| BỘ GIAO THÔNG VẬN TẢI | CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM<br>Độc lập - Tự do - Hạnh phúc |
|---|---|
| Số: 724 /QĐ-BGTVT | *Hà Nội, ngày 13 tháng 06 năm 2024* |

# QUYẾT ĐỊNH

**Ban hành Quy chế bảo đảm an toàn thông tin, an ninh mạng 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 An ninh mạng số 24/2018/QH14 ngày 12/6/2018;*

*Căn cứ Nghị định số 56/2022/NĐ-CP ngày 24/8/2022 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 Nghị định số 53/2016/NĐ-CP ngày 15/8/2022 của Chính phủ quy định chi tiết một số điều của Luật An ninh mạng;*

*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 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 về bảo đảm an toàn hệ thống thông tin theo cấp độ;*

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

## QUYẾT ĐỊNH:

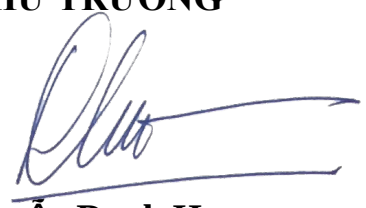
**Điều 1.** Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn thông tin, an ninh mạng Bộ Giao thông vận tải.

**Điều 2.** Quyết định này có hiệu lực từ ngày ký ban hành và thay thế Quyết định số 2018/QĐ-BGTVT ngày 17/7/2017 của Bộ trưởng Bộ Giao thông vận tải ban hành Quy chế bảo đảm an toàn, an ninh thông tin mạng Bộ Giao thông vận tải.

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

***Nơi nhận:***
- Như Điều 3;
- Bộ trưởng (để báo cáo);
- Bộ Công an;
- Bộ Thông tin và Truyền thông;
- Các đồng chí Thứ trưởng;
- Cổng TTĐT Bộ GTVT;
- Lưu: VT, TTCNTT.

**KT. BỘ TRƯỞNG**
**THỨ TRƯỞNG**



**Nguyễn Danh Huy**

| BỘ GIAO THÔNG VẬN TẢI | CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM |
|---|---|
| | **Độc lập - Tự do - Hạnh phúc** |

# QUY CHẾ
# BẢO ĐẢM AN TOÀN THÔNG TIN, AN NINH MẠNG BỘ GIAO THÔNG VẬN TẢI

*(Kèm theo Quyết định số 724 /QĐ-BGTVT ngày 13 tháng 06 năm 2024 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. Phạm vi điều chỉnh:

Quy chế này quy định về bảo đảm an toàn thông tin, an ninh mạng trong các hoạt động ứng dụng công nghệ thông tin của Bộ Giao thông vận tải.

2. Đối tượng áp dụng:

a) Các cơ quan, đơn vị, doanh nghiệp thuộc Bộ Giao thông vận tải.

b) Cán bộ, công chức, viên chức và người lạo động trong các cơ quan, đơn vị, doanh nghiệp thuộc Bộ Giao thông vận tải.

c) Các tổ chức, cá nhân cung cấp dịch vụ công nghệ thông tin và an toàn thông tin, an ninh mạng; tham gia kết nối vào các hệ thống thông tin của 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 toàn thông tin là sự bảo vệ thông tin số và các 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. An ninh 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.

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 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. Nguyên tắc bảo đảm an toàn thông tin, an ninh mạng**

1. Bảo đảm an toàn thông tin, an ninh mạng là yêu cầu bắt buộc, tuân thủ các nguyên tắc chung quy định tại Điều 4 Luật An toàn thông tin mạng, Điều 4 Luật An ninh mạng và các quy định pháp luật khác có liên quan.

2. Từng đơn vị phải có trách nhiệm bảo đảm an toàn thông tin, an ninh mạng của đơn vị mình, theo đúng quy định của pháp luật, bảo đảm quốc phòng, an ninh quốc gia, bí mật nhà nước.

3. 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, an ninh mạng.

