UBND TỈNH THỪA THIÊN HUẾ
SỞ GIAO THÔNG VẬN TẢI

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

Số: 2154 /QĐ-SGTVT

Thừa Thiên Huế, ngày 15 tháng 10 năm 2024

QUYẾT ĐỊNH
Ban hành Bảo đảm an toàn, an ninh mạng
"Hệ thống Mạng nội bộ (LAN) của Sở Giao thông vận tải Thừa Thiên Huế"

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

Căn cứ 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 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ trưởng 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 2688/QĐ-UBND ngày 13/11/2023 của UBND tỉnh Thừa Thiên Huế Ban hành Quy chế Bảo đảm an toàn Hệ thống thông tin tại Trung tâm dữ liệu tỉnh Thừa Thiên Huế;

Căn cứ Quyết định số 34/2022/QĐ-UBND ngày 03/8/2022 của UBND tỉnh Thừa Thiên Huế Ban hành quy định quản lý, vận hành và khai thác mạng tin học diện rộng tỉnh Thừa Thiên Huế;

Căn cứ Quyết định số 68/2021/QĐ-UBND ngày 22/11/2021 của UBND tỉnh Thừa Thiên Huế về việc quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Sở Giao thông Vận tải;

Theo đề nghị của Chánh Văn phòng Sở.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Bảo đảm an toàn, an ninh mạng Hệ thống Mạng nội bộ (LAN) của Sở Giao thông vận tải tỉnh Thừa Thiên Huế.

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

Điều 3. Chánh Văn phòng Sở, Trưởng các phòng chuyên môn, thủ trưởng các đơn vị liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như điều 3;
- Sở TTTT;
- Trung tâm IOC;
- Lưu: VT.

GIÁM ĐỐC

SỞ GIAO THÔNG VẬN TẢI

Lê Anh Tuấn

UBND TỈNH THỪA THIÊN HUẾ
SỞ GIAO THÔNG VẬN TẢI

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

QUY CHẾ
Bảo đảm an toàn, an ninh mạng
Hệ thống Mạng nội bộ (LAN) của Sở Giao thông vận tải tỉnh Thừa Thiên Huế

(Ban hành kèm theo Quyết định số 2154 /QĐ-SGTVT ngày 15 tháng 10 năm 2024)

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 các chính sách quản lý và các biện pháp nhằm bảo đảm an toàn thông tin cho Hệ thống Mạng nội bộ của Sở Giao thông vận tải tỉnh Thừa Thiên Huế bao gồm:

- Phạm vi quản lý về vật lý và logic của của cơ quan;

- Các ứng dụng, dịch vụ hệ thống cung cấp;

- Nguồn nhân lực bảo đảm an toàn thông tin.

2. Đối tượng áp dụng

a) Cán bộ, công chức, viên chức và người lạo động trong cơ quan, đơn vị trực thuộc Sở Giao thông vận tải.

b) Cơ quan, đơn vị, cá nhân có kết nối, sử dụng Hệ thống Mạng nội bộ.

c) Cơ quan, đơn vị, cá nhân cung cấp dịch vụ quản lý, vận hành, duy trì, phát triển và bảo đảm an toàn thông tin mạng phục vụ hoạt động của Hệ thống Mạng nội bộ.

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, 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. Mạng: là môi trường trong đó thông tin được cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông qua mạng viễn thông và mạng máy tính.

3. Hệ thống thông tin: là tập hợp 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 trên mạng.

4. 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…

5. Chủ quản hệ thống thông tin là cơ quan, tổ chức, cá nhân có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin.

6. Đơn vị vận hành hệ thống thông tin là cơ quan, tổ chức được chủ quản hệ thống thông tin giao nhiệm vụ vận hành hệ thống thông tin.

7. Đơn vị chuyên trách về an toàn thông tin là đơn vị có chức năng, nhiệm vụ bảo đảm an toàn thông tin của chủ quản hệ thống thông tin.

