BỘ GIAO THÔNG VẬN TẢI	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Số: 2081 /QĐ-BGTVT	Độc lập - Tự do - Hạnh phúc

Hà Nội, ngày 17 tháng 7 năm 2017

QUYẾT ĐỊNH

Về việc ban hành Quy chế bảo đảm an toàn, an ninh thông tin mạng của Bộ Giao thông vận tải

BỘ TRƯỞNG BỘ GIAO THÔNG VẬN TẢI

Căn cứ Luật An toàn thông tin mạng số 86/2015/QH13 ngày 19/11/2015;

Căn cứ Luật Công nghệ thông tin số 67/2006/QH11 ngày 29/6/2006;

Căn cứ Luật Giao dịch điện tử số 51/2005/QH11 ngày 29/11/2005;

Căn cứ Nghị định số 12/2017/NĐ-CP ngày 10/2/2017 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Giao thông vận tải;

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 Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định 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 ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

Căn cứ Quyết định số 898/QĐ-TTg ngày 27/5/2016 của Thủ tướng Chính phủ phê duyệt phương hướng, mục tiêu, nhiệm vụ bảo đảm an toàn thông tin mạng giai đoạn 2016 - 2020;

Căn cứ Quyết định số 645/QĐ-BGTVT ngày 9/3/2017 của Bộ trưởng Bộ Giao thông vận tải phê duyệt Kế hoạch bảo đảm an toàn, an ninh thông tin của Bộ Giao thông vận tải đến năm 2020;

Theo đề nghị của Giám đốc Trung tâm Công nghệ thông tin,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn, an ninh thông tin mạng của Bộ Giao thông vận tải.

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

Điều 3. Chánh Văn phòng Bộ, Chánh Thanh tra Bộ, các Vụ trưởng, Giám đốc Trung tâm Công nghệ thông tin, Thủ trưởng các cơ quan, đơn vị, doanh nghiệp thuộc Bộ chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Các đồng chí Thứ trưởng;
- Lưu: VT, TTCNTT (03b).

BỘ TRƯỞNG

Trương Quang Nghĩa

BỘ GIAO THÔNG VẬN TẢI

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 BỘ GIAO THÔNG VẬN TẢI

(Ban hành kèm theo Quyết định số 2081/QĐ-BGTVT ngày 17 tháng 7 năm 2017 của Bộ trưởng Bộ Giao thông vận tải)

Chương I
QUY ĐỊNH CHUNG

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

1. Quy chế này quy định về bảo đảm an toàn, an ninh thông tin mạng (sau đây gọi tắt là an toàn thông tin) trong các hoạt động của Bộ Giao thông vận tải và các đơn vị thuộc Bộ.

2. Quy chế này áp dụng đối với các cơ quan, đơn vị, doanh nghiệp (gọi chung là đơn vị) thuộc Bộ Giao thông vận tải.

Điều 2. Giải thích từ ngữ

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

1. 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.

2. An toàn thông tin mạng là sự bảo vệ thông tin và các hệ thống thông tin tránh bị truy cập, 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.

3. Bên thứ ba là các tổ chức, cá nhân được đơn vị thuê hoặc hợp tác với đơn vị nhằm cung cấp hàng hóa, dịch vụ kỹ thuật cho hệ thống thông tin.

4. 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.

5. 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.

6. Hệ thống thông tin là tập hợp các thiết bị viễn thông, 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.

7. 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 đơn vị.

8. 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.

9. 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.

10. 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.

11. 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.

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

13. 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.

14. 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.

15. Tường lửa là tập hợp các thành phần hoặc một hệ thống các trang thiết bị, phần mềm được đặt giữa hai mạng, nhằm kiểm soát tất cả các kết nối từ bên trong ra bên ngoài mạng hoặc ngược lại.

16. 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.

17. 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.