4. An toàn thông tin, an ninh mạng 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.

5. Việc bảo đảm an toàn thông tin, an ninh mạng được thực hiện trên cơ sở hài hòa giữa lợi ích, chi phí và mức độ chấp nhận rủi ro của đơn vị.

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

7. Xử lý sự cố an toàn thông tin, an ninh mạng phải phù hợp với trách nhiệm, quyền hạn và bảo đảm lợi ích hợp pháp của cơ quan, đơn vị, cá nhân liên quan và theo quy định của pháp luật.

**Điều 4. Các hành vi bị nghiêm cấm**

1. Các hành vi bị nghiêm cấm về an toàn thông tin quy định tại Điều 7 Luật An toàn thông tin mạng.

2. Các hành vi bị nghiêm cấm về an ninh mạng quy định tại Điều 8 Luật An ninh mạng.

3. Hành vi nghiêm cấp khác về an toàn thông tin, an ninh mạng theo quy định của pháp luật.

**Điều 5. Quy chế bảo đảm an toàn thông tin, an ninh mạng**

1. Các đơn vị thuộc Bộ phải xây dựng và ban hành quy chế bảo đảm an toàn thông tin, an ninh 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, an ninh 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 bảo đảm an toàn thông tin, an ninh mạng;

c) Các biện pháp quản lý truy cập mạng.

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

đ) Bảo đảm toàn thông tin, an ninh mạng đối với thiết bị đầu cuối.

e) Quản lý vận hành và trao đổi thông tin.

g) Bảo đảm an toàn thông tin, an ninh mạng trong xây dựng, duy trì, hủy bỏ hệ thống thông tin.

h) Quản lý sản phẩm, dịch vụ của bên thứ ba.

i) Quản lý sự cố an toàn thông tin, an ninh mạng.

k) Kiểm tra, giám sát an toàn thông tin, an ninh mạng.

l) Bảo đảm hoạt động liên tục của hệ thống thông tin.

m) Chế độ báo cáo.

3. Quy chế bảo đảm an toàn thông tin, an ninh mạng của đơn vị phải 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 thông tin, an ninh mạng. 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 quy chế đã ban hành.

## Chương II

## CÁC QUY ĐỊNH VỀ BẢO ĐẢM AN TOÀN THÔNG TIN, AN NINH MẠNG

### Mục 1

### QUẢN LÝ TÀI SẢN CÔNG NGHỆ THÔNG TIN

**Điều 6. 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 7 Quy chế này.

**Điều 7. 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 BẢO ĐẢM AN TOÀN THÔNG TIN, AN NINH MẠNG

### Điều 8. Điều kiện, yêu cầu nhân sự

1. Có phẩm chất đạo đức tốt, có đủ tiêu chuẩn chính trị, có kiến thức pháp luật và chuyên môn, nghiệp vụ về bảo vệ thông tin bí mật, nghiêm chỉnh chấp hành đường lối, chủ trương, chính sách của Đảng, pháp luật của Nhà nước.

2. Có trình độ, chuyên môn về lĩnh vực công nghệ thông tin, an toàn thông tin, an ninh mạng phù hợp với vị trí tuyển dụng.

### Điều 9. Phân công nhiệm vụ

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

2. 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 10. 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, an ninh 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 11. 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

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

### Điều 12. 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 13. Yêu cầu đối với phòng máy chủ, trung tâm dữ liệu

Ngoài việc đảm bảo yêu cầu tại Điều 12 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

## ĐẢM BẢO AN TOÀN THÔNG TIN, AN NINH MẠNG ĐỐI VỚI THIẾT BỊ ĐẦU CUỐI

### Điều 14. Quản lý an toàn thiết bị đầu cuối

Quy định về quản lý an toàn thiết bị đầu cuối bao gồm các nội dung:

1. Quản lý, vận hành hoạt động bình thường cho thiết bị đầu cuối.

2. Kết nối, truy cập và sử dụng thiết bị đầu cuối từ xa.

3. Cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống.

4. Cấu hình tối ưu và tăng cường bảo mật cho máy tính người sử dụng và thực hiện quy trình trước khi đưa hệ thống vào sử dụng.

