điều 12 quy chế này.

Điều 12. Trách nhiệm của cán bộ phụ trách CNTT

1. Được đảm bảo điều kiện về đào tạo, bồi dưỡng, học tập, nghiên cứu, tiếp thu kiến thức, kỹ thuật và công nghệ mới đối với lĩnh vực an toàn, an ninh thông tin.

2. Kịp thời tham mưu Lãnh đạo Sở những quy định, hướng dẫn có liên quan đến công tác đảm bảo an toàn, an ninh thông tin do cơ chuyên môn hướng dẫn.

3. Trực tiếp vận hành và duy trì hoạt động máy chủ, hệ thống mạng internet, mạng wifi của cơ quan đảm bảo cho hệ thống hoạt động thông suốt. Quản lý chặt chẽ việc di chuyển các trang thiết bị như: máy trạm, thiết bị ngoại vi,...

4. Trực tiếp quản lý thiết bị đầu cuối để kết nối internet và hệ thống mạng wifi, thực hiện thiết lập mật khẩu truy cập đủ mạnh cho hệ thống wifi của cơ quan.

5. Là đầu mối thực hiện cấp phát, thu hồi, cập nhật và quản lý các tài khoản truy cập vào hệ thống thông tin của Sở theo sự phân công của Lãnh đạo Sở; hướng dẫn người dùng thay đổi mật khẩu cá nhân theo quy định.

6. 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.

7. 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 khi có yêu cầu của Lãnh đạo Sở và các cơ quan chuyên môn.

8. Tích cực phối hợp với các cơ quan chức năng trong điều tra làm rõ các nguyên nhân gây ra sự cố mất an toàn, an ninh thông tin của cơ quan, đơn vị.

Điều 13. Trách nhiệm của các tổ chức, cá nhân, doanh nghiệp khi đến liên hệ công tác

1. Tổ chức, cá nhân, doanh nghiệp chỉ được truy cập mạng internet qua các thiết bị phát sóng không dây (wifi). Khi được sử dụng mạng internet của Sở không được truyền bá các luồng tư tưởng, văn hóa, vi phạm thuần phong mỹ tục Việt Nam, có tính chất kích động, chống phá lại các chủ trương, đường lối, chính sách của Đảng và Nhà nước.

2. Khi đem trang thiết bị tin học vào sử dụng mạng có dây tại Sở phải được chấp thuận của Lãnh đạo Văn phòng và tùy theo mức độ trách nhiệm của tổ chức, cá nhân, doanh nghiệp mà Lãnh đạo Văn phòng sẽ yêu cầu cán bộ chuyên trách công nghệ thông tin của Sở trợ giúp về mặt kỹ thuật để thực hiện.

Chương IV
ĐIỀU KHOẢN THI HÀNH

Điều 14. Khen thưởng, kỷ luật

1. 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.

2. Các phòng chuyên môn, đơn vị trực thuộc; cán bộ, công chức, viên chức có hành vi vi phạm Quy chế này hoặc quy định khác của pháp luật về an toàn, an ninh thông tin 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.

3. Văn phòng Sở căn cứ vào các quy định của Pháp luật về thi đua, khen thưởng để trình Lãnh đạo Sở xem xét hạ bậc thi đua, không xét khen thưởng cho các phòng, đơn vị trực thuộc và CB, CC, VC, NLĐ vi phạm quy định của Quy chế này.

Điều 15. Tổ chức thực hiện

1. Văn phòng Sở chủ trì, tổ chức triển khai, theo dõi, kiểm tra, hướng dẫn thực hiện quy chế này; hàng năm tổng hợp, báo cáo Lãnh đạo Sở và các cơ quan chức năng khi có yêu cầu.

2. Lãnh đạo các phòng, đơn vị trực thuộc tổ chức triển khai thực hiện Quy chế này trong phạm vi quản lý của mình. Trong quá trình thực hiện, nếu gặp vướng mắc phản ánh về Sở (qua Văn phòng tổng hợp), báo cáo Lãnh đạo Sở xem xét, chỉ đạo kịp thời.

3. CBCCVC, NLĐ của cơ quan nghiêm túc thực hiện Quy chế này.

GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ GIAO THÔNG VẬN TẢI
TỈNH HƯNG YÊN

Trần Minh Hải