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

Điều 3. Nguyên tắc chung

Nguyên tắc bảo đảm an toàn thông tin mạng phải tuân thủ các nguyên tắc tại Điều 4 của Luật An toàn thông tin mạng và Điều 4 của Nghị định số 85/2016/NĐ-CP, cụ thể:

1. Từng đơn vị thuộc Bộ Giao thông vận tải có trách nhiệm bảo đảm an toàn thông tin mạng của đơn vị mình, theo đúng quy định của pháp luật, bảo đảm quốc phòng, an ninh quốc gia, bí mật nhà nước.

2. Được thực hiện thường xuyên, liên tục từ khâu thiết kế, xây dựng, vận hành đến khi hủy bỏ; tuân thủ theo các tiêu chuẩn, quy chuẩn kỹ thuật được các cơ quan chức năng ban hành.

3. Nhận biết, phân loại, đánh giá kịp thời và xử lý có hiệu quả các rủi ro an toàn thông tin mạng có thể xảy ra trong đơn vị.

4. Xây dựng, triển khai quy chế an toàn thông tin mạng trên cơ sở hài hòa giữa lợi ích, chi phí và mức độ chấp nhận rủi ro của đơn vị.

5. Bố trí nhân sự chuyên trách chịu trách nhiệm bảo đảm an toàn thông tin mạng.

6. Xác định rõ quyền hạn, trách nhiệm của Thủ trưởng đơn vị (hoặc người đại diện hợp pháp), từng bộ phận và cá nhân trong đơn vị đối với công tác bảo đảm an toàn thông tin mạng.

Điều 4. Quy chế bảo đảm an toàn thông tin mạng

1. Các đơn vị phải xây dựng và ban hành quy chế bảo đảm an toàn thông tin mạng phù hợp với hệ thống thông tin, cơ cấu tổ chức, yêu cầu quản lý và hoạt động của đơn vị.

2. Quy chế bảo đảm an toàn thông tin mạng cần quy định tối thiểu các nội dung cơ bản sau:

a) Quản lý tài sản công nghệ thông tin;

b) Quản lý nguồn nhân lực;

c) Quản lý truy cập;

d) Bảo đảm an toàn, an ninh về mặt vật lý và môi trường;

đ) Quản lý vận hành và trao đổi thông tin;

e) Quản lý tiếp nhận, phát triển, duy trì hệ thống thông tin;

g) Quản lý sản phẩm, dịch vụ của bên thứ ba;

h) Quản lý sự cố an toàn thông tin;

i) Bảo đảm hoạt động liên tục của hệ thống thông tin;

k) Kiểm soát tuân thủ và chế độ báo cáo.

3. Đơn vị phải rà soát, chỉnh sửa, hoàn thiện các quy chế bảo đảm an toàn thông tin, đảm bảo sự đầy đủ theo các quy định tại Quy chế này và phù hợp với các văn bản quy phạm pháp luật liên quan trong lĩnh vực an toàn, an ninh thông tin. Khi phát hiện những bất cập, bất hợp lý gây ra mất an toàn hệ thống thông tin hoặc theo yêu cầu của cơ quan có thẩm quyền, đơn vị phải tiến hành chỉnh sửa, bổ sung ngay quy chế an toàn thông tin mạng đã ban hành.

Chương II

CÁC QUY ĐỊNH VỀ BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Mục 1

QUẢN LÝ TÀI SẢN CÔNG NGHỆ THÔNG TIN

Điều 5. Quản lý tài sản công nghệ thông tin

1. Các loại tài sản công nghệ thông tin bao gồm:

a) Tài sản vật lý: các thiết bị công nghệ thông tin, phương tiện truyền thông và các thiết bị phục vụ cho hoạt động của hệ thống thông tin;

b) Tài sản thông tin: các thông tin, dữ liệu ở dạng số;

c) Tài sản phần mềm: các phần mềm hệ thống, phần mềm tiện ích, cơ sở dữ liệu, chương trình ứng dụng và công cụ phát triển.

2. Căn cứ phân loại tài sản công nghệ thông tin tại Khoản 1 Điều này, đơn vị xây dựng và thực hiện các quy định về quản lý và sử dụng tài sản theo quy định tại Điều 6 Quy chế này.