5. Kiểm tra, đánh giá, xử lý điểm yếu an toàn thông tin cho thiết bị đầu cuối trước khi đưa vào sử dụng.

**Điều 15. 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. Quản lý truy cập, sử dụng tài nguyên nội bộ.

2. Quản lý truy cập mạng và tài nguyên trên Internet.

3. Cài đặt và sử dụng máy tính an toàn.

**Điều 16. Quản lý phòng chống phần mềm độc hại**

1. Cài đặt, cập nhật, sử dụng phần mềm phòng chống mã độc; dò quét, kiểm tra phần mềm độc hại trên máy tính, máy chủ và thiết bị di động.

2. Định kỳ hằng năm thực hiện kiểm tra và dò quét phần mềm độc hại trên các thiết bị đầu cuối; thực hiện kiểm tra và xử lý phần mềm độc hại khi phát hiện dấu hiệu hoặc cảnh báo về dấu hiệu phần mềm độc hại xuất hiện trên thiết bị đầu cuối.

**Điều 17: Trách nhiệm của cá nhân**

1. Gắn trách nhiệm cho cá nhân quản lý, sử dụng thiết bị đầu cuối.

2. Quy định các quy tắc sử dụng, giữ gìn bảo vệ thiết bị đầu cuối:

a) Cá nhân chỉ cài đặt phần mềm hợp lệ trên máy tính và thường xuyên cập nhật phần mềm và hệ điều hành.

b) Cài đặt phần mềm phòng chống mã độc và thiết lập chế độ tự động cập nhật cho phần mềm; khi phát hiện bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại trên máy tính phải báo trực tiếp cho bộ phận chuyên trách về công nghệ thông tin để được xử lý kịp thời.

c) Chỉ truy nhập vào các trang/cổng thông tin điện tử, ứng dụng trực tuyến tin cậy phù hợp với chức năng, trách nhiệm, quyền hạn của mình; có trách nhiệm bảo mật tài khoản truy nhập thông tin, không chia sẻ mật khẩu, thông tin cá nhân với người khác.

d) Chỉ sử dụng thiết bị lưu trữ di động cho các hoạt động nghiệp vụ, quản lý khi và thực hiện các biện pháp bảo đảm an toàn thông tin, an ninh mạng cho thiết bị lưu trữ di động như mã hóa dữ liệu, quét mã độc định kỳ.

đ) Khóa màn hình máy tính khi rời khỏi bàn làm việc; đăng xuất khỏi hệ thống, ứng dụng khi ngừng sử dụng; tắt máy an toàn sau mỗi buổi làm việc.

**Điều 18: Trách nhiệm của đơn vị**

a) Các đơn vị có trách nhiệm xây dựng quy trình bảo dưỡng, bảo trì và hướng dẫn người dùng cách sử dụng, quản lý, vận hành hệ thiết bị đầu cuối.

b) Chỉ định bộ phận chuyên trách về công nghệ thông tin thực hiện định kỳ kiểm tra công tác bảo đảm an toàn thông tin, an ninh mạng đối với thiết bị đầu cuối.

## Mục 5
## QUẢN LÝ, VẬN HÀNH HỆ THỐNG THÔNG TIN

### Điều 19. Trách nhiệm quản lý và quy trình vận hành của 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 toàn thông tin, an ninh mạng.

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

### Điều 20. 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 21. Trao đổi thông tin, dữ liệu

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, 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 22. 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 23. 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, xử lý 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 thông tin, an ninh mạng của đơn vị.

## Mục 6
## CÁC BIỆN PHÁP QUẢN LÝ TRUY CẬP MẠNG

**Điều 24. 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 thông tin, an ninh mạng, 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 25. 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, hệ thống 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.

