BỘ VĂN HÓA, THỂ THAO VÀ DU LỊCH

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

QUY CHẾ
Bảo đảm an toàn, an ninh thông tin mạng của Bộ Văn hóa, Thể thao và Du lịch

(Kèm theo Quyết định số /QĐ-BVHTTDL ngày tháng năm 2023 của Bộ trưởng Bộ Văn hóa, Thể thao và Du lịch)

Chương I
QUY ĐỊNH CHUNG

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

1. Quy chế này quy định về công tác bảo đảm an toàn, an ninh thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của Bộ Văn hóa, Thể thao và Du lịch.

2. Quy chế này áp dụng đối với các cơ quan hành chính, đơn vị sự nghiệp thuộc Bộ Văn hóa, Thể thao và Du lịch (theo Nghị định số 01/2023/NĐ-CP ngày 16/01/2023 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Văn hóa, Thể thao và Du lịch và Quyết định số 527/QĐ-TTg ngày 15/5/2018 của Thủ tướng Chính phủ về việc ban hành danh sách các đơn vị sự nghiệp công lập trực thuộc Bộ Văn hóa, Thể thao và Du lịch).

Điều 2. Giải thích từ ngữ

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

1. *An toàn thông tin mạng* là sự bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

2. *An ninh mạng* là sự bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

3. *An ninh thông tin* 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.

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

5. *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.

6. *Thiết bị xử lý thông tin* là thiết bị dùng để tạo lập, xử lý, lưu trữ, truyền đưa thông tin dưới dạng điện tử (máy tính, máy in, điện thoại thông minh, thiết bị mạng, thiết bị an ninh mạng, camera giám sát và các thiết bị tương tự khác).

7. *Thiết bị mạng* là các thiết bị phần cứng công nghệ thông tin đóng vai trò xử lý một công việc nhất định trong mạng máy tính; Các thiết bị mạng phổ biến như: tường lửa (firewall), định tuyến (router), điểm truy cập không dây (access point), thiết bị cầu nối (bridge), bộ lặp (repeater), chuyển mạch (switch), bộ chuyển đổi mạng hoặc ứng dụng…

8. *Người dùng* là cán bộ, công chức, viên chức và người lao động tham gia vào hoạt động ứng dụng công nghệ thông tin phục vụ công việc của Bộ Văn hóa, Thể thao và Du lịch.

9. *Tường lửa* là một thiết bị phần cứng hoặc một phần mềm hoạt động trong một môi trường máy tính nối mạng nhằm ngăn chặn (hoặc cho phép nhưng kiểm soát được) những lưu lượng bị cấm (hoặc cho phép) bởi chính sách an ninh của một cá nhân hay một tổ chức.

10. *Thiết bị lưu trữ* là thiết bị được sử dụng để đọc, ghi dữ liệu. Căn cứ tính năng lưu trữ, thiết bị lưu trữ gồm: thiết bị lưu trữ chuyên dụng cho máy chủ (DAS, NAS, SAN, iSCSI SAN...) và thiết bị lưu trữ phổ thông (ổ cứng HHD/SSD, USB flash, thẻ nhớ, đĩa từ...).

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

12. *Phần mềm độc hại* 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.

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

1. Hoạt động an toàn, an ninh thông tin mạng của các cơ quan, đơn vị thuộc Bộ đúng quy định của pháp luật. Tuân thủ quy định của pháp luật về an toàn thông tin mạng, an ninh mạng; bảo vệ bí mật nhà nước, bí mật công tác, dữ liệu cá nhân; giao dịch điện tử và các quy định khác có liên quan. 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.

2. Cơ quan, đơn vị được Bộ giao nhiệm vụ là đầu mối xử lý sự cố về an toàn, an ninh thông tin mạng có trách nhiệm hướng dẫn, xử lý, phối hợp xử lý sự cố an toàn thông tin mạng tại các cơ quan, đơn vị thuộc Bộ trong phạm vi được phân công.

3. An toàn, an ninh thông tin mạng phải gắn liền và hỗ trợ các hoạt động ứng dụng công nghệ thông tin, giao dịch điện tử, chuyển đổi số của Bộ Văn hóa, Thể thao và Du lịch; hỗ trợ việc sử dụng thiết bị xử lý thông tin để xử lý công

việc của cán bộ, công chức, viên chức, người lao động thuộc Bộ Văn hóa, Thể thao và Du lịch.

4. Ứng cứu sự cố an toàn, an ninh mạng là hoạt động quan trọng nhằm phát hiện, ngăn chặn, xử lý và khắc phục kịp thời sự cố an toàn, an ninh mạng.

5. Mỗi cán bộ, công chức, viên chức, người lao động tại các cơ quan, đơn vị thuộc Bộ Văn hóa, Thể thao và Du lịch nêu cao tinh thần chủ động, tự giác trong việc áp dụng các biện pháp an toàn, an ninh mạng.