8. Hệ thống thông tin quan trọng là hệ thống thông tin khi phát sinh sự cố sẽ làm tổn hại nghiêm trọng đến hoạt động của cơ quan, đơn vị.

9. Rủi ro an toàn thông tin là những nhân tố chủ quan hoặc khách quan có khả năng ảnh hưởng đến trạng thái an toàn thông tin mạng.

10. Phần mềm độc hại (mã độc) 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.

11. Sự cố an toàn thông tin mạng là việc thông tin, hệ thống thông tin bị gây nguy hại, ảnh hưởng đến tính toàn vẹn, tính bảo mật và tính khả dụng.

12. Tài khoản người dùng là một tập hợp thông tin đại diện duy nhất cho người sử dụng trên hệ thống thông tin, người dùng sử dụng để đăng nhập và truy cập các tài nguyên được cấp phép trên hệ thống thông tin đó. Tài khoản người dùng ít nhất phải bao gồm tên định danh và mã khóa bí mật.

13. Tính bảo mật của thông tin là đảm bảo thông tin chỉ được tiếp cận bởi những người được cấp quyền tương ứng.

14. Tính toàn vẹn của thông tin là bảo vệ sự chính xác và đầy đủ của thông tin và thông tin chỉ được thay đổi bởi những người được cấp quyền.

15. Tính sẵn sàng của thông tin là đảm bảo những người được cấp quyền có thể truy xuất thông tin ngay khi có nhu cầu

16. Bên thứ ba là các tổ chức, cá nhân có chuyên môn được đơn vị thuê hoặc hợp tác với đơn vị nhằm cung cấp sản phẩm, dịch vụ kỹ thuật cho hệ thống công nghệ thông tin.

17. Thiết bị di động là thiết bị số có thể cầm tay, có hệ điều hành, có khả năng xử lý, kết nối mạng và có màn hình hiển thị như máy tính xách tay, máy tính bảng, điện thoại di động thông minh.

18. Trung tâm dữ liệu bao gồm hạ tầng kỹ thuật (nhà trạm, hệ thống cáp) và hệ thống máy tính cùng các thiết bị phụ trợ được lắp đặt vào đó để lưu trữ, trao đổi và quản lý tập trung dữ liệu của một hay nhiều tổ chức, cá nhân.

19. Vật mang tin là các phương tiện vật chất dùng để lưu giữ và truyền nhận thông tin điện tử.

20. 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.

21. Điểm yếu về mặt kỹ thuật là vị trí trong hệ thống thông tin dễ bị khai thác, lợi dụng khi bị tấn công hoặc xâm nhập bất hợp pháp.

Điều 3. Mục tiêu, nguyên tắc bảo đảm an toàn thông tin

1. Mục tiêu bảo đảm an toàn thông tin

Bảo vệ thông tin, 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 Hệ thống Mạng nội bộ.

2. Nguyên tắc

a) Cơ quan, đơn vị thuộc đối tượng áp dụng Quy chế này có trách nhiệm bảo đảm an toàn thông tin và hệ thống thông tin trong phạm vi xử lý công việc của mình theo quy định của pháp luật, hướng dẫn của cơ quan, đơn vị có thẩm quyền và các quy định tại Quy chế này.

b) Bảo đảm an toàn thông tin (ATTT) là yêu cầu bắt buộc, phải được thực hiện thường xuyên, liên tục trong quá trình:

i. Thu thập, tạo lập, xử lý, truyền tải, lưu trữ và sử dụng thông tin, dữ liệu.

ii. Thiết kế, thiết lập và vận hành, nâng cấp, hủy bỏ hệ thống thông tin.

c) Việc bảo đảm an toàn Hệ thống Mạng nội bộ được thực hiện một cách tổng thể, đồng bộ, tập trung trong việc đầu tư các giải pháp bảo vệ, có sự dùng chung, chia sẻ tài nguyên để tối ưu hiệu năng, tránh đầu tư thừa, trùng lặp.

Điều 4. Những hành vi nghiêm cấm

Các hành vi bị nghiêm cấm quy định tại Điều 7 Luật An toàn thông tin mạng và Điều 8 Luật An ninh mạng.