3. Quản lý truy cập và cấu hình hệ thống

a) Cán bộ quản lý, vận hành truy cập, khai thác thông tin tại hệ thống theo trách nhiệm và phân quyền được quy định; việc khai thác thông tin phải bảo đảm nguyên tắc bảo mật, không được tự ý cung cấp thông tin ra bên ngoài.

b) Cán bộ quản lý, vận hành có trách nhiệm theo dõi và phát hiện các trường hợp truy cập hệ thống trái phép hoặc thao tác vượt quá giới hạn, báo cáo cho cán bộ quản lý để tiến hành ngăn chặn, thu hồi, khóa quyền truy cập của các tài khoản vi phạm.

c) Quy trình kết nối thiết bị đầu cuối của người sử dụng vào hệ thống mạng; truy cập và quản lý cấu hình hệ thống; cấu hình tối ưu, tăng cường bảo mật cho các thiết bị mạng, bảo mật trong hệ thống cần được thực hiện trước khi đưa hệ thống vào vận hành, khai thác.

## Mục 7

## BẢO ĐẢM AN TOÀN THÔNG TIN, AN NINH MẠNG TRONG XÂY DỰNG, DUY TRÌ, HỦY BỎ HỆ THỐNG THÔNG TIN

**Điều 26. Thiết kế an toàn hệ thống thông tin**

1. Trong quá trình xây dựng hoặc nâng cấp hệ thống, phải có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin; thiết kế và các thành phần của hệ thống thông tin; phương án bảo đảm an toàn thông tin theo cấp độ; phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin, an ninh mạng.

2. Khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống; có phương án quản lý và bảo vệ hồ sơ thiết kế.

3. Đánh giá hồ sơ thiết kế hệ thống thông tin, các biện pháp bảo đảm an toàn thông tin trước khi triển khai thực hiện.

**Điều 27. Yêu cầu về an toàn thông tin, an ninh mạng cho hệ thống**

1. Xây dựng các yêu cầu về an toàn thông tin, an ninh mạng 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, an ninh mạng 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 của hệ thống thông tin được phát hiện trong quá trình vận hành.

**Điều 28. Quản lý an toàn thông tin, an ninh mạng máy chủ**

1. Quản lý, vận hành hoạt động của hệ thống máy chủ

a) Bảo đảm cho hệ điều hành, phần mềm cài đặt trên máy chủ hoạt động liên tục, ổn định và an toàn.

b) Thường xuyên kiểm tra cấu hình, các file nhật ký hoạt động của hệ điều hành, phần mềm nhằm kịp thời phát hiện và xử lý những sự cố nếu có.

c) Quản lý các thay đổi cấu hình kỹ thuật; thường xuyên cập nhật các bản vá lỗi và loại bỏ các thành phần của hệ điều hành, phần mềm không cần thiết hoặc không còn nhu cầu sử dụng.

2. Truy cập mạng của máy chủ

Bảo đảm các kết nối mạng trên máy chủ hoạt động liên tục, ổn định và an toàn. Cấu hình, kiểm soát các kết nối, các cổng dịch vụ từ bên trong đi ra cũng nhưng bên ngoài vào hệ thống.

3. Quản trị máy chủ

a) Thay đổi các tài khoản, mật khẩu mặc định ngay khi đưa hệ điều hành, phần mềm vào sử dụng.

b) Cấp quyền quản lý truy cập của người sử dụng trên máy chủ cài đặt hệ điều hành.

c) Toàn bộ máy chủ, ngoại trừ các hệ thống bắt buộc phải có giao tiếp với Internet (các hệ thống phục vụ truy cập Internet; cung cấp giao diện ra Internet của trang tin thông tin điện tử; phục vụ cập nhật bản vá hệ điều hành, mẫu mã độc, mẫu điểm yếu, mẫu tấn công) không được kết nối Internet.

d) Sử dụng cơ chế xác thực đa nhân tố khi truy cập vào các máy chủ trong hệ thống; có cơ chế yêu cầu người sử dụng thay đổi thông tin xác thực định kỳ.