Điều 4. Các hành vi bị nghiêm cấm

1. Ngăn chặn việc truyền tải thông tin trên mạng, can thiệp, truy nhập, gây nguy hại, xóa, thay đổi, sao chép và làm sai lệch thông tin trên mạng trái pháp luật.

2. 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.

3. Tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng của biện pháp bảo vệ an toàn thông tin mạng của hệ thống thông tin; tấn công, chiếm quyền điều khiển, phá hoại hệ thống thông tin.

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. Xâm nhập trái pháp luật bí mật, mật mã và thông tin đã mã hóa hợp pháp của cơ quan, tổ chức, cá nhân; tiết lộ thông tin về sản phẩm mật mã dân sự, thông tin về khách hàng sử dụng hợp pháp sản phẩm mật mã dân sự; sử dụng, kinh doanh các sản phẩm mật mã dân sự không rõ nguồn gốc.

Chương II

VAI TRÒ CỦA CƠ QUAN, ĐƠN VỊ VỀ BẢO ĐẢM AN TOÀN, AN NINH THÔNG TIN MẠNG

Điều 5. Phân công thực hiện các vai trò về bảo đảm an toàn, an ninh thông tin mạng theo quy định của pháp luật

1. Chủ quản hệ thống thông tin.

Bộ Văn hóa, Thể thao và Du lịch (Bộ) là chủ quản của hệ thống thông tin được xây dựng, thiết lập, nâng cấp, mở rộng từ dự án hoặc kế hoạch thuê dịch vụ thuộc thẩm quyền phê duyệt của Bộ trưởng Bộ Văn hóa, Thể thao và Du lịch; chủ quản của hệ thống thông tin được xây dựng, thiết lập, nâng cấp, mở rộng từ dự án, kế hoạch thuê dịch vụ, đề cương và dự toán chi tiết thuộc thẩm quyền phê duyệt của các cơ quan, đơn vị thuộc Bộ.

2. Đơn vị vận hành hệ thống thông tin.

a) Chủ trì xây dựng, thiết lập, nâng cấp, mở rộng, bảo trì, bảo dưỡng, duy trì hoạt động của hệ thống thông tin thực hiện vai trò đơn vị vận hành hệ thống thông tin. Trung tâm Công nghệ thông tin là đơn vị vận hành hệ thống an toàn, an ninh mạng của Bộ và các hệ thống thông tin dùng chung khác theo quyết định của Bộ trưởng Bộ Văn hóa, Thể thao và Du lịch.

b) Trường hợp hệ thống thông tin đang trong thời gian thuê dịch vụ công nghệ thông tin, đơn vị cung cấp dịch vụ thực hiện vai trò đơn vị vận hành hệ thống thông tin.

3. Đơn vị chuyên trách an toàn, an ninh mạng.

a) Trung tâm Công nghệ thông tin đảm nhiệm vai trò đơn vị chuyên trách an toàn, an ninh mạng của Bộ Văn hóa, Thể thao và Du lịch.

b) Chủ quản hệ thống thông tin thành lập hoặc chỉ định bộ phận chuyên trách an toàn, an ninh mạng thuộc đơn vị của chủ quản hệ thống thông tin.

4. Đơn vị chuyên trách về ứng cứu sự cố an toàn, an ninh mạng (gọi tắt là Đơn vị chuyên trách ứng cứu sự cố).

a) Trung tâm Công nghệ thông tin đảm nhiệm vai trò đơn vị chuyên trách ứng cứu sự cố của Bộ Văn hóa, Thể thao và Du lịch, chịu trách nhiệm triển khai công tác ứng cứu sự cố các hệ thống thông tin do Bộ Văn hóa, Thể thao và Du lịch làm chủ quản (không bao gồm các hệ thống thông tin mà Bộ đã ủy quyền thực hiện trách nhiệm của chủ quản hệ thống thông tin).

b) Đơn vị chuyên trách ứng cứu sự cố trình chủ quản hệ thống thông tin thành lập Đội ứng cứu sự cố và tổ chức hoạt động ứng cứu sự cố trong lĩnh vực, địa bàn, phạm vi mình quản lý.

c) Các đơn vị thuộc Bộ phải cử ít nhất 01 nhân sự làm thành viên tham gia Đội ứng cứu sự cố, thành viên đội ứng cứu sự cố đảm nhiệm vai trò ứng cứu sự cố và phối hợp đơn vị chuyên trách ứng cứu sự cố và các thành viên trong Đội ứng cứu triển khai ứng cứu sự cố của đơn vị.

5. Lực lượng bảo vệ an ninh mạng Bộ Văn hóa, Thể thao và Du lịch bao gồm bộ phận chuyên trách an toàn, an ninh mạng thuộc Trung tâm Công nghệ thông tin và các thành viên mạng lưới ứng cứu sự cố tại Quyết định số 3623/QĐ-BVHTTDL ngày 23/12/2022 của Bộ trưởng Bộ Văn hóa, Thể thao và Du lịch về việc thành lập Đội Ứng cứu sự cố an toàn, thông tin mạng của Bộ Văn hóa, Thể thao và Du lịch.

