

Số: /QĐ-BTNMT

Hà Nội, ngày tháng năm 2023

QUYẾT ĐỊNH

**Ban hành Quy chế bảo đảm an toàn, an ninh thông tin mạng
Bộ Tài nguyên và Môi trường**

BỘ TRƯỞNG BỘ TÀI NGUYÊN VÀ MÔI TRƯỜNG

Căn cứ Luật An toàn thông tin mạng năm 2015;

Căn cứ Luật An ninh mạng năm 2018;

Căn cứ Luật Bảo vệ bí mật nhà nước năm 2018;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Nghị định số 53/2022/NĐ-CP ngày 15 tháng 8 năm 2022 của Chính phủ về quy định chi tiết một số điều của Luật An ninh mạng;

Căn cứ Nghị định số 68/2022/NĐ-CP ngày 22 tháng 9 năm 2022 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Tài nguyên và Môi trường;

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 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 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc;

Căn cứ Thông tư số 31/2017/TT-BTTTT ngày 15 tháng 11 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 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 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Theo đề nghị của Cục trưởng Cục Chuyển đổi số và Thông tin dữ liệu tài nguyên môi trường.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn, an ninh thông tin mạng Bộ Tài nguyên và Môi trường.

Điều 2. Quyết định này có hiệu lực từ ngày ký và thay thế Quyết định số 3210/QĐ-BTNMT ngày 24 tháng 10 năm 2018 của Bộ trưởng Bộ Tài nguyên và Môi trường Ban hành Quy chế bảo đảm an toàn, an ninh thông tin mạng Bộ Tài nguyên và Môi trường.

Điều 3. Chánh Văn phòng Bộ; Cục trưởng Cục Chuyển đổi số và Thông tin dữ liệu tài nguyên môi trường; Thủ trưởng các đơn vị trực thuộc Bộ Tài nguyên và Môi trường; công chức, viên chức Bộ Tài nguyên và Môi trường và tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:

- Như Điều 3;
- Bộ Thông tin và Truyền thông;
- Văn phòng Chính phủ;
- Bộ Công an;
- Bộ Quốc phòng;
- Bộ trưởng, các Thứ trưởng;
- Sở Tài nguyên và Môi trường các tỉnh, thành phố;
- Công thông tin điện tử Bộ;
- Lưu: VT, CĐS.

**KT. BỘ TRƯỞNG
THỨ TRƯỞNG**

Trần Quý Kiên

QUY CHẾ
BẢO ĐẢM AN TOÀN, AN NINH THÔNG TIN MẠNG
BỘ TÀI NGUYÊN VÀ MÔI TRƯỜNG

(Kèm theo Quyết định số /QĐ-BTNMT ngày tháng năm 2023
của Bộ trưởng Bộ Tài nguyên và Môi trường)

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, an ninh thông tin mạng trong các hoạt động của Bộ Tài nguyên và Môi trường và các đơn vị trực thuộc Bộ.

2. Đối tượng áp dụng

a) Các đơn vị trực thuộc Bộ Tài nguyên và Môi trường (sau đây gọi là đơn vị trực thuộc Bộ) và cán bộ, công chức, viên chức và người lao động thuộc các đơn vị trực thuộc Bộ.

b) Cơ quan, tổ chức, cá nhân có kết nối vào hệ thống mạng của Bộ Tài nguyên và Môi trường.

c) Cơ quan, tổ chức, cá nhân cung cấp dịch vụ công nghệ thông tin và an toàn thông tin mạng cho các đơn vị trực thuộc 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 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. *Trang thông tin điện tử* là hệ thống thông tin dùng để thiết lập một hoặc nhiều trang thông tin được trình bày dưới dạng ký hiệu, số, chữ viết, hình ảnh, âm thanh và các dạng thông tin khác phục vụ cho việc cung cấp và sử dụng thông tin trên Internet.

7. *Cổng thông tin điện tử* là điểm truy nhập duy nhất của cơ quan, đơn vị trên môi trường mạng, liên kết, tích hợp các kênh thông tin, các dịch vụ và các ứng dụng mà qua đó người dùng có thể khai thác, sử dụng và cá nhân hóa việc hiển thị thông tin.

8. *Sự cố an toàn thông tin mạng* là việc thông tin, hệ thống thông tin bị gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng.

Điều 3. Nguyên tắc bảo đảm an toàn, an ninh thông tin mạng

1. Bảo đảm an toàn, an ninh thông tin là yêu cầu bắt buộc, thường xuyên, liên tục, có tính xuyên suốt quá trình liên quan đến thông tin và thiết kế, xây dựng, vận hành, nâng cấp, hủy bỏ hệ thống thông tin. Bảo đảm an toàn, an ninh thông tin tuân thủ các nguyên tắc chung quy định tại Điều 4 Luật An toàn thông tin mạng và Điều 4 Nghị định số 85/2016/NĐ-CP và các quy định pháp luật khác có liên quan.

2. Tuân thủ các quy định và hướng dẫn về bảo đảm an toàn, an ninh thông tin của cơ quan có thẩm quyền. Trường hợp có văn bản, quy định cập nhật, thay thế hoặc quy định khác tại văn bản quy phạm pháp luật, quyết định của cấp có thẩm quyền cao hơn thì áp dụng quy định tại văn bản đó.

3. Trách nhiệm bảo đảm an toàn thông tin mạng và an ninh mạng gắn với trách nhiệm của người đứng đầu cơ quan, đơn vị và cá nhân trực tiếp liên quan.

4. Việc bảo đảm an toàn hệ thống thông tin 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. Các nhiệm vụ, dự án ứng dụng công nghệ thông tin hoặc có cấu phần công nghệ thông tin thuộc phạm vi quy định tại khoản 1 và khoản 2 Điều 1 của Nghị định 73/2019/NĐ-CP ngày 05/9/2019 của Chính phủ quy định quản lý đầu tư ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước phải có ý kiến thẩm định nội dung liên quan đến an toàn, an ninh thông tin, phê duyệt hồ sơ cấp độ và phương án bảo đảm an toàn hệ thống thông tin theo cấp độ trước khi được phê duyệt.

5. Quản lý, sử dụng và bảo đảm an ninh mạng, mạng máy tính nội bộ có lưu trữ, truyền đưa bí mật nhà nước phải được tách biệt vật lý hoàn toàn với mạng máy tính, các thiết bị, phương tiện điện tử có kết nối mạng Internet, trường hợp khác phải bảo đảm quy định của pháp luật về bảo vệ bí mật nhà nước;

6. Xử lý sự cố an toàn thông tin 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 quy định tại Điều 7 Luật An toàn thông tin mạng, Điều 8 Luật An ninh mạng và Điều 5 Luật Bảo vệ bí mật nhà nước.

2. Tự ý đầu nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập mạng không dây của cá nhân vào mạng nội bộ; tự ý thay đổi, gỡ bỏ biện pháp an toàn thông tin cài đặt trên thiết bị công nghệ thông tin phục vụ công việc; tự ý thay thế, lắp mới, tháo đổi thành phần của máy tính phục vụ công việc.

3. Sử dụng hạ tầng, trang thiết bị công nghệ thông tin của cơ quan, đơn vị để đào tiền ảo, đánh bạc, cá độ.

4. Phát tán thư rác, phần mềm độc hại, thiết lập hệ thống thông tin giả mạo, lừa đảo.

5. Thu thập, sử dụng, phát tán, kinh doanh trái pháp luật thông tin cá nhân của người khác; lợi dụng sơ hở, điểm yếu của hệ thống thông tin để thu thập, khai thác thông tin cá nhân.

6. Bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã và thông tin của cơ quan, cá nhân khác trên môi trường mạng.

7. Gây ảnh hưởng, cản trở trái pháp luật tới hoạt động bình thường của hệ thống thông tin hoặc tới khả năng truy nhập hệ thống thông tin của người sử dụng.

8. Các hành vi khác làm mất an toàn, bí mật thông tin của cơ quan, cá nhân khác được trao đổi, truyền đưa, lưu trữ trên môi trường mạng.

Chương II

QUY ĐỊNH BẢO ĐẢM AN TOÀN, AN NINH THÔNG TIN MẠNG

Điều 5. Xác định cấp độ và phương án bảo đảm an toàn hệ thống thông tin

1. Việc xác định cấp độ hệ thống thông tin và xây dựng phương án bảo vệ hệ thống thông tin theo cấp độ phục vụ mục đích đánh giá an toàn thông tin và bảo đảm an toàn thông tin cho các hệ thống thông tin. Nguyên tắc bảo đảm an toàn thông tin theo cấp độ và nguyên tắc xác định cấp độ căn cứ trên các nguyên tắc quy định tại Điều 4, Điều 5 Nghị định 85/2016/NĐ-CP.

2. Chủ quản hệ thống thông tin

a) Bộ Tài nguyên và Môi trường là chủ quản hệ thống thông tin đối với các hệ thống do Bộ quyết định đầu tư hoặc Bộ được giao làm chủ đầu tư nhiệm vụ, dự án xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin.

b) Các đơn vị trực thuộc Bộ là chủ quản hệ thống thông tin do đơn vị quyết định đầu tư dự án xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin hoặc được Bộ ủy quyền theo quy định tại khoản 3 Điều 4 Thông tư số 12/2022/TT-BTTTT.

c) Chủ quản hệ thống thông tin (hoặc đơn vị được ủy quyền quản lý trực tiếp hệ thống thông tin) thực hiện trách nhiệm theo quy định tại Điều 20 Nghị định 85/2016/NĐ-CP.

3. Đơn vị chuyên trách về an toàn thông tin

a) Cục Chuyển đổi số và Thông tin dữ liệu tài nguyên môi trường là đơn vị chuyên trách về an toàn thông tin của Bộ Tài nguyên và Môi trường.

b) Đơn vị chuyên trách về công nghệ thông tin, chuyển đổi số tại các đơn vị trực thuộc Bộ đồng thời là đơn vị chuyên trách về an toàn thông tin.

4. Đơn vị vận hành hệ thống thông tin

a) Giao Cục Chuyển đổi số và Thông tin dữ liệu tài nguyên môi trường là đơn vị vận hành các hệ thống thông tin, cơ sở dữ liệu dùng chung của Bộ và các hệ thống thông tin do các Vụ trực thuộc Bộ làm chủ quản.

b) Các hệ thống thông tin trước khi đưa vào khai thác, sử dụng phải được giao cho đơn vị quản lý, vận hành. Đơn vị vận hành hệ thống thông tin theo quy định tại Điều 5 Thông tư số 12/2022/TT-BTTTT.

5. Trình tự, thủ tục, thẩm quyền xác định cấp độ hệ thống thông tin

a) Đơn vị lập hồ sơ đề xuất cấp độ:

Đối với các hệ thống thông tin thuộc các nhiệm vụ, dự án đang trong giai đoạn lập dự án, đơn vị lập dự án lập hồ sơ đề xuất cấp độ. Đối với các hệ thống thông tin đang triển khai và vận hành, đơn vị vận hành lập hồ sơ đề xuất cấp độ.

b) Đối với các hệ thống thông tin do các đơn vị trực thuộc Bộ làm chủ quản và được đề xuất từ cấp độ 3 trở lên thì đơn vị chuyên trách về an toàn thông tin của các đơn vị trực thuộc Bộ cần gửi xin ý kiến chuyên môn của Cục Chuyển đổi số và Thông tin dữ liệu tài nguyên môi trường trước khi trình các cấp có thẩm quyền thẩm định, phê duyệt cấp độ.

c) Nội dung của hồ sơ đề xuất cấp độ hệ thống thông tin theo quy định tại Điều 15 Nghị định 85/2016/NĐ-CP và Điều 8, Điều 9 Thông tư số 12/2022/TT-BTTTT.

d) Nội dung, thời gian thẩm định hồ sơ đề xuất cấp độ hệ thống thông tin quy định tại Điều 16 Nghị định 85/2016/NĐ-CP.

đ) Thẩm quyền, trình tự, thủ tục xác định cấp độ hệ thống thông tin theo quy định tại Điều 12, Điều 13, Điều 14 Nghị định 85/2016/NĐ-CP và Điều 6 Thông tư số 12/2022/TT-BTTTT.

6. Phương án bảo đảm an toàn hệ thống thông tin

a) Phương án bảo đảm an toàn hệ thống thông tin phải phù hợp với cấp độ của hệ thống thông tin và đáp ứng yêu cầu quy định tại Thông tư số 12/2022/TT-BTTTT, phù hợp với tiêu chuẩn TCVN 11930:2017, các tiêu chuẩn, quy chuẩn kỹ thuật khác và chính sách an toàn thông tin mạng của Bộ Tài nguyên và Môi trường, chính sách an toàn thông tin mạng của các đơn vị trực thuộc Bộ (nếu có).

b) Chủ quản hệ thống thông tin hoặc đơn vị được ủy quyền quản lý trực tiếp hệ thống thông tin tổ chức triển khai phương án bảo đảm an toàn hệ thống thông tin sau khi hồ sơ đề xuất cấp độ hoặc phương án bảo đảm an toàn hệ thống được phê duyệt.

c) Đơn vị/bộ phận chuyên trách về an toàn thông tin thuộc đơn vị chịu trách nhiệm giám sát việc triển khai các phương án bảo đảm an toàn thông tin đã được phê duyệt.

7. Quy chế bảo đảm an toàn, an ninh mạng cho hệ thống thông tin phải được xây dựng, đáp ứng các yêu cầu về quản lý theo cấp độ an toàn hệ thống thông tin tương ứng; có thể ban hành độc lập hoặc lồng ghép vào Quy chế quản lý, duy trì, vận hành, sử dụng hệ thống thông tin; và được cấp có thẩm quyền phê duyệt, ban hành trước khi Hồ sơ đề xuất cấp độ được phê duyệt.

8. Chủ quản hệ thống thông tin có trách nhiệm rà soát, xác định hệ thống mạng thông tin và thông tin quan trọng cần ưu tiên bảo đảm an ninh mạng theo Điều 3 Nghị định 53/2022/NĐ-CP.

Điều 6. Bảo đảm an toàn thông tin về vật lý đối với trung tâm dữ liệu, phòng máy chủ

1. Trung tâm dữ liệu/phòng máy chủ

a) Là khu vực hạn chế tiếp cận, chỉ những cá nhân có quyền, nhiệm vụ theo quy định của thủ trưởng cơ quan, đơn vị mới được phép vào trung tâm dữ liệu/phòng máy chủ. Quá trình vào, ra phòng máy chủ phải được ghi nhận vào nhật ký quản lý trung tâm dữ liệu/phòng máy chủ.

b) Phải được trang bị hệ thống lưu điện đủ công suất và duy trì thời gian hoạt động của các máy chủ ít nhất 15 phút khi có sự cố mất điện.

c) Phải có hệ thống giám sát và đảm bảo an toàn phù hợp với yêu cầu của từng cấp độ an toàn theo quy định tại Phụ lục A - Yêu cầu cơ bản về an toàn vật lý cho hệ thống thông tin theo cấp độ tại TCVN 11930:2017.

d) Đơn vị chủ quản trung tâm dữ liệu/phòng máy chủ có trách nhiệm xây dựng nội quy hoặc hướng dẫn làm việc tại khu vực này; phải cử cán bộ thường xuyên giám sát thiết bị, hạ tầng của trung tâm dữ liệu/phòng máy chủ.