Điều 6. Yêu cầu cơ bản về quản lý tài sản công nghệ thông tin

1. Lập danh mục tài sản công nghệ thông tin. Thường xuyên cập nhật và quản lý danh mục

2. Giao, gắn trách nhiệm cho cá nhân hoặc tập thể quản lý, sử dụng tài sản.

3. Quy định các quy tắc sử dụng, gìn giữ, bảo vệ tài sản trong các trường hợp như: mang tài sản ra khỏi cơ quan, tài sản liên quan tới dữ liệu nhạy cảm, cài đặt và cấu hình,...

4. Tài sản vật lý có lưu trữ dữ liệu nhạy cảm khi thay đổi mục đích sử dụng hoặc thanh lý, đơn vị 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 biện pháp tiêu hủy cấu phần lưu trữ dữ liệu trên tài sản đó.

Mục 2
QUẢN LÝ NGUỒN NHÂN LỰC

Điều 7. Phân công nhiệm vụ

1. Xác định trách nhiệm trong việc bảo đảm an toàn thông tin mạng của vị trí phân công.

2. Đảm bảo người được phân công làm việc tại các vị trí có tiếp xúc với thông tin, dữ liệu nhạy cảm phải qua bước đánh giá, thẩm tra nhân thân và lý lịch tư pháp.

3. Yêu cầu người được phân công phải cam kết bảo mật thông tin bằng văn bản riêng hoặc cam kết trong hợp đồng làm việc, hợp đồng lao động, bao gồm các điều khoản về trách nhiệm của cá nhân sau khi thôi việc tại đơn vị.

Điều 8. Sử dụng nguồn nhân lực

Đơn vị có trách nhiệm thực hiện:

1. Phổ biến và cập nhật các quy định về bảo đảm an toàn thông tin mạng cho tất cả cán bộ, nhân viên.

2. Có biện pháp quản lý tài khoản người dùng của cán bộ, nhân viên trên các hệ thống thông tin quan trọng.

3. Thường xuyên rà soát, kiểm tra quyền truy cập vào các hệ thống thông tin đối với tất cả cán bộ, nhân viên đảm bảo quyền truy cập phù hợp với nhiệm vụ được giao.

Điều 9. Chấm dứt hoặc thay đổi công việc

Khi cán bộ, nhân viên chấm dứt hoặc thay đổi công việc, đơn vị phải:

1. Xác định rõ trách nhiệm của cán bộ, nhân viên và các bên liên quan trong quản lý, sử dụng các tài sản công nghệ thông tin được giao.

2. Lập biên bản bàn giao tài sản công nghệ thông tin.

3. Thay đổi hoặc thu hồi quyền truy cập các hệ thống thông tin.

4. Rà soát, kiểm tra đối chiếu định kỳ giữa bộ phận quản lý nhân sự và bộ phận quản lý cấp phát, thu hồi quyền truy cập hệ thống thông tin để đảm bảo tài khoản người dùng của cán bộ, nhân viên đã nghỉ việc được thu hồi.

Mục 3
ĐẢM BẢO AN TOÀN VỀ MẶT VẬT LÝ VÀ MÔI TRƯỜNG NƠI LẮP ĐẶT TRANG THIẾT BỊ CÔNG NGHỆ THÔNG TIN

Điều 10. Yêu cầu chung đối với nơi lắp đặt

1. Có biện pháp bảo vệ, kiểm soát, hạn chế rủi ro xâm nhập trái phép, phòng chống nguy cơ do cháy nổ, thiên tai, thảm họa.

2. Các khu vực có yêu cầu cao về an toàn như khu vực lắp đặt máy chủ, thiết bị lưu trữ, thiết bị an ninh bảo mật, thiết bị truyền thông phải được cách ly với khu vực dùng chung; ban hành nội quy, hướng dẫn làm việc và áp dụng biện pháp kiểm soát ra vào khu vực đó.