đ) Kiểm tra tính toàn vẹn của các tệp tin hệ thống và tính toàn vẹn của các quyền đã được cấp trên các tài khoản hệ thống.

e) Cấu hình tối ưu và tăng cường bảo mật cho hệ thống máy chủ trước khi đưa vào vận hành, khai thác.

**Điều 29. Quản lý an toàn thông tin, an ninh mạng ứng dụng**

Các chương trình ứng dụng nghiệp vụ phải đạt các yêu cầu tối thiểu về an toàn thông tin, an ninh mạng sau:

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

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

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

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

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

2. Quản trị ứng dụng

a) Có cơ chế yêu cầu người sử dụng thay đổi thông tin xác thực định kỳ đối với tài khoản quản trị của ứng dụng.

b) Sử dụng cơ chế mã hóa thông tin xác thực của người sử dụng/bên sử dụng trước khi gửi đến ứng dụng qua môi trường mạng.

c) Xác thực thông tin, nguồn gửi khi trao đổi thông tin trong quá trình quản trị ứng dụng (không phải là thông tin, dữ liệu công khai) qua môi trường mạng.

**Điều 30. Quản lý an toàn dữ liệu**

1. Yêu cầu an toàn đối với phương pháp mã hóa:

a) Đơn vị phải xây dựng và áp dụng quy định sử dụng các phương thức mã hóa thích hợp theo các chuẩn quốc gia hoặc quốc tế đã được công nhận để bảo vệ thông tin.

b) Phải có biện pháp quản lý khóa mã hóa thích hợp để hỗ trợ việc sử dụng các kỹ thuật mã hóa.

2. Phân loại, quản lý và sử dụng khóa bí mật và dữ liệu mã hóa.

3. Có cơ chế mã hóa và kiểm tra tính nguyên vẹn của dữ liệu.

4. Trao đổi dữ liệu qua môi trường mạng và phương tiện lưu trữ.

5. Sao lưu dự phòng và khôi phục dữ liệu (tần suất sao lưu dự phòng, phương tiện lưu trữ, thời gian lưu trữ; nơi lưu trữ, phương thức lưu trữ và phương thức lấy dữ liệu ra khỏi phương tiện lưu trữ).

6. Cập nhật đồng bộ thông tin, dữ liệu giữa hệ thống sao lưu dự phòng chính và hệ thống phụ.

7. 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 (nếu có).

**Điều 31. 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 32. 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.

**Điều 33. Quản lý rủi ro an toàn thông tin, an ninh mạng**

Quản lý rủi ro an toàn thông tin, an ninh mạng bao gồm:

1. Xác định mức rủi ro.

2. Quy trình đánh giá và quản lý rủi ro.

3. Biện pháp kiểm soát rủi ro.

**Điều 34. Thử nghiệm và nghiệm thu hệ thống**

1. Thực hiện thử nghiệm và nghiệm thu hệ thống trước khi bàn giao và đưa vào sử dụng.

2. Có nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống.

3. Có bộ phận có trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống.

4. Có đơn vị độc lập (bên thứ ba) hoặc bộ phận độc lập thuộc đơn vị thực hiện tư vấn và giám sát quá trình thử nghiệm và nghiệm thu hệ thống.

5. Có báo cáo nghiệm thu được xác nhận của bộ phận chuyên trách và phê duyệt của chủ quản hệ thống thông tin trước khi đưa vào sử dụng.

**Điều 35. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ**

1. Quy định về bảo đảm an toàn thông tin, an ninh mạng khi kết thúc vận hành, khai thác, thanh lý, hủy bỏ.

2. Quy trình xử lý thông tin trên hệ thống khi thay đổi mục đích sử dụng hoặc gỡ bỏ.

3. Phương án kỹ thuật thực hiện xử lý thông tin trên hệ thống khi thay đổi mục đích sử dụng hoặc gỡ bỏ.

## Mục 8
## QUẢN LÝ SẢN PHẨM, DỊCH VỤ CỦA BÊN THỨ BA

**Điều 36. 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 thông tin, an ninh mạng 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 37. Trách nhiệm của đơn vị trong quản lý các sản phẩm, 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 thông tin, an ninh mạng 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 38. Trách nhiệm của bên thứ ba khi cung cấp sản phẩm, 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.