2. Các thiết bị kết nối mạng, thiết bị bảo mật quan trọng như tường lửa, thiết bị định tuyến, hệ thống máy chủ, hệ thống lưu trữ...

a) Phải được đặt trong trung tâm dữ liệu/phòng máy chủ.

b) Phải được thiết lập cơ chế bảo vệ, theo dõi phát hiện xâm nhập và biện pháp kiểm soát truy nhập, kết nối vật lý phù hợp với từng khu vực: máy chủ và hệ thống lưu trữ; tủ mạng và đầu nối; thiết bị nguồn điện và dự phòng điện khẩn cấp; vận hành, kiểm soát, quản trị hệ thống.

Điều 7. Quản lý an toàn thông tin mạng máy tính

1. Hệ thống mạng nội bộ

a) Phải được thiết kế phân vùng theo chức năng cơ bản (theo các chính sách an toàn thông tin riêng), bao gồm: vùng mạng người dùng; vùng mạng kết nối hệ thống ra bên ngoài Internet và các mạng khác; vùng mạng máy chủ công cộng; vùng mạng máy chủ nội bộ; vùng mạng máy chủ quản trị.

b) Dữ liệu trao đổi giữa các vùng mạng phải được quản lý, giám sát bởi hệ thống các thiết bị bảo mật và giám sát an toàn, an ninh thông tin.

c) Thiết lập, cấu hình các tính năng theo thiết kế của các trang thiết bị bảo mật mạng; thực hiện các biện pháp, giải pháp để dò tìm và phát hiện kịp thời các điểm yếu, lỗ hổng về mặt kỹ thuật của hệ thống mạng; thường xuyên kiểm tra, phát hiện những kết nối, trang thiết bị, phần mềm cài đặt bất hợp pháp vào mạng.

d) Định kỳ sao lưu cấu hình thiết bị kết nối mạng nội bộ. Lưu trữ tối thiểu trong 03 tháng đối với nhật ký của các thiết bị mạng và bảo đảm đồng bộ thời gian nhật ký với máy chủ thời gian thực theo múi giờ Việt Nam.

đ) Định kỳ thực hiện kiểm soát các phần mềm cài đặt, cập nhật, vá lỗi các điểm yếu bảo mật phần mềm, máy tính cá nhân, thiết bị kết nối mạng đang hoạt động thuộc hệ thống mạng nội bộ.

e) Các đường truyền dữ liệu, đường truyền Internet và các hệ thống dây cáp mạng phải được lắp đặt trong ống, máng che đậy kín, hạn chế khả năng tiếp cận trái phép. Ngắt kết nối các cổng mạng không sử dụng.

g) Không được tiết lộ thiết kế, thông số cấu hình hệ thống mạng nội bộ cho tổ chức, cá nhân khác khi không được phép; Không được tìm cách truy cập dưới bất cứ hình thức nào vào các khu vực không được phép truy cập.

2. Kết nối mạng Internet

Các đơn vị trực thuộc Bộ phải áp dụng các biện pháp kỹ thuật cần thiết bảo đảm an toàn thông tin trong kết nối vào Internet, tối thiểu đáp ứng các yêu cầu sau:

a) Có hệ thống tường lửa và hệ thống bảo vệ truy cập Internet, đáp ứng nhu cầu kết nối đồng thời, hỗ trợ các công nghệ mạng riêng ảo thông dụng và có khả năng bảo vệ hệ thống trước các loại tấn công từ chối dịch vụ.

b) Lọc bỏ, không cho phép truy nhập các trang tin có nghi ngờ chứa mã độc; hoạt động đánh bạc, lừa đảo trực tuyến; tuyên truyền phản động hoặc các nội dung không phù hợp khác.

3. Các đơn vị khi có nhu cầu kết nối trang thiết bị vào hệ thống mạng máy tính của Bộ Tài nguyên và Môi trường với mục đích phục vụ công việc, có trách nhiệm thông báo bằng công văn cho Cục Chuyển đổi số và Thông tin dữ liệu tài nguyên môi trường để phối hợp thực hiện việc kết nối vào mạng máy tính của Bộ.

4. Các đơn vị và cá nhân tham gia vào hệ thống mạng máy tính không được tự ý thay đổi những thông số mạng hay tự ý đưa các thiết bị mạng, thiết bị viễn thông khác tham gia kết nối vào hệ thống mạng.

5. Các cơ quan bên ngoài khi có kết nối trực tiếp vào mạng của Bộ Tài nguyên và Môi trường phải được sự đồng ý bằng văn bản của Cục Chuyển đổi số và Thông tin dữ liệu tài nguyên môi trường và tuân theo các quy định, các tiêu chuẩn kỹ thuật phù hợp với hệ thống mạng của Bộ Tài nguyên và Môi trường.

Điều 8. Quản lý an toàn thông tin cho máy chủ và ứng dụng

1. Hệ thống máy chủ

a) Phải được đặt trong các vùng mạng dành riêng cho máy chủ, tối thiểu gồm vùng mạng máy chủ công cộng, vùng mạng máy chủ nội bộ và vùng mạng máy chủ quản trị.

b) Chỉ cho phép kết nối đến những dịch vụ cần thiết trên Internet.

c) Chỉ mở và cung cấp các dịch vụ cần thiết ra Internet.

d) Chỉ cài đặt và sử dụng các phần mềm đúng bản quyền, nguồn gốc rõ ràng, thực sự cần thiết. Không sử dụng các phần mềm đã được cảnh báo không an toàn hoặc không được nhà sản xuất hỗ trợ kỹ thuật khi không thực sự cần thiết.

đ) Cài đặt các giải pháp phòng chống mã độc tập trung và phòng chống tấn công xâm nhập mạng phù hợp với yêu cầu theo từng cấp độ.

e) Triển khai các biện pháp sao lưu dự phòng để nâng cao khả năng phục hồi hoạt động khi xảy ra sự cố.

g) Giám sát thường xuyên, liên tục để phát hiện và cảnh báo sớm nguy cơ mất an toàn thông tin.

2. Các phần mềm, ứng dụng, dịch vụ cài đặt trên máy chủ

a) Yêu cầu về bảo đảm an toàn thông tin phải được đưa vào tất cả các công đoạn thiết kế, xây dựng, triển khai và vận hành, sử dụng phần mềm, ứng dụng, dịch vụ.

b) Phần mềm, ứng dụng phải đáp ứng các yêu cầu sau: cấu hình phần mềm, ứng dụng để xác thực người sử dụng; giới hạn số lần đăng nhập sai liên tiếp; giới hạn thời gian để chờ đóng phiên kết nối; mã hóa thông tin xác thực trên hệ thống; không khuyến khích việc đăng nhập tự động.

c) Thiết lập, phân quyền truy nhập, quản trị, sử dụng tài nguyên khác nhau của phần mềm, ứng dụng với người sử dụng/nhóm người sử dụng có chức năng, yêu cầu nghiệp vụ khác nhau; tách biệt cổng giao tiếp quản trị phần mềm ứng dụng với cổng giao tiếp cung cấp dịch vụ; đóng các cổng giao tiếp không sử dụng.

d) Chỉ cho phép sử dụng các giao thức mạng có hỗ trợ chức năng mã hóa thông tin như SSH, SSL, VPN hoặc tương đương khi truy nhập, quản trị phần mềm, ứng dụng từ xa trên môi trường mạng; hạn chế truy cập đến mã nguồn của phần mềm, ứng dụng và phải đặt mã nguồn trong môi trường an toàn do bộ phận chuyên trách công nghệ thông tin quản lý.