Điều 11. Yêu cầu đối với Phòng máy chủ, Trung tâm dữ liệu

Ngoài việc đảm bảo yêu cầu tại Điều 10 Quy chế này, Phòng máy chủ, Trung tâm dữ liệu phải đảm bảo các yêu cầu sau:

1. Khu vực lắp đặt thiết bị phải được tránh nắng chiếu rọi trực tiếp, chống thấm dột nước, tránh ngập lụt. Cửa vào ra phải chắc chắn, có khả năng chống cháy, sử dụng khóa an toàn.

2. Khu vực lắp đặt thiết bị của hệ thống thông tin quan trọng phải được bảo vệ, giám sát 24/7.

3. Có tối thiểu một nguồn điện chính và một nguồn dự phòng có khả năng duy trì hoạt động của thiết bị trong thời gian tối thiểu 30 phút.

4. Có hệ thống điều hòa không khí đảm bảo khả năng hoạt động liên tục.

5. Có hệ thống chống sét trực tiếp và lan truyền.

6. Có hệ thống báo cháy và chữa cháy tự động đảm bảo khi chữa cháy không làm hư hỏng thiết bị lắp đặt bên trong.

7. Có hệ thống sàn kỹ thuật hoặc lớp cách ly chống nhiễm điện.

8. Có hệ thống camera giám sát, lưu trữ dữ liệu tối thiểu 90 ngày.

9. Có hệ thống theo dõi, kiểm soát nhiệt độ, độ ẩm.

10. Có sổ ghi nhật ký ra vào.

Mục 4
QUẢN LÝ VẬN HÀNH VÀ THÔNG TIN LIÊN LẠC

Điều 12. Trách nhiệm quản lý và quy trình vận hành của các đơn vị

1. Ban hành các quy trình vận hành hệ thống thông tin, tối thiểu bao gồm: Quy trình khởi động, đóng hệ thống; quy trình sao lưu, phục hồi dữ liệu; quy trình vận hành ứng dụng; quy trình xử lý sự cố; quy trình giám sát và ghi nhật ký hoạt động của hệ thống.

2. Kiểm soát sự thay đổi của phiên bản phần mềm, cấu hình phần cứng, quy trình vận hành: ghi chép lại các thay đổi; lập kế hoạch, thực hiện kiểm tra, thử nghiệm sự thay đổi, báo cáo kết quả và phải được phê duyệt trước khi áp dụng chính thức.

3. Hệ thống thông tin vận hành chính thức phải đáp ứng yêu cầu:

a) Tách biệt với môi trường phát triển và môi trường kiểm tra, thử nghiệm;

b) Có biện pháp, giải pháp bảo đảm an ninh, an toàn thông tin mạng;

c) Không cài đặt các công cụ, phương tiện phát triển ứng dụng trên hệ thống vận hành chính thức.

Điều 13. Sao lưu dự phòng

1. Lập danh sách các dữ liệu, phần mềm cần được sao lưu, có phân loại theo mức độ quan trọng, thời gian lưu trữ, thời gian sao lưu, phương pháp sao lưu và thời gian kiểm tra phục hồi hệ thống từ dữ liệu sao lưu.

2. Dữ liệu của các hệ thống thông tin quan trọng phải được sao lưu ra phương tiện lưu trữ ngoài (như băng từ, đĩa cứng, đĩa quang hoặc phương tiện lưu trữ khác) và cất giữ, bảo quản an toàn tách rời với khu vực tiến hành sao lưu. Kiểm tra, phục hồi dữ liệu sao lưu từ phương tiện lưu trữ ngoài tối thiểu sáu tháng một lần.

3. Cần tách biệt giữa sao lưu dữ liệu và sao lưu ứng dụng. Mọi ứng dụng được cài đặt hoặc xóa bỏ khỏi hệ thống thông tin đều cần được sao lưu vào hệ thống dự phòng, tách biệt khỏi hệ thống sao lưu dữ liệu.