4. Đối với sản phẩm phần mềm: cung cấp mã nguồn phần mềm, thực hiện kiểm tra đánh giá an toàn thông tin, an ninh mạng, kiểm thử phần mềm trên môi trường thử nghiệm trước khi đưa vào sử dụng.

## Mục 9
## QUẢN LÝ SỰ CỐ AN TOÀN THÔNG TIN, AN NINH MẠNG

### Điều 39. Nguyên tắc kiểm soát và khắc phục sự cố

1. Các sự cố mất an toàn thông tin, an ninh 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.

### Điều 40. Quản lý sự cố

1. Phân nhóm sự cố an toàn thông tin mạng theo quy định tại Quyết định số 05/2017/QĐ-TTg của Thủ tướng Chính phủ ngày 16/3/2017 quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia; xây dựng phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin, an ninh mạng, ứng phó sự cố an toàn thông tin, an ninh mạng.

2. Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin, an ninh mạng.

3. Kế hoạch ứng phó sự cố an toàn thông tin, an ninh mạng.

4. Giám sát, phát hiện và cảnh báo sự cố an toàn thông tin, an ninh mạng.

5. Quy trình ứng cứu sự cố an toàn thông tin, an ninh mạng thông thường.

6. Quy trình ứng cứu sự cố an toàn thông tin, an ninh mạng nghiêm trọng.

7. Cơ chế phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an toàn thông tin, an ninh mạng.

8. Định kỳ tổ chức diễn tập phương án xử lý sự cố an toàn thông tin, an ninh mạng.

### Điều 41. Quy trình xử lý sự cố

Thực hiện theo quy định tại Điều 13, Điều 14 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; Điều 11 Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc và Quyết định số 991/QĐ-BGTVT ngày 22/5/2019 của Bộ trưởng Bộ Giao thông vận tải ban hành Quy trình điều phối, ứng cứu sự cố an toàn thông tin mạng Bộ Giao thông vận tải, cụ thể như sau:

1. Đối với sự cố thông thường:

Bước 1. Phát hiện, tiếp nhận thông tin sự cố.

Bước 2. Xác minh sự cố.

Bước 3. Phân tích, phân loại sự cố.

Bước 4. Xử lý sự cố.

Bước 5. Kết quả sử lý sự cố.

Bước 6. Tổng kết đánh giá kết quả.

Bước 7. Báo cáo kết quả ứng cứu sự cố và lưu hồ sơ.

2. Đối với sự cố nghiêm trọng:

Bước 1. Phát hiện, tiếp nhận thông tin sự cố.

Bước 2. Xác minh sự cố.

Bước 3. Phân tích, phân loại sự cố.

Bước 4. Báo cáo sự cố.

Bước 5. Lựa chọn phương án điều phối ứng cứu sự cố.

Bước 6. Điều phối ứng cứu sự cố.

Bước 7. Báo cáo kết quả xử lý sự cố.

Bước 8. Tổng kết đánh giá kết quả.

Bước 9. Báo cáo kết quả ứng cứu sự cố và lưu hồ sơ.

**Điều 42. Ứng phó sự cố an toàn thông tin, an ninh mạng**

1. Kế hoạch ứng phó sự cố bảo đảm an toàn thông tin, an ninh mạng

a) Hằng năm, các đơn vị tổ chức xây dựng, phê duyệt kế hoạch ứng phó sự cố an toàn thông tin, an ninh mạng cho các hệ thống thông tin do đơn vị mình trực tiếp quản lý. Tổ chức triển khai kế hoạch sau khi được phê duyệt.

b) Kế hoạch ứng phó sự cố của đơn vị phải gửi cho Trung tâm Công nghệ thông tin trước ngày 31 tháng 10 hằng năm để tổng hợp thành kế hoạch chung của Bộ. Trung tâm Công nghệ thông tin có trách nhiệm xây dựng kế hoạch ứng phó sự cố của Bộ Giao thông vận tải, trình Lãnh đạo Bộ phê duyệt.

2. Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố

a) Triển khai hệ thống/phương tiện lưu trữ độc lập với hệ thống lưu trữ trên các máy chủ dịch vụ để sao lưu dự phòng; phân loại và quản lý thông tin, dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau; thực hiện sao lưu, dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

b) Triển khai phương án dự phòng nóng cho các thiết bị mạng chính bảo đảm khả năng vận hành liên tục của hệ thống; năng lực của thiết bị dự phòng phải đáp ứng theo quy mô hoạt động của hệ thống.

c) Triển khai hệ thống/phương tiện lưu trữ nhật ký độc lập và phù hợp với hoạt động của các thiết bị mạng. Dữ liệu nhật ký phải được lưu tối thiểu 06 tháng.

d) Triển khai hệ thống/phương tiện chống thất thoát dữ liệu trong hệ thống.

3. Diễn tập bảo đảm an toàn thông tin, an ninh mạng

a) Chủ quản hệ thống thông tin tổ chức diễn tập bảo đảm an toàn thông tin, an ninh mạng theo kế hoạch ứng phó sự cố an toàn thông tin, an ninh mạng của đơn vị được phê duyệt. Tham gia các cuộc diễn tập chức diễn tập bảo đảm an toàn thông tin, an ninh mạng do Bộ Thông tin và Truyền thông, Bộ Công an và Bộ Giao thông vận tải tổ chức.

b) Trung tâm Công nghệ thông tin chủ trì, phối hợp với các đơn vị thuộc Bộ tổ chức diễn tập bảo đảm an toàn thông tin, an ninh mạng chung của Bộ.

## Mục 10
## ĐẢM BẢO HOẠT ĐỘNG LIÊN TỤC CỦA HỆ THỐNG THÔNG TIN

### Điều 43. Xây dựng hệ thống dự phòng

1. Đơn vị phải xây dựng hoặc thuê 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 44. 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, an ninh mạng.

### Điều 45. Quản lý, vận hành hoạt động bình thường của hệ thống

1. Thường xuyên kiểm tra cấu hình, các file nhật ký hoạt động của hệ điều hành, phần mềm nhằm kịp thời phát hiện và xử lý những sự cố (nếu có).

2. Quản lý các thay đổi cấu hình kỹ thuật; thường xuyên cập nhật các bản vá lỗi và loại bỏ các thành phần của hệ điều hành, phần mềm không cần thiết hoặc không còn nhu cầu sử dụng.

3. Các bản quyền phần mềm cần được thống kê, quản lý thời gian phục vụ cho việc gia hạn.

4. Triển khai hệ thống phát hiện phòng chống xâm nhập giữa các vùng mạng quan trọng.

5. Sử dụng thêm các phương pháp xác thực đa nhân tố đối với các thiết bị mạng quan trọng.

6. Triển khai phương án cảnh báo thời gian thực trực tiếp đến người quản trị hệ thống thông qua hệ thống giám sát khi phát hiện sự cố trên các thiết bị mạng.

7. Duy trì ít nhất 02 kết nối mạng Internet từ các nhà cung cấp dịch vụ Internet sử dụng hạ tầng kết nối trong nước khác nhau (nếu hệ thống buộc phải có kết nối mạng Internet).

## Mục 11

## KIỂM TRA, GIÁM SÁT AN TOÀN THÔNG TIN, AN NINH MẠNG

### Điều 46. Quản lý điểm yếu an toàn thông tin, an ninh mạng

Chính sách, quy trình quản lý điểm yếu an toàn thông tin, an ninh mạng bao gồm các nội dung:

1. Quản lý thông tin các thành phần có trong hệ thống có khả năng tồn tại điểm yếu an toàn thông tin, an ninh mạng: thiết bị hệ thống, hệ điều hành, máy chủ, ứng dụng, dịch vụ và các thành phần khác (nếu có).