đ) Ghi và lưu giữ bản ghi nhật ký hệ thống của phần mềm, ứng dụng trong khoảng thời gian tối thiểu 03 tháng với những thông tin cơ bản: thời gian, địa chỉ kết nối, tài khoản (nếu có), nội dung truy cập dữ liệu và sử dụng phần mềm, ứng dụng, dịch vụ; các lỗi phát sinh trong quá trình hoạt động; thông tin đăng nhập khi quản trị, thông tin thay đổi cấu hình máy chủ.

e) Phần mềm, ứng dụng cần được kiểm tra phát hiện và khắc phục các điểm yếu về an toàn, an ninh thông tin trước khi đưa vào sử dụng và trong quá trình sử dụng. Định kỳ thực hiện quy trình kiểm soát cài đặt, cập nhật, vá lỗi bảo mật phần mềm, ứng dụng trên các máy chủ.

3. Tài khoản và thiết bị phục vụ quản trị hệ thống.

a) Tài khoản quản trị

- Tài khoản quản trị hệ thống phải tách biệt với tài khoản truy cập của người dùng thông thường. Tài khoản hệ thống phải được giao đích danh cá nhân làm công tác quản trị. Hạn chế dùng chung tài khoản quản trị.

- Mật khẩu quản trị phải được quản lý trong các phần mềm mã hóa trên các thiết bị dành riêng cho quản trị hệ thống. Trường hợp cần thiết để bảo đảm an toàn, an ninh cho hệ thống, phải triển khai hệ thống quản lý tài khoản đặc quyền để thực hiện quản lý, lưu giữ, cấp phát tài khoản quản trị hệ thống.

- Mật khẩu phải được thay đổi tối thiểu 02 tháng một lần.

b) Mật khẩu tài khoản dùng để quản trị hệ thống thông tin; truy cập thiết bị lưu khóa bí mật phải đáp ứng các yêu cầu sau:

- Có tối thiểu 10 ký tự.

- Gồm tối thiểu 3 trong 5 loại ký tự sau: chữ cái viết hoa (A - Z); chữ cái viết thường (a - z); chữ số (0 - 9); các ký tự khác trên bàn phím máy tính (' ~ ! @ # \$ % ^ & * () _ - + = { } [] \ | : ; “ ‘ < > , . ? /) và dấu cách.

- Không chứa tên tài khoản.

c) Thiết bị (máy tính cá nhân, máy tính xách tay, máy tính bảng, điện thoại...) phục vụ quản trị hệ thống

- Chỉ được sử dụng cho mục đích quản trị hệ thống.

- Chỉ cài đặt và sử dụng các phần mềm quản trị đúng bản quyền, nguồn gốc rõ ràng, thực sự cần thiết.

- Không được kết nối trực tiếp đến máy chủ để thực hiện quản trị cấu hình mà phải kết nối với máy chủ quản trị qua các đường truyền có mã hóa bảo mật theo quy định.

Điều 9. Quản lý an toàn thông tin dữ liệu

1. Đơn vị phải thực hiện bảo vệ thông tin, dữ liệu liên quan đến hoạt động công vụ, thông tin có nội dung quan trọng, nhạy cảm hoặc không phải là thông tin công khai bằng các biện pháp như: thiết lập phương án bảo đảm tính bí mật, nguyên vẹn và khả dụng của thông tin, dữ liệu; mã hóa thông tin, dữ liệu khi lưu trữ trên hệ thống/thiết bị lưu trữ dữ liệu di động; sử dụng chữ ký số để xác thực và bảo mật thông tin, dữ liệu.

2. Đơn vị cần 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.

3. Trang thiết bị công nghệ thông tin 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 tiêu hủy cấu phần lưu trữ dữ liệu trên trang thiết bị công nghệ thông tin đó.

4. Trang thiết bị công nghệ thông tin có bộ phận lưu trữ hoặc thiết bị lưu trữ khi mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài hoặc ngừng sử dụng phải 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 phải xóa nội dung dữ liệu lưu trữ bằng phần mềm, thiết bị hủy dữ liệu chuyên dụng hoặc phá hủy vật lý.

5. Bộ trí máy tính riêng không kết nối mạng, đặt mật khẩu và các biện pháp bảo mật phù hợp để soạn thảo, lưu trữ thông tin, tài liệu mật. Đối với các thiết bị chứa thông tin mật bắt buộc phải kết nối mạng thì phải áp dụng các giải pháp bảo mật an toàn, an ninh thông tin được Ban Cơ yếu Chính phủ đánh giá và cho phép.

6. Các đơn vị trực thuộc Bộ phải thường xuyên kiểm tra, giám sát các hoạt động chia sẻ, gửi, nhận thông tin, dữ liệu trong hoạt động nội bộ của mình; khuyến cáo việc chia sẻ, gửi, nhận thông tin trên môi trường mạng cần phải sử dụng mật khẩu để bảo vệ thông tin.

7. Đối với hoạt động trao đổi thông tin, dữ liệu với bên ngoài, đơn vị và cá nhân thực hiện trao đổi thông tin, dữ liệu ra bên ngoài cam kết và có biện pháp bảo mật thông tin, dữ liệu được trao đổi. Giao dịch trực tuyến phải được truyền đầy đủ, đúng địa chỉ, tránh bị sửa đổi, tiết lộ hoặc nhân bản một cách trái phép; sử dụng các cơ chế xác thực mạnh, chữ ký số khi tham gia giao dịch, sử dụng các giao thức truyền thông an toàn.

Điều 10. Quản lý trang thiết bị đầu cuối

1. Giao, gán trách nhiệm cho cá nhân hoặc tập thể quản lý, sử dụng trang thiết bị công nghệ thông tin.

2. Quy định các quy tắc sử dụng, giữ gìn bảo vệ trang thiết bị công nghệ thông tin:

a) Cá nhân chỉ cài đặt phần mềm hợp lệ và thuộc danh mục phần mềm được phép sử dụng do cơ quan, đơn vị có thẩm quyền ban hành trên máy tính được cơ quan, đơn vị cấp cho mình; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm khi chưa có sự đồng ý của bộ phận chuyên trách về công nghệ thông tin; 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 cơ sở dữ liệu 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 tắt máy và 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 và các thông tin 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 được sự đồng ý của Lãnh đạo đơn vị; thực hiện các biện pháp bảo đảm an ninh, an toàn 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.

e) Báo cáo và phải được thủ trưởng cơ quan, đơn vị đồng ý, cho phép trước khi mang máy tính, thiết bị công nghệ thông tin có kết nối mạng thuộc sở hữu riêng đến nơi làm việc và kết nối với mạng nội bộ để xử lý công việc.

3. Các đơn vị trực thuộc Bộ có trách nhiệm xây dựng quy trình bảo dưỡng, bảo trì và hướng dẫn cách sử dụng, quản lý, vận hành hệ thống hạ tầng kỹ thuật của mình; chỉ định bộ phận chuyên trách về công nghệ thông tin thực hiện quản lý, vận hành và định kỳ kiểm tra, sửa chữa, bảo trì thiết bị (bao gồm thiết bị đang hoạt động và thiết bị dự phòng).