Điều 14. Đảm bảo an toàn, bảo mật trong trao đổi thông tin

Đơn vị có trách nhiệm:

1. Ban hành quy định về trao đổi thông tin tối thiểu gồm: Phân loại thông tin theo mức độ nhạy cảm; quyền và trách nhiệm của cá nhân khi tiếp cận thông tin; biện pháp đảm bảo tính toàn vẹn, bảo mật khi truyền nhận, xử lý, lưu trữ thông tin; chế độ bảo quản thông tin.

2. Các thông tin, tài liệu, dữ liệu nhạy cảm phải được mã hóa trước khi trao đổi, truyền nhận qua mạng máy tính.

3. Thực hiện các biện pháp quản lý, giám sát và kiểm soát chặt chẽ các trang/cổng thông tin điện tử cung cấp thông tin, dịch vụ, giao dịch trực tuyến cho các tổ chức, cá nhân bên ngoài.

4. Thực hiện biện pháp bảo vệ trang thiết bị, phần mềm phục vụ trao đổi thông tin nội bộ nhằm hạn chế việc xâm nhập, khai thác bất hợp pháp các thông tin nhạy cảm.

Điều 15. Giám sát và ghi nhật ký hoạt động của hệ thống

1. Ghi và lưu trữ nhật ký về hoạt động của hệ thống và người sử dụng hệ thống thông tin.

2. Thực hiện các biện pháp giám sát, phân tích nhật ký, cảnh báo rủi ro, xử lý và báo cáo kết quả.

3. Bảo vệ các chức năng ghi nhật ký và thông tin nhật ký, chống giả mạo, sửa đổi, phá hủy và truy cập trái phép.

4. Thực hiện việc đồng bộ thời gian giữa các hệ thống thông tin.

Điều 16. Phòng chống mã độc

Xây dựng và thực hiện quy định về phòng chống mã độc đáp ứng các yêu cầu cơ bản sau:

1. Xác định trách nhiệm của người sử dụng và các bộ phận liên quan trong công tác phòng chống mã độc.

2. Triển khai biện pháp, giải pháp phòng chống mã độc cho toàn bộ hệ thống thông tin của đơn vị.

3. Cập nhật mẫu mã độc và phần mềm phòng chống mã độc mới.

4. Kiểm tra, diệt mã độc đối với vật mang tin nhận từ bên ngoài trước khi sử dụng.

5. Kiểm soát việc cài đặt phần mềm đảm bảo tuân thủ theo quy chế an toàn, an ninh của đơn vị.

Mục 5
CÁC BIỆN PHÁP QUẢN LÝ TRUY CẬP

Điều 17. Yêu cầu nghiệp vụ đối với kiểm soát truy cập

1. Quy định về quản lý truy cập đối với người sử dụng, nhóm người sử dụng, các thiết bị, công cụ sử dụng để truy cập đảm bảo đáp ứng yêu cầu nghiệp vụ và yêu cầu an toàn, an ninh, bao gồm các nội dung cơ bản sau:

a) Đăng ký, cấp phát, gia hạn và thu hồi quyền truy cập;

b) Giới hạn và kiểm soát các truy cập sử dụng tài khoản quản trị hệ thống;

c) Quản lý, cấp phát mã khóa bí mật về truy cập mạng, hệ điều hành, hệ thống thông tin và ứng dụng;

d) Rà soát, kiểm tra, xét duyệt lại quyền truy cập của người sử dụng;

đ) Yêu cầu, điều kiện an toàn, an ninh đối với các thiết bị, công cụ sử dụng để truy cập.

2. Quy định về quản lý mã khóa bí mật phải đáp ứng các yêu cầu sau:

a) Có quy định về độ phức tạp của mã khóa bí mật. Các yêu cầu về độ phức tạp của mã khóa bí mật hợp lệ phải được kiểm tra tự động khi thiết lập;

b) Các mã khóa bí mật mặc định của nhà sản xuất cài đặt sẵn trên các trang thiết bị, phần mềm, cơ sở dữ liệu phải được thay đổi trước khi đưa vào sử dụng.