2. Quản lý, cập nhật nguồn cung cấp điểm yếu an toàn thông tin, an ninh mạng; phân nhóm và mức độ của điểm yếu cho các thành phần trong hệ thống đã xác định.

3. Cơ chế phối hợp với các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục điểm yếu an toàn thông tin, an ninh mạng.

4. Kiểm tra, đánh giá và xử lý điểm yếu an toàn thông tin, an ninh mạng cho thiết bị hệ thống, máy chủ, dịch vụ trước khi đưa vào sử dụng.

### Điều 47. Kiểm tra, đánh giá an toàn thông tin, an ninh mạng

1. Chủ quản hệ thống thông tin có trách nhiệm chỉ đạo, tổ chức thực hiện kiểm tra, đánh giá an toàn thông tin, an ninh mạng trong phạm vi cơ quan, tổ chức mình.

2. Định kỳ kiểm tra, đánh giá an toàn thông tin, an ninh mạng theo quy định tại điểm c khoản 2 Điều 20 Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ.

### Điều 48. Giám sát an toàn thông tin, an ninh mạng

1. Nguyên tắc giám sát

a) Đảm bảo được thực hiện thường xuyên, liên tục.

b) Chủ động theo dõi, phân tích, phòng ngừa để kịp thời phát hiện, ngăn chặn rủi ro, sự cố an toàn thông tin, an ninh mạng.

c) Đảm bảo hoạt động ổn định, bí mật cho thông tin được cung cấp, trao đổi trong quá trình giám sát.

2. Yêu cầu giám sát

a) Chủ quản hệ thống thông tin có trách nhiệm chủ động thực hiện giám sát an toàn thông tin, an ninh mạng đối với các hệ thống thông tin do mình quản lý theo quy định hiện hành.

b) Đối với hệ thống thông tin cấp độ 3 trở lên, hoạt động giám sát an toàn thông tin, an ninh mạng cần đáp ứng các yêu cầu tối thiểu quy định tại Điều 5 Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin.

c) Chủ quản hệ thống thông tin có trách nhiệm cử cá nhân hoặc bộ phận làm đầu mối giám sát, cảnh báo an toàn thông tin, an ninh mạng để phối hợp với các cơ quan chức năng liên quan.

3. Quản lý giám sát

Chính sách, quy trình quản lý giám sát an toàn thông tin, an ninh mạng bao gồm các nội dung sau:

a) Quản lý, vận hành hoạt động bình thường của hệ thống giám sát.

b) Đối tượng giám sát bao gồm: thiết bị hệ thống, máy chủ, ứng dụng, dịch vụ và các thành phần khác trong hệ thống (nếu có).

c) Kết nối và gửi nhật ký hệ thống từ đối tượng giám sát về hệ thống giám sát.

d) Truy cập và quản trị hệ thống giám sát.

đ) Loại thông tin cần được giám sát.

e) Lưu trữ và bảo vệ thông tin giám sát (nhật ký hệ thống).

g) Đồng bộ thời gian giữa hệ thống giám sát và thiết bị được giám sát.

h) Theo dõi, giám sát và cảnh báo sự cố phát hiện được trên hệ thống thông tin.

i) Bố trí nguồn lực và tổ chức giám sát an toàn hệ thống thông tin 24/7.

## Mục 12
## CHẾ ĐỘ BÁO CÁO

### Điều 49. 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 thông tin, an ninh mạng theo quy định tại Quy chế này;

- Các nội dung chỉnh sửa, bổ sung quy chế bảo đảm an toàn thông tin, an ninh mạng 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, an ninh 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 (nếu có).

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

## Chương III
## ĐIỀU KHOẢN THI HÀNH

**Điều 50. Trách nhiệm thi hành**

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

a) Theo dõi, tổng hợp báo cáo Bộ Giao thông vận tải tình hình thực hiện công tác bảo đảm an toàn thông tin, an ninh mạng 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./.