Điều 11. Quản lý tài khoản truy cập

1. 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. Các hệ thống thông tin dùng chung của Bộ sử dụng cơ chế đăng nhập một lần, chung một tài khoản truy nhập và mật khẩu.

2. Trường hợp người dùng thay đổi vị trí công tác, chuyển công tác, thôi việc hoặc nghỉ hưu thì đơn vị quản lý người dùng phải thông báo bằng văn bản cho chủ quản hệ thống thông tin, phần mềm ứng dụng để thực hiện điều chỉnh, thu hồi, hủy bỏ các quyền sử dụng của người dùng đó. Quy định cụ thể như sau:

a) Văn bản đề nghị cấp mới/thêm quyền/sửa quyền/ xóa tài khoản khi người dùng thay đổi vị trí công tác, chuyển công tác, thôi việc, nghỉ hưu phải gửi về chủ quản hệ thống thông tin, phần mềm ứng dụng. Trường hợp thay đổi vị trí công tác không sử dụng hình thức văn bản quyết định, đơn vị quản lý người dùng phải thông báo cho chủ quản hệ thống thông tin, phần mềm ứng dụng bằng công văn hoặc theo cách thức quy định trong quy trình quản lý tài khoản công nghệ thông tin áp dụng tại đơn vị chủ quản hệ thống thông tin, phần mềm ứng dụng.

b) Tài khoản phải được điều chỉnh, thu hồi, hủy bỏ trong thời gian không quá 03 ngày làm việc tính từ ngày người dùng chính thức chuyển công tác ra khỏi Bộ, thôi việc, nghỉ hưu; không quá 05 ngày làm việc trong trường hợp thay đổi vị trí công tác hoặc chuyển công tác tới đơn vị khác thuộc Bộ.

c) Phải có văn bản đề nghị của đơn vị quản lý người dùng trong trường hợp cần duy trì tài khoản của người dùng sau thời điểm người dùng chính thức thay đổi vị trí công tác, chuyển công tác, thôi việc, nghỉ hưu; trong đó nêu rõ lý do, các quyền sử dụng cần duy trì và thời gian duy trì.

3. Người dùng có trách nhiệm bảo vệ thông tin tài khoản được cấp, không tiết lộ mật khẩu hoặc đưa cho người khác phương tiện xác thực tài khoản của mình ngoại trừ các trường hợp: cần xử lý công việc khẩn cấp của đơn vị; cần cung cấp, bàn giao cho đơn vị các thông tin, tài liệu do cá nhân quản lý.

4. Mật khẩu phải được đổi ngay sau khi nhận bàn giao từ người khác hoặc có thông báo về sự cố an toàn thông tin, điểm yếu liên quan đến khả năng lộ mật khẩu.

5. Khi có yêu cầu khóa quyền truy cập hệ thống thông tin của tài khoản đang hoạt động, lãnh đạo đơn vị phải yêu cầu bằng văn bản gửi đơn vị chủ quản hệ thống thông tin. Đơn vị vận hành hệ thống thông tin thực hiện việc khóa quyền truy cập của tài khoản khi có chỉ đạo của đơn vị chủ quản hệ thống thông tin. Đơn vị chủ quản hệ thống thông tin có quyền khóa quyền truy cập của tài khoản trong trường hợp tài khoản đó thực hiện các hành vi tấn công hoặc để xảy ra vấn đề mất an toàn, an ninh thông tin.

6. Hệ thống tài khoản công nghệ thông tin phải được rà soát hàng năm, bảo đảm các tài khoản và quyền truy cập hệ thống được cấp phát đúng. Các tài khoản không sử dụng trong thời gian 01 năm phải bị khóa hoặc xóa bỏ (sau khi trao đổi, xác nhận với đơn vị sử dụng).

7. Việc quản lý tài khoản thư điện tử của Bộ Tài nguyên và Môi trường theo quy định của Quy chế quản lý, sử dụng hệ thống thư điện tử của Bộ Tài nguyên và Môi trường (Quyết định số 2019/QĐ-BTNMT ngày 01/9/2016). Công tác phòng chống thư rác theo quy định tại Nghị định số 91/2020/NĐ-CP ngày 14 tháng 8 năm 2020 của Chính phủ và Thông tư số 22/2021/TT-BTTTT ngày 13/12/2021 của Bộ Thông tin và Truyền thông quy định chi tiết một số điều của Nghị định số 91/2020/NĐ-CP ngày 14 tháng 8 năm 2020 của Chính phủ về chống tin nhắn rác, thư điện tử rác, cuộc gọi rác.

Điều 12. Bảo đảm an toàn, an ninh thông tin trong việc quản lý cán bộ, công chức, viên chức và người lao động

1. Điều kiện, yêu cầu của nhân sự làm công tác quản trị mạng, vận hành hệ thống, bảo đảm an toàn, an ninh mạng

a) 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.

b) Có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, an toàn thông tin, phù hợp với vị trí tuyển dụng.

2. Quy định trách nhiệm bảo đảm an toàn, an ninh thông tin trong quản lý và sử dụng nhân sự

Các đơn vị trực thuộc Bộ có trách nhiệm:

a) Xác định các yêu cầu và trách nhiệm cụ thể của bộ phận, cán bộ, nhân viên trong việc bảo đảm an toàn, an ninh thông tin cho từng vị trí phân công.

b) Phổ biến cho nhân sự mới tuyên dụng các quy định về bảo đảm an toàn, an ninh thông tin tại đơn vị. Định kỳ tổ chức quán triệt các quy định về an toàn, an ninh thông tin, nhằm nâng cao nhận thức về trách nhiệm bảo đảm an toàn, an ninh thông tin của từng cá nhân trong đơn vị.

c) Đối với các vị trí tiếp xúc, quản lý các thông tin, dữ liệu quan trọng hoặc quản trị các hệ thống thông tin quan trọng, đơn vị phải yêu cầu nhân sự mới cam kết bảo mật thông tin bằng văn bản 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.

d) Có biện pháp quản lý tài khoản người dùng của cán bộ, công chức, viên chức và người lao động trên các hệ thống thông tin quan trọng.

đ) Thực hiện đúng quy trình cấp mới, quản lý và thu hồi tài khoản, phân quyền truy cập các hệ thống thông tin và tất cả các tài sản liên quan đến hệ thống thông tin đối với các cá nhân do đơn vị quản lý. Thường xuyên rà soát, kiểm tra quyền truy cập vào các hệ thống thông tin đối với tất cả cán bộ, công chức, viên chức và người lao động bảo đảm quyền truy cập phù hợp với nhiệm vụ được giao.

3. Khi cán bộ, công chức, viên chức và người lao động chấm dứt hoặc thay đổi công việc, các đơn vị phải:

a) Xác định rõ trách nhiệm của cán bộ, công chức, viên chức, người lao động và các bên liên quan trong quản lý, sử dụng các tài sản công nghệ thông tin được giao.

b) Lập biên bản bàn giao tài sản công nghệ thông tin với đơn vị chủ quản và các đơn vị liên quan.

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

d) 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 bảo đảm tài khoản người dùng của cán bộ, công chức, viên chức và người lao động đã nghỉ việc được thu hồi.