3. Có quy định trách nhiệm bảo quản mã khóa bí mật của người sử dụng khi được cấp quyền truy cập.

Điều 18. Quy định về kiểm soát truy cập mạng

1. Đơn vị phải ban hành các quy định về quản lý kết nối, truy cập, trách nhiệm cá nhân của người sử dụng khi truy cập, sử dụng các hệ thống mạng, thông tin sau:

a) Mạng Internet;

b) Mạng nội bộ;

c) Hệ thống thông tin và các ứng dụng.

2. Đơn vị phải có biện pháp kiểm soát, bảo đảm người sử dụng tuân thủ các quy định đề ra.

Mục 6

TIẾP NHẬN, PHÁT TRIỂN, DUY TRÌ HỆ THỐNG THÔNG TIN

Điều 19. Yêu cầu về an toàn, an ninh cho hệ thống thông tin

Khi xây dựng mới hoặc nâng cấp, cải tiến hệ thống thông tin, đơn vị phải:

1. Xây dựng các yêu cầu về an toàn, an ninh đồng thời với việc đưa ra các yêu cầu kỹ thuật, nghiệp vụ.

2. Đánh giá, xác định cấp độ và tuân thủ đầy đủ các quy định về bảo đảm an toàn thông tin của hệ thống theo cấp độ tương ứng.

3. Xây dựng các yêu cầu về trách nhiệm cập nhật, vá lỗi, khắc phục lỗ hổng bảo mật... (hạn chế để lửng, nên liệt kê đầy đủ) của hệ thống thông tin, được phát hiện trong quá trình vận hành.

4. Xây dựng kế hoạch định kỳ, kiểm tra, rà soát về an toàn an ninh thông tin trong quá trình vận hành hệ thống.

Điều 20. Đảm bảo an toàn, an ninh các ứng dụng

Các chương trình ứng dụng nghiệp vụ phải đạt các yêu cầu tối thiểu sau:

1. Kiểm tra tính hợp lệ của dữ liệu đầu vào khi nhập liệu từ người dùng hoặc các hệ thống bên ngoài.

2. Kiểm tra tính hợp lệ của dữ liệu trao đổi giữa các thành phần của hệ thống.

3. Có các biện pháp đảm bảo tính xác thực và tính toàn vẹn dữ liệu.

4. Kiểm tra tính hợp lệ của dữ liệu xuất ra từ các ứng dụng.

5. Mã khóa bí mật của người sử dụng trong các hệ thống thông tin quan trọng phải được mã hóa ở lớp ứng dụng.

Điều 21. Quản lý mật mã

1. Quy định và đưa vào sử dụng các biện pháp mã hóa mật mã theo các chuẩn quốc gia hoặc quốc tế đã được công nhận, có biện pháp quản lý khóa để bảo vệ thông tin.

2. Dữ liệu về mã khóa bí mật người sử dụng và các dữ liệu nhạy cảm khác phải được mã hóa, bảo vệ khi truyền qua mạng và khi lưu trữ.

Điều 22. Quản lý sự thay đổi hệ thống thông tin

Ban hành quy trình, biện pháp quản lý và kiểm soát sự thay đổi hệ thống thông tin, tối thiểu bao gồm:

1. Có quy định để đảm bảo hệ thống hoạt động ổn định, an toàn khi thay đổi các phần mềm hệ thống như hệ điều hành, hệ quản trị cơ sở dữ liệu.

2. Kiểm soát chặt chẽ việc sửa đổi mã nguồn phần mềm.

3. Giám sát, quản lý chặt chẽ việc thuê mua phần mềm bên ngoài.

Mục 7
QUẢN LÝ SẢN PHẨM, DỊCH VỤ CỦA BÊN THỨ BA

Điều 23. Ký kết hợp đồng với bên thứ ba

Đơn vị phải thực hiện:

1. Xác định rõ trách nhiệm, quyền hạn và nghĩa vụ của các bên về an toàn, an ninh công nghệ thông tin khi ký hợp đồng. Hợp đồng với bên thứ ba phải bao gồm các điều khoản về việc xử lý vi phạm và trách nhiệm bồi thường thiệt hại của bên thứ ba do vi phạm của bên thứ ba gây ra.

