UBND TỈNH TÂY NINH
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 trong hoạt động ứng dụng công nghệ thông tin của Sở Giao thông vận tải tỉnh Tây Ninh

(Ban hành kèm theo Quyết định số: 190/QĐ-SGTVT ngày 29 tháng 7 năm 2022)

Chương I

QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định về công tác đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin (CNTT) phục vụ cho công tác điều hành và quản lý hành chính nhà nước của Sở Giao thông vận tải Tây Ninh.

Điều 2. Đối tượng áp dụng

Quy chế này được áp dụng đối với các phòng, đơn vị và tất cả công chức, viên chức thuộc Sở Giao thông vận tải tỉnh Tây Ninh.

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

1. Việc áp dụng Quy chế này nhằm giảm thiểu được các nguy cơ gây mất an toàn thông tin (ATTT) và đảm bảo an ninh thông tin trong quá trình ứng dụng CNTT trong hoạt động của cơ quan.

2. Đảm bảo an toàn thông tin là yêu cầu bắt buộc trong quá trình tạo lập, xử lý, sử dụng thông tin và quá trình thiết kế, xây dựng, vận hành, nâng cấp, bảo trì các hạ tầng kỹ thuật CNTT.

3. Công chức, viên chức các phòng, đơn vị phải được phổ biến kiến thức chung về an toàn thông tin trên môi trường máy tính, mạng máy tính phù hợp với công việc được phân công.

4. Công tác đảm bảo ATTT mạng phải được thực hiện trên cơ sở có sự phối hợp chặt chẽ giữa các phòng, đơn vị và công chức, viên chức thuộc Sở.

5. Đảm bảo bố trí ít nhất một máy tính không có kết nối Internet để soạn thảo văn bản, lưu giữ thông tin có nội dung mật theo quy định. Các thiết bị viễn thông, máy tính được sử dụng để lưu giữ và truyền thông tin bí mật nhà nước phải được cơ quan chức năng hướng dẫn trước khi đưa vào sử dụng.

6. Cơ quan phải có phương án tổ chức sao lưu dữ liệu đối với các dữ liệu quan trọng.

7. Các thiết bị viễn thông, máy tính có chứa tài liệu của cơ quan nhà nước khi đưa đi công tác nước ngoài phải thực hiện theo quy định của pháp luật về bảo vệ bí mật nhà nước.

Điều 4. Các hành vi bị nghiêm cấm

1. Tạo ra, cài đặt, phát tán vi rút máy tính, phần mềm độc hại trái pháp luật.

2. Xâm nhập, sửa đổi, xóa bỏ nội dung thông tin của cơ quan, cá nhân khác.

3. Cản trở hoạt động cung cấp dịch vụ của hệ thống thông tin.

4. Ngăn chặn việc truy nhập đến thông tin của cơ quan, cá nhân khác trên môi trường mạng, trừ trường hợp pháp luật cho phép.

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. Hành vi khác làm mất an toàn, bí mật thông tin của cơ quan, cá nhân khác được trao đổi, lưu trữ,… trên môi trường mạng.

Chương II

NỘI DUNG BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Điều 5. Quản lý máy tính và thiết bị CNTT

1. Máy tính và thiết bị CNTT được trang bị tại các phòng, đơn vị thuộc Sở Giao thông vận tải tỉnh Tây Ninh là tài sản của Nhà nước, được quản lý, sử dụng theo quy định của pháp luật. Công chức, viên chức có trách nhiệm quản lý thiết bị được giao.

2. 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 6. Quản lý, khai thác, sử dụng cơ sở dữ liệu và phần mềm

1. Văn phòng Sở có trách nhiệm xây dựng quy chế vận hành, khai thác sử dụng các phần mềm, ứng dụng CNTT tại Sở theo quy định; Phối hợp các phòng, đơn vị nghiên cứu, đề xuất, phát triển cơ sở dữ liệu, phần mềm theo quy định quản lý nhà nước của ngành và tuân theo quy định của Nhà nước.

2. Các phòng, đơn vị thuộc Sở và toàn thể công chức, viên chức có trách nhiệm phối hợp với Văn phòng Sở trong quá trình triển khai xây dựng, phát triển vào bảo vệ hệ thống cơ sở dữ liệu, phần mềm theo quy định của pháp luật.

Điều 7. Bảo đảm an toàn thông tin khi sử dụng máy tính và thiết bị công nghệ thông tin

1. Công chức, viên chức sử dụng máy tính để xử lý công việc tuân thủ các quy định về cài đặt phần mềm, chỉ cài đặt các phần mềm hợp lệ và các phần mềm thuộc danh mục phần mềm được phép sử dụng. Kiểm soát chặt chẽ việc cài đặt các phần mềm mới lên máy tính, thiết bị CNTT. Các phần mềm phải được thường xuyên theo dõi, cập nhật bản vá lỗi bảo mật của nhà phát triển.