Điều 13. Bảo đảm an toàn, an ninh thông tin khi tiếp nhận, phát triển, vận hành và bảo trì hệ thống thông tin

1. Khi thực hiện nâng cấp, mở rộng, thay thế một phần hệ thống thông tin, phải rà soát cấp độ, phương án bảo đảm an toàn của hệ thống thông tin và thực hiện điều chỉnh, bổ sung hoặc thay mới hồ sơ đề xuất cấp độ trong trường hợp cần thiết.

2. Khi tiếp nhận, phát triển, nâng cấp, bảo trì hệ thống thông tin, đơn vị phải tiến hành phân tích, xác định rủi ro có thể xảy ra, đánh giá phạm vi tác động và phải chuẩn bị các biện pháp hạn chế, loại trừ các rủi ro này và yêu cầu các bên cung cấp, thi công, các cá nhân liên quan thực hiện.

3. Các hệ thống thông tin được cài đặt tại Trung tâm dữ liệu của Bộ cần đáp ứng các yêu cầu:

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

- b) Áp dụng các giải pháp bảo đảm an toàn, an ninh thông tin;
- c) Không cài đặt các công cụ, phương tiện phát triển ứng dụng;
- d) Loại bỏ hoặc tắt các tính năng, phần mềm tiện ích không sử dụng trên hệ thống thông tin;
- đ) Áp dụng các biện pháp bảo đảm tính toàn vẹn dữ liệu;
- e) Mọi thao tác trên hệ thống phải được lưu vết, sẵn sàng cho kiểm tra, kiểm soát khi cần thiết.

4. Trong quá trình vận hành hệ thống thông tin, đơn vị chủ quản hệ thống thông tin cần thực hiện đánh giá, phân loại hệ thống thông tin theo cấp độ; triển khai phương án bảo đảm an toàn hệ thống thông tin đáp ứng yêu cầu cơ bản trong tiêu chuẩn, quy chuẩn kỹ thuật về bảo đảm an toàn hệ thống thông tin theo cấp độ; thường xuyên kiểm tra, giám sát an toàn hệ thống thông tin; tuân thủ quy trình vận hành, quy trình xử lý sự cố đã xây dựng; ghi lại và lưu trữ đầy đủ thông tin nhật ký hệ thống để phục vụ quản lý, kiểm soát thông tin.

5. Các đơn vị thuộc Bộ liên quan đến việc phát triển phần mềm ứng dụng có trách nhiệm yêu cầu các đối tác (nếu có) thực hiện các công tác bảo đảm an toàn thông tin, tránh lộ, lọt mã nguồn và dữ liệu, tài liệu thiết kế, quản trị hệ thống mà đối tác đang xử lý ra bên ngoài.

Điều 14. Giám sát an toàn, an ninh thông tin mạng

1. Chủ quản hệ thống thông tin chỉ đạo việc giám sát an toàn, an ninh thông tin mạng đối với các hệ thống thông tin thuộc phạm vi quản lý, phối hợp với Cục Chuyên đổi số và Thông tin dữ liệu tài nguyên môi trường và các đơn vị chức năng của Bộ Thông tin và Truyền thông giám sát theo quy định.

2. Các hệ thống thông tin bắt buộc phải có chức năng ghi và lưu trữ nhật ký về hoạt động của hệ thống và người sử dụng hệ thống thông tin. Thực hiện việc 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.

3. Nguyên tắc, yêu cầu, nội dung, phương thức, hệ thống kỹ thuật phục vụ công tác giám sát thực hiện theo quy định tại Thông tư số 31/2017/TT-BTTTT.

4. Đơn vị chuyên trách về an toàn thông tin của các đơn vị trực thuộc Bộ cử 01 lãnh đạo đơn vị và 01 cán bộ (hoặc 01 đơn vị trực thuộc) làm đầu mối giám sát an toàn, an ninh thông tin để tiếp nhận cảnh báo, cung cấp, trao đổi, chia sẻ thông tin với Cục Chuyên đổi số và Thông tin dữ liệu tài nguyên môi trường trong các hoạt động giám sát an toàn, an ninh thông tin tại đơn vị và tại Bộ Tài nguyên và Môi trường.

Điều 15. Kiểm tra, đánh giá an toàn, an ninh thông tin

1. Chủ quản hệ thống thông tin có thẩm quyền yêu cầu kiểm tra, đánh giá an toàn, an ninh thông tin đối với các hệ thống thông tin thuộc thẩm quyền quản lý. Đơn vị chuyên trách về an toàn, an ninh thông tin của chủ quản hệ thống thông tin

có thẩm quyền yêu cầu kiểm tra, đánh giá đối với các hệ thống thông tin do đơn vị này phê duyệt hồ sơ đề xuất cấp độ.

2. Đơn vị chủ trì kiểm tra, đánh giá là đơn vị được cấp có thẩm quyền giao nhiệm vụ hoặc được lựa chọn để thực hiện việc kiểm tra, đánh giá. Đối tượng kiểm tra, đánh giá là chủ quản hệ thống thông tin hoặc đơn vị vận hành hệ thống thông tin và các hệ thống thông tin có liên quan.

3. Nội dung, hình thức kiểm tra, đánh giá theo quy định tại Điều 11 và Điều 12 Thông tư số 12/2022/TT-BTTTT.

4. Cục Chuyển đổi số và Thông tin dữ liệu tài nguyên môi trường thực hiện việc kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ tại Bộ Tài nguyên và Môi trường theo quy định tại Điều 12 Thông tư số 12/2022/TT-BTTTT.

5. Cục Chuyển đổi số và Thông tin dữ liệu tài nguyên môi trường, đơn vị chuyên trách về an toàn thông tin của các đơn vị trực thuộc Bộ thực hiện việc đánh giá hiệu quả các biện pháp bảo đảm an toàn thông tin theo thẩm quyền. Nội dung đánh giá là cơ sở để điều chỉnh phương án bảo đảm an toàn thông tin cho phù hợp.

Điều 16. Ứng cứu sự cố an toàn thông tin mạng

1. Ban chỉ đạo, đơn vị chuyên trách ứng cứu khẩn cấp sự cố an toàn thông tin mạng

a) Ban chỉ đạo ứng dụng và phát triển công nghệ thông tin theo Quyết định số 674/QĐ-BTNMT ngày 31/3/2017 đảm nhiệm chức năng Ban chỉ đạo ứng cứu khẩn cấp sự cố an toàn thông tin mạng của Bộ Tài nguyên và Môi trường. Trách nhiệm và quyền hạn của Ban chỉ đạo ứng cứu khẩn cấp sự cố an toàn thông tin mạng của Bộ Tài nguyên và Môi trường được quy định tại khoản 2, Điều 5 Quyết định số 05/2017/QĐ-TTg.

b) Cục Chuyển đổi số và Thông tin dữ liệu tài nguyên môi trường là đơn vị chuyên trách về ứng cứu sự cố an toàn thông tin mạng của Bộ Tài nguyên và Môi trường. Bộ phận chuyên trách về an toàn thông tin mạng tại các đơn vị thuộc Bộ đảm nhiệm vai trò chuyên trách về ứng cứu sự cố an toàn thông tin mạng trong phạm vi quản lý công nghệ thông tin của đơn vị. Đơn vị chuyên trách về ứng cứu sự cố an toàn thông tin mạng thực hiện trách nhiệm quy định tại khoản 2 Điều 6 Quyết định số 05/2017/QĐ-TTg.

c) Cục Chuyển đổi số và Thông tin dữ liệu tài nguyên môi trường trình Bộ thành lập, cập nhật nhân sự của Đội ứng cứu an toàn thông tin mạng của Bộ và tổ chức, điều phối hoạt động ứng cứu sự cố trong phạm vi của Bộ quản lý. Các đơn vị chuyên trách về ứng cứu sự cố tại các đơn vị trực thuộc Bộ thành lập, cập nhật nhân sự Đội ứng cứu sự cố thuộc đơn vị.