2. Đơn vị không được thuê bên thứ ba thực hiện toàn bộ công việc quản trị (chỉnh sửa cấu hình, dữ liệu, nhật ký) đối với các hệ thống thông tin quan trọng.

Điều 24. Trách nhiệm của đơn vị trong quản lý các dịch vụ do bên thứ ba cung cấp

1. Cung cấp, thông báo và yêu cầu bên thứ ba thực hiện các quy định của đơn vị về an toàn bảo mật hệ thống thông tin.

2. Đảm bảo triển khai, duy trì các biện pháp an toàn, an ninh của dịch vụ do bên thứ ba cung cấp theo đúng thỏa thuận.

3. Xác định và ghi rõ các tính năng an toàn, các mức độ bảo mật của dịch vụ và yêu cầu quản lý trong các thỏa thuận về dịch vụ do bên thứ ba cung cấp.

4. Áp dụng các biện pháp giám sát chặt chẽ và giới hạn quyền truy cập của bên thứ ba khi cho phép họ truy cập vào hệ thống thông tin của đơn vị.

5. Giám sát nhân sự của bên thứ ba trong quá trình thực hiện hợp đồng. Khi phát hiện nhân sự bên thứ ba vi phạm quy định về an toàn bảo mật phải thông báo và phối hợp với bên thứ ba áp dụng biện pháp xử lý kịp thời.

6. Thu hồi quyền truy cập hệ thống thông tin đã được cấp cho bên thứ ba, thay đổi các khóa, mã khóa bí mật nhận bàn giao từ bên thứ ba ngay sau khi hoàn thành công việc hoặc kết thúc hợp đồng.

Điều 25. Trách nhiệm của bên thứ ba khi cung cấp dịch vụ công nghệ thông tin

1. Ký và thực hiện cam kết bảo mật thông tin cả trong quá trình triển khai và sau khi hoàn tất hợp đồng.

2. Lập kế hoạch, bố trí nhân sự và các nguồn lực khác để thực hiện hợp đồng. Thông báo danh sách nhân sự triển khai cho bên ký kết hợp đồng và phải được đơn vị chấp thuận. Nhân sự bên thứ ba phải ký cam kết không tiết lộ thông tin quan trọng của bên ký kết hợp đồng.

3. Bàn giao tài sản, quyền truy cập hệ thống thông tin do bên ký kết hợp đồng cung cấp khi hoàn thành công việc hoặc kết thúc hợp đồng.

Mục 8

QUẢN LÝ SỰ CỐ AN TOÀN THÔNG TIN MẠNG

Điều 26. Quy trình xử lý sự cố

1. Tiếp nhận thông tin sự cố.

2. Xác thực sự cố.

3. Thông tin cho Lãnh đạo về sự cố.

4. Cô lập hệ thống (bật hệ thống dự phòng nếu có).

5. Thu thập thông tin về sự cố.

6. Phân tích thông tin về sự cố.

7. Xử lý sự cố (yêu cầu hỗ trợ nếu cần).

8. Phục hồi hệ thống (tắt hệ thống dự phòng).

9. Tổng kết đánh giá kết quả.

10. Báo cáo Lãnh đạo và các đơn vị liên quan.

Điều 27. Nguyên tắc kiểm soát và khắc phục sự cố

1. Các sự cố mất an toàn thông tin mạng phải được lập tức báo cáo đến những người có thẩm quyền và những người có liên quan.

2. Xác định nguyên nhân và thực hiện các biện pháp phòng ngừa.

3. Quá trình xử lý sự cố phải được ghi chép và lưu trữ. Thực hiện biện pháp bảo vệ, chống chỉnh sửa, hủy hoại đối với tài liệu lưu trữ về sự cố.