Điều 5. Phối hợp với những cơ quan/tổ chức có thẩm quyền

1. Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin:

Văn phòng Sở chuyên trách là đầu mối liên hệ, phối hợp các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin phục vụ việc bảo đảm an toàn, an ninh mạng cho Hệ thống Mạng nội bộ của cơ quan.

2. Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin:

a) Sở Thông tin và Truyền thông tỉnh Thừa Thiên Huế

- Người liên hệ/bộ phận: Phòng Giám sát, điều hành an toàn, an ninh mạng.

+ Số điện thoại: 0234 3940 999

+ Email: tiepnhan@thuathienhue.gov.vn

b) Cục An toàn thông tin/Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC)

- Người liên hệ/bộ phận: Phòng Ứng cứu sự cố

- Số điện thoại: 0869 100 317

- Email: ir@vncert.vn

- Báo cáo sự cố qua nền tảng điều phối, xử lý sự cố an toàn thông tin mạng quốc gia: https://irlab.vn

- Báo cáo sự cố qua website của VNCERT/CC: https://vncert.vn

Điều 6. Bảo đảm nguồn nhân lực

1. Tuyển dụng

Cán bộ được tuyển dụng vào vị trí làm về an toàn thông tin có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, an toàn thông tin, phù hợp với vị trí tuyển dụng.

2. Trong quá trình làm việc

a) Trách nhiệm bảo đảm an toàn thông tin cho người sử dụng, cán bộ quản lý và vận hành hệ thống:

- Với người sử dụng:

+ Người sử dụng có trách nhiệm đảm bảo ATTT đối với từng vị trí công việc.

+ Phải được thường xuyên tổ chức quán triệt các quy định về ATTT, nhằm nâng cao nhận thức về trách nhiệm đảm bảo ATTT.

+ Phải có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng; không tự ý thay đổi, tháo lắp thiết bị.

- Với cán bộ quản lý và vận hành hệ thống

+ Cán bộ quản lý và vận hành hệ thống phải thiết lập phương pháp hạn chế truy cập mạng không dây, giám sát và điều khiển truy cập không dây, tổ chức sử dụng chứng thực và mã hóa để bảo vệ truy cập không dây tới hệ thống thông tin.

+ Cán bộ quản lý và vận hành hệ thống phải tổ chức quản lý định danh đối với tất cả người dùng tham gia sử dụng hệ thống thông tin.

b) Định kỳ hàng năm tổ chức hoặc tham gia phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin cho người sử dụng do đơn vị chắc năng tổ chức.

3. Chấm dứt thay đổi công việc

a) Cán bộ chấm dứt hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác (nếu có) thuộc sở hữu của tổ chức;

b) Bộ phận chuyên trách thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc.

Chương II:
BẢO ĐẢM AN TOÀN THÔNG TIN TRONG QUẢN LÝ THIẾT KẾ, XÂY DỰNG HỆ THỐNG

Điều 7. Thiết kế an toàn hệ thống thông tin

1. Bộ phận chuyên trách xây dựng tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin và thuyết minh trong Hồ sơ đề xuất cấp độ của hệ thống.

2. Bộ phận chuyên trách xây dựng tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin thuyết minh trong Hồ sơ đề xuất cấp độ của hệ thống.

Điều 8. Thử nghiệm và nghiệm thu hệ thống

1. Bên triển khai xây dựng kế hoạch, nội dung thử nghiệm hệ thống trước khi thực hiện thử nghiệm và nghiệm thu hệ thống.

2. Đơn vị vận hành thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác theo phương án thiết kế được phê duyệt trong Hồ sơ đề xuất cấp độ.

Chương III:
BẢO ĐẢM AN TOÀN THÔNG TIN TRONG QUẢN LÝ VẬN HÀNH HỆ THỐNG

Điều 9. Quản lý an toàn mạng

1. Hệ thống mạng phải được thiết kế thống nhất, được quản lý định danh, xác thực đối với tất cả người sử dụng nhằm mục đích quản lý và bảo đảm an toàn và bảo mật.