2. Kế hoạch ứng phó sự cố bảo đảm an toàn thông tin mạng

a) Các đơn vị trực thuộc Bộ tổ chức xây dựng, phê duyệt kế hoạch ứng phó sự cố cho các hệ thống thông tin do đơn vị trực tiếp quản lý theo đề cương tại Phụ lục II Quyết định số 05/2017/QĐ-TTg (bao gồm các điều chỉnh do Bộ Thông tin và Truyền thông ban hành nếu có) và tổ chức triển khai kế hoạch sau khi phê duyệt. Đối với các nội dung trong kế hoạch vượt thẩm quyền quyết định của đơn vị, đơn vị lấy ý kiến của Cục Chuyển đổi số và Thông tin dữ liệu tài nguyên môi trường, Vụ Kế hoạch - Tài chính (đối với các nội dung yêu cầu có kinh phí), báo cáo Bộ xem xét, quyết định.

b) Các kế hoạch ứng phó sự cố sau khi được phê duyệt phải gửi Cục Chuyển đổi số và Thông tin dữ liệu tài nguyên môi trường tổng hợp thành kế hoạch chung của Bộ Tài nguyên và Môi trường. Cục Chuyển đổi số và Thông tin dữ liệu tài nguyên môi trường có trách nhiệm xây dựng kế hoạch ứng phó sự cố của Bộ Tài nguyên và Môi trường, trình Lãnh đạo Bộ phê duyệt.

c) Kế hoạch ứng phó sự cố được rà soát và điều chỉnh hàng năm (nếu cần thiết) trước ngày 31 tháng 10, làm cơ sở để xây dựng kế hoạch bảo đảm an toàn thông tin năm tiếp theo.

3. Quy trình ứng cứu sự cố an toàn thông tin mạng

a) Các tổ chức, cá nhân khi phát hiện dấu hiệu tấn công hoặc sự cố an toàn thông tin mạng cần nhanh chóng báo cho đơn vị vận hành hệ thống thông tin, cơ quan chủ quản hệ thống thông tin liên quan và Cục Chuyển đổi số và Thông tin dữ liệu tài nguyên môi trường. Cục Chuyển đổi số và Thông tin dữ liệu tài nguyên môi trường có trách nhiệm cập nhật, công khai thông tin liên lạc, đường dây nóng của các đơn vị/bộ phận tiếp nhận thông tin sự cố của Bộ và của các đơn vị trực thuộc Bộ trên Cổng thông tin điện tử của Bộ Tài nguyên và Môi trường.

b) Khi xảy ra sự cố an toàn thông tin mạng thuộc loại hình tấn công mạng, đơn vị vận hành hệ thống thông tin thực hiện báo cáo theo quy định tại Điểm a khoản 1 Điều 11 Quyết định 05/2017/QĐ-TTg và Điều 9 Thông tư 20/2017/TT-BTTTT, đồng thời báo cáo Cục Chuyển đổi số và Thông tin dữ liệu tài nguyên môi trường để tổng hợp, báo cáo Ban Chỉ đạo ứng cứu khẩn cấp sự cố an toàn thông tin mạng Bộ Tài nguyên và Môi trường. Trách nhiệm của các đơn vị khi phát hiện, tiếp nhận xác minh, xử lý ban đầu và phân loại sự cố an toàn thông tin mạng theo quy định tại Điều 12 Quyết định 05/2017/QĐ-TTg và Điều 10 Thông tư số 20/2017/TT-BTTTT.

c) Quy trình ứng cứu sự cố an toàn thông tin mạng theo quy định tại Điều 13, Điều 14 Quyết định 05/2017/QĐ-TTg và Điều 11 Thông tư số 20/2017/TT-BTTTT.

4. Diễn tập ứng cứu sự cố an toàn thông tin mạng

a) Chủ quản hệ thống thông tin tổ chức diễn tập ứng cứu sự cố theo kế hoạch ứng phó sự cố được phê duyệt.

b) Cục Chuyển đổi số và Thông tin dữ liệu tài nguyên môi trường chủ trì, phối hợp với các đơn vị thuộc Bộ tham gia các cuộc diễn tập quốc gia, quốc tế do Cơ quan điều phối quốc gia, Bộ Thông tin và Truyền thông tổ chức và tổ chức diễn tập

ứng cứu sự cố trong phạm vi Bộ Tài nguyên và Môi trường theo tần suất quy định tại điểm b Nhiệm vụ 4 mục II Điều 1 Quyết định số 1622/QĐ-TTg ngày 25/10/2017 của Thủ tướng Chính phủ.

Chương III

TRÁCH NHIỆM CỦA CÁC TỔ CHỨC LIÊN QUAN

Điều 17. Trách nhiệm của các đơn vị thuộc Bộ

1. Thực hiện các trách nhiệm được giao tại Quy chế này.
2. Tổ chức triển khai thực hiện Quy chế này tại đơn vị.
3. Xây dựng, triển khai Quy chế bảo đảm an toàn, an ninh thông tin tại đơn vị bảo đảm phù hợp với Quy chế này và các yêu cầu cụ thể của đơn vị.
4. Thực hiện việc quản lý trang thiết bị công nghệ thông tin và cán bộ, công chức, viên chức, người lao động theo Điều 10, Điều 11 và Điều 12 của Quy chế này.
5. Thường xuyên tổ chức các hoạt động tuyên truyền, phổ biến nâng cao nhận thức về bảo đảm an toàn, an ninh thông tin; nhận diện, cảnh giác, phòng ngừa và ngăn chặn các hoạt động vi phạm pháp luật trên không gian mạng đến toàn thể cán bộ, công chức, viên chức và người lao động tại đơn vị.
6. Đối với các Vụ thuộc Bộ: Phối hợp với Cục Chuyển đổi số và Thông tin dữ liệu tài nguyên môi trường bảo đảm an toàn, an ninh thông tin cho các hệ thống thông tin, cơ sở dữ liệu dùng chung của Bộ và các hệ thống thông tin do đơn vị quản lý, vận hành.

Điều 18. Trách nhiệm của Cục Chuyển đổi số và Thông tin dữ liệu tài nguyên môi trường

1. Thực hiện trách nhiệm của đơn vị chuyên trách về an toàn thông tin theo quy định tại Điều 21 Nghị định 85/2016/NĐ-CP, Quy chế này và các nhiệm vụ do chủ quản hệ thống thông tin phân công.
2. Hướng dẫn triển khai Quy chế này và các quy định liên quan của Nhà nước.
3. Xây dựng kế hoạch, báo cáo về an toàn thông tin mạng của Bộ Tài nguyên và Môi trường.
4. Theo dõi, đôn đốc, giám sát, kiểm tra và báo cáo Bộ việc thực hiện Quy chế này tại các đơn vị thuộc Bộ.
5. Thường xuyên tổ chức các hoạt động tuyên truyền, phổ biến nâng cao nhận thức về an toàn, an ninh thông tin mạng; nhận diện, cảnh giác, phòng ngừa và ngăn chặn các hoạt động vi phạm pháp luật trên không gian mạng tại Bộ lồng ghép trong các chương trình hội nghị, tập huấn, hội thảo về ứng dụng công nghệ thông tin và chuyển đổi số của ngành tài nguyên và môi trường.
6. Bảo đảm an toàn, an ninh thông tin cho các hệ thống thông tin, cơ sở dữ liệu dùng chung, trọng yếu của Bộ.