2. Cài đặt các phần mềm chống mã độc có bản quyền và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm, thực hiện quét dữ liệu thường xuyên để tránh tình trạng nhiễm virus khi sử dụng máy tính. Khi phát hiện bất kì dấu hiệu nào liên quan đến việc bị nhiễm virus, công chức, viên chức phải báo ngay cho cán bộ phụ trách về CNTT để được hướng dẫn thao tác xử lý kịp thời.

3. Sử dụng các trình duyệt an toàn, không truy cập hoặc mở các trang tin, thư điện tử không rõ nguồn gốc; máy tính cá nhân phải được thiết lập mật khẩu; thực hiện thao tác khóa máy tính khi rời khỏi nơi đặt máy tính; tắt máy tính khi rời khỏi cơ quan.

4. Phải sử dụng hộp thư điện tử công vụ có tên miền @tayninh.gov.vn khi thực hiện xử lý công việc trên môi trường mạng hoặc hộp thư điện tử có tên miền đặc thù theo quy định của ngành nhưng vẫn phải đảm bảo tính an toàn, bảo mật tránh xảy ra tình trạng lộ, lọt thông tin.

5. Về 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.

b) Trường hợp cá nhân thay đổi vị trí công tác, chuyển công tác, thôi việc hoặc nghỉ hưu, phòng, đơn vị quản lý cá nhân đó phải phối hợp với Văn phòng Sở thông báo, điều chỉnh/ thu hồi/ hủy bỏ tài khoản và các quyền sử dụng đối với hệ thống thông tin.

c) Cá nhân có trách nhiệm bảo mật tài khoản truy nhập thông tin, không chia sẻ mật khẩu, thông tin cá nhân với người khác. Đặt mật khẩu với độ an toàn cao (có chữ thường, có chữ in hoa, có số và ký tự đặc biệt như @, #, !) và khuyến khích thay đổi mật khẩu ít nhất 03 tháng/lần; các tài khoản đăng nhập các hệ thống phải được đăng xuất khi không sử dụng; thường xuyên xóa các biểu mẫu, mật khẩu, bộ nhớ cache và cookie trong trình duyệt trên máy tính.

d) Tạm dừng quyền sử dụng đối với tài khoản đã được đăng ký trên hệ thống nhưng không làm việc trong hệ thống từ 30 ngày trở lên.

Điều 8. Bảo đảm an toàn thông tin đối với mạng máy tính

1. Quản lý hệ thống mạng nội bộ (LAN):

a) Mạng nội bộ khi kết nối với mạng Internet phải phải được quản lý giám sát bởi các hệ thống thiết bị mạng, thiết bị bảo mật.

b) Có phân chia hệ thống mạng nội bộ thành các vùng mạng theo phạm vi truy cập, vô hiệu hóa tất cả các dịch vụ không sử dụng tại từng vùng mạng, thực hiện nguyên tắc chỉ mở các dịch vụ cần thiết khi có yêu cầu.

2. Quản lý hệ thống mạng không dây (Wifi): Khi thiết lập mạng không dây có kết nối vào mạng nội bộ phải thiết lập các thông số cần thiết như định danh, mật mã, mã hóa dữ liệu, có thay đổi mật mã định kỳ.

3. Quản lý truy cập từ xa vào mạng nội bộ: Đối với việc truy cập từ xa vào mạng nội bộ phải được theo dõi, quản lý chặt chẽ, nhất là truy cập có sử dụng chức năng quản trị, phải thiết lập mật mã độ an toàn cao, thường xuyên thay đổi mật mã, hạn chế truy cập từ xa vào mạng nội bộ từ các điểm truy cập Internet công cộng.

Điều 9. Bảo đảm an toàn, cơ chế sao lưu, phục hồi thông tin, dữ liệu

1. Thông tin, dữ liệu khi được lưu trữ, khai thác, trao đổi phải được đảm bảo tính toàn vẹn, tính tin cậy, tính sẵn sàng. Thông tin, dữ liệu quan trọng khi được lưu trữ, trao đổi phải áp dụng kỹ thuật mã hóa, thiết lập mật mã, ứng dụng chữ ký số và phải có cơ chế sao lưu dự phòng.