2. Hệ thống mạng nội bộ (LAN) phải được bảo vệ bằng tường lửa (có thể tích hợp tường lửa trên modem hoặc router) và phân chia hệ thống mạng thành các vùng mạng quản lý theo chính sách an toàn thông tin riêng.

3. Mạng không dây (WIFI), cần thiết lập các thông số an toàn và định kỳ ít nhất 3 tháng thay đổi mật khẩu truy cập nhằm tăng cường công tác bảo mật. Hệ thống mạng không dây phải được bảo vệ bởi mật khẩu an toàn và phải tách biệt hoàn toàn với hệ thống mạng tin học diện rộng của tỉnh.

Điều 10. Quản lý an toàn máy chủ và ứng dụng

1. Máy chủ phải được thiết lập chính sách xác thực và kiểm soát truy cập. Các hệ thống thông tin cần có phướng án giới hạn số lần đăng nhập, tự động khóa tài khoản khi liên tục đăng nhập sai vượt quá số lần quy định. Tổ chức theo dõi, giám sát tất cả các phương pháp đăng nhập từ xa, nhất là các trường hợp đăng nhập vào hệ thống với mục đích quản trị.

2. Kiểm tra, giám sát các hoạt động liên quan đến các nơi lưu trữ mật khẩu và cảnh báo khi có những hành động bất thường (Ví dụ: user không có quyền nhưng cố tình truy xuất đến các file lưu mật khẩu…).

Điều 11. Quản lý an toàn dữ liệu

1. Có cơ chế sao lưu dữ liệu dự phòng, lưu trữ dữ liệu tại nơi an toàn đồng thời thường xuyên kiểm tra để đảm bảo sẵn sàng phục hồi nhằm ngăn ngừa và hạn chế khi sự cố an toàn thông tin mạng xảy ra. Dữ liệu trên máy chủ được sao lưu thông qua hệ

thống sao lưu dữ liệu.

2. Định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ và các thông tin, dữ liệu quan trọng khác trên hệ thống theo yêu cầu của đơn vị vận hành.

3. Quyền truy cập phải được phân ra theo từng cấp độ tương ứng với từng nhiệm vụ của nhân viên và phải được phê duyệt từ cấp trên.

Điều 12. Quản lý an toàn người sử dụng đầu cuối

Chính sách, quy trình quản lý an toàn người sử dụng đầu cuối bao gồm:

1. Việc sử dụng các thiết bị lưu trữ ngoài như ổ cứng di động, các loại thẻ nhớ, thiết bị lưu trữ USB,... phải thường xuyên quét virus trước khi đọc hoặc sao chép dữ liệu.

2. Không sử dụng các máy tính thuộc sở hữu cá nhân (máy xách tay của cá nhân, PDA) hoặc những thiết bị lưu trữ di động cá nhân vào mục đích kinh doanh của công ty. Hạn chế tối đa việc sử dụng các thiết bị lưu trữ ngoài để sao chép, di chuyển dữ liệu.

3. Các thiết bị đầu cuối khi kết nối phải được quản lý và cập nhật thông tin (tên theo nguyên tắc: *<viết tắt của họ và tên đệm>+<tên>-<tên của cơ quan, đơn vị, địa phương đang công tác>*, chủng loại, địa chỉ MAC, địa chỉ IP, thiết lập mật khẩu đăng nhập), cập nhật các bản vá lỗi bảo mật đầy đủ, cài đặt chương trình phần mềm phòng chống virus, mã độc tập trung, phần mềm Phát hiện và phản ứng sự cố an toàn thông tin. Cần sử dụng cơ chế xác thực và sử dụng giao thức mạng an toàn

4. Bộ phận chuyên trách về an toàn thông tin phải thường xuyên theo dõi, kiểm tra các lỗ hổng bảo mật và quản lý kết nối, truy cập khi sử dụng thiết bị đầu cuối từ xa.