Điều 19. Trách nhiệm của Vụ Tổ chức cán bộ

Căn cứ nhu cầu về đào tạo nguồn nhân lực bảo đảm an toàn thông tin của các đơn vị trực thuộc Bộ, phối hợp với Cục Chuyên đổi số và Thông tin dữ liệu tài nguyên môi trường xây dựng trình Bộ phê duyệt kế hoạch dài hạn, kế hoạch hàng năm về đào tạo, bồi dưỡng nghiệp vụ an toàn, an ninh thông tin cho cán bộ, công chức, viên chức và người lao động của Bộ và thực hiện tổ chức đào tạo theo kế hoạch đã phê duyệt.

Điều 20. Trách nhiệm của chủ quản hệ thống thông tin

1. Thực hiện trách nhiệm của đơn vị chủ quản hệ thống thông tin theo quy định tại Điều 20 Nghị định 85/2016/NĐ-CP và Quy chế này.

2. Chỉ đạo, phân công các đơn vị vận hành các hệ thống thông tin triển khai công tác bảo đảm an toàn thông tin trong tất cả các công đoạn liên quan đến hệ thống thông tin.

Điều 21. Trách nhiệm của đơn vị vận hành hệ thống thông tin

1. Thực hiện trách nhiệm của đơn vị vận hành hệ thống thông tin theo quy định tại Điều 22 Nghị định 85/2016/NĐ-CP, Quy chế này và các nhiệm vụ do chủ quản hệ thống thông tin phân công.

2. Chỉ đạo, phân công các bộ phận kỹ thuật thuộc đơn vị (quản lý ứng dụng; quản lý dữ liệu; vận hành hệ thống thông tin; triển khai và hỗ trợ kỹ thuật) triển khai công tác bảo đảm an toàn thông tin trong tất cả các công đoạn liên quan đến hệ thống thông tin.

Điều 22. Trách nhiệm cá nhân

1. Thủ trưởng đơn vị thuộc đối tượng áp dụng của Quy chế này có trách nhiệm: phổ biến tới từng cán bộ, công chức, viên chức, người lao động của đơn vị; thường xuyên kiểm tra việc thực hiện Quy chế này tại đơn vị; chịu trách nhiệm trước pháp luật và Lãnh đạo Bộ Tài nguyên và Môi trường về các vi phạm, thất thoát thông tin, dữ liệu mật thuộc phạm vi quản lý của đơn vị do không tổ chức, chỉ đạo, kiểm tra cán bộ của đơn vị thực hiện đúng quy định.

2. Cán bộ, công chức, viên chức, người lao động của Bộ Tài nguyên và Môi trường, các đơn vị trực thuộc Bộ và các đơn vị khác thuộc đối tượng áp dụng của Quy chế có trách nhiệm: tuân thủ Quy chế; thông báo các dấu hiệu mất an toàn thông tin cho đơn vị, bộ phận chuyên trách về an toàn thông tin mạng của đơn vị; chịu trách nhiệm trước pháp luật và Lãnh đạo đơn vị về các vi phạm, thất thoát dữ liệu quan trọng hoặc dữ liệu mật của ngành tài nguyên và môi trường do không tuân thủ Quy chế.

Chương IV

TỔ CHỨC THỰC HIỆN

Điều 23. Kinh phí thực hiện

Kinh phí bảo đảm an toàn, an ninh thông tin mạng được lấy từ nguồn ngân sách nhà nước dự toán hàng năm của Bộ Tài nguyên và Môi trường theo quy định.

Căn cứ vào kế hoạch hàng năm, các đơn vị liên quan có trách nhiệm xây dựng kế hoạch, đề xuất dự toán cho các hoạt động bảo đảm an toàn, an ninh thông tin mạng gửi Cục Chuyên đổi số và Thông tin dữ liệu tài nguyên môi trường để tổng hợp, gửi Vụ Kế hoạch - Tài chính thẩm định, trình Bộ phê duyệt.

Điều 24. Công tác kiểm tra

1. Các đơn vị trực thuộc Bộ phải thường xuyên kiểm tra, theo dõi và đánh giá công tác bảo đảm an toàn, an ninh thông tin mạng tại cơ quan, đơn vị mình, coi đây là nhiệm vụ trọng tâm của đơn vị.

2. Giao Cục Chuyên đổi số và Thông tin dữ liệu tài nguyên môi trường kiểm tra và báo cáo Bộ việc thực hiện Quy chế này tại các đơn vị trực thuộc Bộ.

Điều 25. Chế độ báo cáo

1. Báo cáo định kỳ:

a) Báo cáo an toàn thông tin định kỳ hàng năm trước ngày 15 tháng 11 gồm các nội dung quy định tại Điều 13, Điều 14 Thông tư 12/2022/TT-BTTTT.

b) Báo cáo hoạt động giám sát của chủ quản hệ thống thông tin định kỳ 6 tháng trước ngày 15 tháng 6 và 15 tháng 12 hàng năm theo mẫu tại Phụ lục 2 Thông tư 31/2017/TT-BTTTT.

2. Báo cáo đột xuất: Báo cáo về công tác khắc phục mã độc, lỗ hổng, điểm yếu, triển khai cảnh báo an toàn thông tin và các báo cáo đột xuất khác theo yêu cầu của các cơ quan quản lý nhà nước về an toàn thông tin.

3. Trách nhiệm lập, phê duyệt báo cáo

a) Các đơn vị trực thuộc Bộ có trách nhiệm lập báo cáo định kỳ, báo cáo đột xuất theo yêu cầu theo nội dung quy định tại khoản 1 Điều này gửi Cục Chuyên đổi số và Thông tin dữ liệu tài nguyên môi trường.

b) Cục Chuyên đổi số và Thông tin dữ liệu tài nguyên môi trường chịu trách nhiệm tập hợp, tổng hợp báo cáo của các đơn vị, trình Bộ phê duyệt, gửi các cơ quan quản lý nhà nước về an toàn thông tin.

Điều 26. Khen thưởng, kỷ luật

1. Kết quả thực hiện Quy chế này là một trong những tiêu chí đánh giá kết quả thực hiện hàng năm của cá nhân, đơn vị đồng thời là tiêu chí bắt buộc để xem xét tình hình khen thưởng và danh hiệu thi đua đối với các tổ chức, cá nhân.

2. Đơn vị, cá nhân vi phạm Quy chế này và các quy định khác của pháp luật về bảo đảm an toàn, an ninh thông tin mạng, tùy theo tính chất, mức độ vi phạm sẽ

bị xử lý kỷ luật hoặc các hình thức xử lý khác theo quy định của pháp luật; nếu vi phạm gây thiệt hại đến tài sản, thiết bị, thông tin, dữ liệu thì chịu trách nhiệm bồi thường theo pháp luật hiện hành.

Điều 27. Trách nhiệm thi hành

1. Thủ trưởng các đơn vị trực thuộc Bộ có trách nhiệm phổ biến, quán triệt đến toàn bộ cán bộ, nhân viên trong đơn vị thực hiện các quy định của Quy chế này.

2. Trong quá trình thực hiện, nếu có những vấn đề khó khăn, vướng mắc, các đơn vị phản ánh về Cục Chuyển đổi số và Thông tin dữ liệu tài nguyên môi trường để tổng hợp, trình Bộ trưởng xem xét, sửa đổi, bổ sung Quy chế./.