4. Thu thập, ghi chép, bảo toàn bằng chứng, chứng cứ phục vụ cho việc kiểm tra, xử lý, khắc phục và phòng ngừa sự cố.

Mục 9

ĐẢM BẢO HOẠT ĐỘNG LIÊN TỤC CỦA CÁC HỆ THỐNG THÔNG TIN

Điều 28. Xây dựng hệ thống dự phòng

1. Đơn vị phải xây dựng hệ thống dự phòng cho các hệ thống thông tin quan trọng.

2. Từng hệ thống dự phòng phải đảm bảo khả năng thay thế hệ thống chính trong thời gian tối đa bốn giờ đồng hồ tính từ thời điểm hệ thống chính có sự cố không khắc phục được.

Điều 29. Xây dựng quy trình đảm bảo hoạt động liên tục

1. Xây dựng quy trình xử lý các tình huống gián đoạn hoạt động của từng cấu phần trong hệ thống thông tin như máy chủ, thiết bị mạng,...

2. Quy trình xử lý phải được kiểm tra và cập nhật khi có sự thay đổi của hệ thống thông tin, cơ cấu tổ chức, nhân sự và phân công trách nhiệm của các bộ phận có liên quan trong đơn vị.

3. Hệ thống dự phòng cần được định kỳ kiểm tra để luôn đảm bảo tính sẵn sàng khi xảy ra các sự cố an toàn thông tin

Mục 10

CHẾ ĐỘ BÁO CÁO

Điều 30. Chế độ báo cáo

Đơn vị trực thuộc Bộ Giao thông vận tải có trách nhiệm gửi báo cáo về Bộ Giao thông vận tải (qua Trung tâm Công nghệ thông tin) như sau:

1. Báo cáo năm

a) Nội dung báo cáo:

- Việc thực hiện bảo đảm an toàn, an ninh thông tin theo quy định tại Quy chế này;

- Các nội dung chỉnh sửa, bổ sung quy chế an toàn, an ninh thông tin của đơn vị (nếu có).

b) Thời hạn gửi báo cáo: trước ngày 31 tháng 01 của năm tiếp theo.

2. Báo cáo đột xuất

a) Các sự cố mất an toàn thông tin mạng:

- Thời hạn gửi báo cáo: trong thời gian 03 (ba) ngày kể từ thời điểm vụ, việc được phát hiện;

- Nội dung vụ, việc;

- Thời gian, địa điểm phát sinh vụ, việc;

- Nguyên nhân xảy ra vụ, việc (nếu có);

- Đánh giá rủi ro, ảnh hưởng đối với hệ thống thông tin và nghiệp vụ tại nơi xảy ra vụ, việc và những địa điểm khác có liên quan;

- Các biện pháp đơn vị đã tiến hành để ngăn chặn, khắc phục và phòng ngừa rủi ro;

- Kiến nghị, đề xuất.

b) Các trường hợp đột xuất khác theo yêu cầu của Bộ Giao thông vận tải.

Chương III
ĐIỀU KHOẢN THI HÀNH

Điều 31. Trách nhiệm thi hành

1. Trung tâm Công nghệ thông tin có trách nhiệm:

a) Theo dõi, tổng hợp báo cáo Bộ trưởng tình hình thực hiện công tác bảo đảm an toàn, an ninh thông tin của các đơn vị theo quy định tại Quy chế này;

b) Hàng năm lập kế hoạch và kiểm tra việc thực hiện Quy chế này tại các đơn vị;

c) Chủ trì, phối hợp với các đơn vị liên quan thuộc Bộ Giao thông vận tải xử lý các vướng mắc phát sinh trong quá trình triển khai thực hiện Quy chế này.

2. Thủ trưởng các đơn vị liên quan thuộc Bộ Giao thông vận tải có trách nhiệm tổ chức thực hiện Quy chế này.

3. Trong quá trình thực hiện nếu có vấn đề phát sinh, vướng mắc, các đơn vị phản ánh kịp thời về Bộ Giao thông vận tải (qua Trung tâm Công nghệ thông tin) để xem xét, bổ sung, sửa đổi./.