5. Bộ phận chuyên trách về an toàn thông tin thường xuyên theo dõi cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống đối với các nhân viên đã nghỉ việc.

6. Bộ phận chuyên trách về an toàn thông tin thường xuyên theo dõi cấu hình tối ưu và tăng cường bảo mật (cứng hóa) cho máy tính người sử dụng và thực hiện quy trình trước khi đưa hệ thống vào sử dụng.

7. Việc bảo trì, sửa chữa máy tính, thiết bị bảo mật, thiết bị mạng, thiết bị lưu trữ của Sở Giao thông vận tải do Văn phòng Sở có trách nhiệm thường xuyên kiểm tra hiện trạng, hướng dẫn sử dụng, quản lý, vận hành hệ thống hạ tầng kỹ thuật của Sở; đề xuất quy trình bảo dưỡng, bảo trì, sửa chữa hoặc mua sắm thiết bị (bao gồm cả thiết bị đang hoạt động và thiết bị dự phòng) phù hợp, an toàn, bảo mật theo quy định về quản lý, sử dụng tài sản cơ quan

Điều 13. Quản lý rủi ro an toàn thông tin mạng

Đơn vị vận hành xây dựng và ban hành Hồ sơ Quản lý rủi ro an toàn thông tin bao gồm các nội dung sau:

1. Danh mục tài sản thông tin, dữ liệu có trong hệ thống.

2. Đánh giá các rủi ro an toàn thông tin đối với mỗi loại tài sản.

3. Có phương án dự phòng và khôi phục sau sự cố đối với thông tin, dữ liệu và ứng dụng.

Điều 14. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ

Quy định, quy trình về Kết thúc vận hành, khai thác, thanh lý, hủy bỏ bao gồm các nội dung sau:

1. Thiết bị CNTT có chứa dữ liệu (máy tính, thiết bị lưu trữ, ...) khi bị hỏng phải được cán bộ vận hành kiểm tra, sửa chữa, khắc phục. Phải có biện pháp kiểm tra, giám sát đảm bảo không để lọt lộ thông tin hay lây nhiễm mã độc đối với máy tính mang ra bên ngoài sửa chữa, bảo hành.

2. Trước khi tiến hành thanh lý/loại bỏ thiết bị công nghệ thông tin cũ, phải áp dụng các biện pháp kỹ thuật xoá bỏ hoàn toàn dữ liệu người dùng đã tạo ra, đảm bảo không thể phục hồi.

3. Các phương tiện và thiết bị CNTT: Máy tính cá nhân (PC), máy tính xách tay, máy chủ, các thiết bị mạng, phương tiện lưu trữ như CD/DVD, thẻ nhớ, ổ cứng phải xóa sạch dữ liệu khi chuyển giao hoặc thay đổi mục đích sử dụng.

Chương IV:
TỔ CHỨC BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 15. Trách nhiệm của lãnh đạo Sở

1. Chịu trách nhiệm toàn diện trước UBND tỉnh trong công tác bảo đảm an toàn, an ninh thông tin và công tác bảo vệ bí mật nhà nước, bảo vệ bí mật nội bộ trong quá trình vận hành, khai thác và sử dụng hệ thống thông tin tại cơ quan.

2. Chỉ đạo phổ biến những kiến thức về an toàn, an ninh thông tin cho CC-VC-NLĐ tham gia sử dụng hệ thống thông tin. Thực hiện và chỉ đạo công chức thuộc thẩm quyền quản lý thực hiện nghiêm túc Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng CNTT tại Sở GTVT.

3. Khi có sự cố hoặc nguy cơ mất an toàn, an ninh thông tin phải chỉ đạo khắc phục sự cố kịp thời và hạn chế thấp nhất mức thiệt hại có thể xảy ra, ưu tiên sử dụng lực lượng kỹ thuật tại chỗ của đơn vị mình.

Điều 16. Trách nhiệm của lãnh đạo các phòng, đơn vị

1. Lãnh đạo các phòng, đơn vị chịu trách nhiệm trước lãnh đạo Sở trong công tác đảm bảo an toàn, an ninh thông tin và công tác bảo vệ bí mật nhà nước, bảo vệ bí mật nội bộ thuộc phạm vi quản lý.