2. Công chức, viên chức có giải pháp sao lưu định kỳ dữ liệu công việc cá nhân. Riêng đối với dữ liệu quan trọng, phải thực hiện sao lưu bằng thiết bị lưu trữ dữ liệu di động để phục vụ cho việc phục hồi dữ liệu khi có sự cố xảy ra; cá nhân phải có trách nhiệm bảo vệ thiết bị này và thông tin trên thiết bị để tránh làm mất hoặc lộ, lọt thông tin, dữ liệu.

3. Thiết bị có bộ phận lưu trữ hoặc thiết bị lưu trữ khi mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài cơ quan, đơn vị hoặc ngừng sử dụng phải được 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). Khi thanh lý thiết bị thì phải xóa nội dung lưu trữ bằng phần mềm hoặc thiết bị hủy dữ liệu chuyên dụng hay phá hủy vật lý.

Điều 10. Quản lý sự cố

1. Phân loại mức độ nghiêm trọng của các sự cố, bao gồm:

- Thấp: sự cố gây ảnh hưởng cá nhân và không làm gián đoạn hay đình trệ hoạt động chính của cơ quan, của các đơn vị khác trong tỉnh.

- Trung bình: sự cố ảnh hưởng đến một nhóm người dùng nhưng không gây gián đoạn hay đình trệ hoạt động chính của đơn vị, của các đơn vị khác của tỉnh.

- Cao: sự cố làm cho thiết bị, phần mềm hay hệ thống không thể sử dụng được và gây ảnh hưởng đến một trong các hoạt động chính của cơ quan, của các đơn vị khác của tỉnh.

- Khẩn cấp: Sự cố ảnh hưởng đến sự liên tục của nhiều hoạt động chính của cơ quan, của các đơn vị khác trong tỉnh.

2. Trường hợp có sự cố nghiêm trọng ở mức độ cao, khẩn cấp hoặc vượt quá khả năng khắc phục của cơ quan, lãnh đạo cơ quan phải báo cáo ngay cho các cơ quan chức năng (Đội ứng cứu ANTT tỉnh, Trung tâm Giám sát điều hành kinh tế xã hội tập trung tỉnh, Trung tâm ứng cứu sự cố máy tính Việt Nam VNCERT, Ủy ban nhân dân tỉnh, Bộ Thông tin và Truyền thông…) cùng phối hợp xử lý.

Điều 11: Kiểm tra, khắc phục sự cố an toàn thông tin

1. Phối hợp với các cơ quan chuyên môn rà soát, đánh giá và xác định các sự cố ATTT, các rủi ro ATTT có thể xảy ra với hệ thống thông tin trong phạm vi quản lý của đơn vị.

Trên cơ sở đó, xây dựng các phương án ứng cứu, xử lý sự cố phù hợp với các rủi ro ATTT có thể xảy ra.

2. Khi có sự cố hoặc nguy cơ mất ATTT, thực hiện quy trình các bước như sau:

a) Xác định nguyên nhân sự cố, có biện pháp khắc phục kịp thời, hạn chế thiệt hại.

b) Trường hợp gặp sự cố nghiêm trọng ở mức độ cao, khẩn cấp (hệ thống bị gián đoạn dịch vụ; dữ liệu tuyệt mật hoặc bí mật nhà nước có khả năng bị tiết lộ; dữ liệu quan trọng của hệ thống không bảo đảm tính toàn vẹn và không có khả năng khôi phục được; hệ thống bị mất quyền điều khiển) hoặc đơn vị không đủ khả năng tự kiểm soát, xử lý được sự cố thì phải phối hợp chặt chẽ với Đội ứng cứu sự cố ATTT mạng của tỉnh và cung cấp đầy đủ thông tin sự cố để được hướng dẫn, hỗ trợ cụ thể.

c) Chuẩn bị nội dung báo cáo sự cố theo quy định tại điểm c khoản 2 Điều 11 của Quy chế kèm theo Quyết định số 29/2021/QĐ-UBND ngày 15 tháng 12 năm 2021 của UBND tỉnh Tây Ninh.

d) Quy trình phối hợp ứng cứu sự cố mạng bảo đảm ATTT thực hiện theo quy định tại Điều 16 của Quy chế kèm theo Quyết định số 29/2021/QĐ-UBND ngày 15 tháng 12 năm 2021 của UBND tỉnh Tây Ninh.

Chương III

TỔ CHỨC THỰC HIỆN

Điều 12. 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 dụnghệ 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 13. 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 14. 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 Tây Ninh 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 15. Trách nhiệm của công chức phụ trách công nghệ thông tin

1. Phân công công chức chuyên trách CNTT là đầu mối liên hệ khi có sự cố về ATTT để phối hợp thực hiện: ông Nguyễn Nam Tư, số điện thoại (0948.800.278).

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 16. 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 17. 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./.