2. Phổ biến những kiến thức về an toàn, an ninh thông tin cho công chức, viên chức thuộc quyền quản lý trước khi tham gia sử dụng hệ thống thông tin. Thực hiện và chỉ đạo công chức, viên chức thuộc quyền quản lý thực hiện nghiêm túc Quy chế này và các quy định khác của pháp luật.

3. Tạo điều kiện thuận lợi cho công chức, viên chức thuộc thẩm quyền quản lý của mình được tham gia các lớp tập huấn, tuyên truyền, hội nghị, hội thảo chuyên đề

về an toàn thông tin do các cấp tổ chức.

4. Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin và các vụ lộ, lọt bí mật nhà nước trong hoạt động ứng dụng CNTT của cơ quan phải thông báo kịp thời cho cán bộ phụ trách CNTT của Sở, lãnh đạo Sở để kịp thời ngăn chặn, xử lý.

5. Chủ động phối hợp với cá nhân, đơn vị có liên quan trong việc kiểm tra, phát hiện và khắc phục sự cố về an toàn, an ninh thông tin và các vụ lộ, lọt bí mật nhà nước trong hoạt động ứng dụng CNTT. Tuân thủ theo sự hướng dẫn kỹ thuật của các đơn vị liên quan trong quá trình khắc phục sự cố về an toàn thông tin.

Điều 17. Trách nhiệm của công chức, viên chức

1. Nâng cao ý thức cảnh giác và trách nhiệm về an toàn, an ninh thông tin. Nghiêm chỉnh thực hiện Quy chế này, đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng CNTT của Sở Giao thông vận tải tỉnh Thừa Thiên Huế và các quy định khác của pháp luật.

2. Khi phát hiện nguy cơ hoặc sự cố mất an toàn, an ninh thông tin và các vụ lộ, lọt bí mật nhà nước trong hoạt động ứng dụng CNTT của cơ quan phải báo cáo kịp thời cho cán bộ phụ trách CNTT để kịp thời ngăn chặn, xử lý.

3. Tham gia các lớp tập huấn, tuyên truyền, hội nghị, hội thảo chuyên đề về an toàn thông tin do các cấp tổ chức.

Điều 18. Trách nhiệm của công chức phụ trách công nghệ thông tin

1. Phân công công chức chuyên trách CNTT tại Văn phòng Sở là đầu mối liên hệ khi có sự cố về ATTT để phối hợp thực hiện.

2. Chịu trách nhiệm triển khai các biện pháp quản lý vận hành, quản lý kỹ thuật cho toàn bộ hệ thống thông tin của cơ quan.Tham mưu báo cáo về tình hình an toàn thông tin tại cơ quan.

3. Chủ động phối hợp với cá nhân, đơn vị có liên quan trong việc giám sát, kiểm tra, phát hiện và khắc phục sự cố về an toàn thông tin và các vụ lộ, lọt bí mật nhà nước trong hoạt động ứng dụng CNTT.

Điều 19. Khen thưởng, xử lý vi phạm

1. Tập thể, cá nhân thuộc Sở thực hiện tốt Quy chế này, mang lại hiệu quả thiết thực sẽ được xem xét, đánh giá, đề xuất khen thưởng.

2. Tập thể, cá nhân có hành vi vi phạm quy chế này thì tuỳ 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 theo quy định của Nhà nước. Nếu gây thiệt hại thì bồi thường theo quy định của pháp luật hiện hành.

Điều 20. Tổ chức thực hiện

Trong quá trình thực hiện, nếu có những vấn đề vướng mắc phát sinh cần sửa đổi, bổ sung; các phòng, đơn vị, công chức, viên chức phản ánh về Văn phòng Sở để tổng hợp, báo cáo Ban Giám đốc Sở xem xét, sửa đổi, bổ sung Quy chế cho phù hợp./.