6. Đơn vị, bộ phận được phân công đảm nhiệm vai trò bảo đảm an toàn, an ninh mạng tại điểm 1 đến điểm 5 Điều này thực hiện trách nhiệm theo quy định của pháp luật áp dụng cho vai trò tương ứng và theo quy định tại Quy chế này.

Điều 6. Bảo đảm an toàn, an ninh thông tin mạng đối với hệ thống thông tin, thiết bị xử lý thông tin

1. Chủ quản hệ thống thông tin, đơn vị vận hành hệ thống thông tin, đơn vị chuyên trách an toàn, an ninh mạng thực hiện các nhiệm vụ sau.

a) Xác định cấp độ an toàn của hệ thống thông tin (lập hồ sơ đề xuất cấp độ; tổ chức thẩm định, phê duyệt hồ sơ đề xuất cấp độ) và triển khai phương án bảo đảm an toàn hệ thống thông tin theo cấp độ theo quy định từ Điều 13 đến Điều 19 của Nghị định số 85/2016/NĐ-CP; từ Điều 7 đến Điều 10 của Thông tư số 12/2022/TT-BTTTT và khoản 1 Điều 7 của Quy chế này. Việc xác định hệ thống thông tin, bao gồm hệ thống thông tin sử dụng camera giám sát, để xác định cấp độ căn cứ trên nguyên tắc được quy định tại khoản 1 Điều 5 Nghị định số 85/2016/NĐ-CP, Điều 7 Thông tư số 12/2022/TT-BTTTT và các hướng dẫn bổ sung của Bộ Thông tin và Truyền thông (nếu có).

b) Bảo đảm an ninh mạng cho hệ thống thông tin quan trọng về an ninh quốc gia theo quy định từ Điều 12 đến Điều 15 của Luật An ninh mạng, Điều 7 đến Điều 17 của Nghị định số 53/2022/NĐ-CP.

2. Đơn vị không thuộc phạm vi khoản 1 Điều này và có thẩm quyền tự trang bị thiết bị xử lý thông tin sử dụng tại đơn vị có trách nhiệm.

a) Bảo đảm an toàn, an ninh mạng cho máy tính của người sử dụng thuộc đơn vị: sử dụng hệ điều hành được hỗ trợ bản vá lỗ hổng bảo mật; chỉ cài đặt tiện ích thiết yếu được cung cấp kèm theo hệ điều hành và các phần mềm phục vụ công việc, có bản quyền hoặc được các cơ quan chức năng đánh giá, xác nhận an toàn; cài đặt phần mềm phòng, diệt mã độc và cập nhật thường xuyên mẫu nhận diện mã độc.

b) Bảo đảm an toàn, an ninh mạng cho thiết bị mạng, thiết bị an ninh mạng sử dụng tại đơn vị: không sử dụng thiết bị không còn được hỗ trợ khắc phục lỗ hổng bảo mật; thực hiện khắc phục lỗ hổng bảo mật ngay khi nhận được cảnh báo, hướng dẫn từ cơ quan chức năng; thay đổi mật khẩu mặc định và giữ bí mật mật khẩu quản trị thiết bị.

3. Đơn vị mua sắm, sử dụng camera giám sát phải tuân thủ quy chuẩn kỹ thuật quốc gia về an toàn thông tin mạng cơ bản cho camera giám sát, theo Chỉ thị số 23/CT-TTg ngày 26/12/2022 của Thủ tướng Chính phủ về tăng cường công tác bảo đảm an toàn thông tin mạng, an ninh thông tin cho thiết bị camera giám sát.

Điều 7. Giám sát an toàn, an ninh mạng

1. Đơn vị chuyên trách an toàn, an ninh mạng tự thực hiện giám sát nếu có đủ năng lực hoặc lựa chọn tổ chức, doanh nghiệp có đủ năng lực thực hiện giám sát an toàn hệ thống thông tin theo quy định tại Điều 5 Thông tư số 31/2017/TT-BTTTT và hướng dẫn của Bộ Thông tin và Truyền thông.

2. Đơn vị chuyên trách an toàn, an ninh mạng thiết lập hệ thống tiếp nhận thông tin giám sát từ các đơn vị thuộc Bộ Văn hóa, Thể thao và Du lịch và

hướng dẫn các đơn vị thuộc Bộ kết nối, chia sẻ thông tin về Bộ Văn hóa, Thể thao và Du lịch; làm đầu mối thực hiện kết nối, chia sẻ thông tin giám sát từ các đơn vị của Bộ với Trung tâm giám sát không gian mạng quốc gia thuộc Cục An toàn thông tin, Bộ Thông tin và Truyền thông. Nội dung thông tin giám sát cần kết nối, chia sẻ theo hướng dẫn của Bộ Thông tin và Truyền thông.

3. Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia phối hợp với Cục An ninh mạng và phòng chống tội phạm công nghệ cao của Bộ Công an triển khai giám sát an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia theo quy định tại khoản 3 Điều 15 Nghị định số 53/2022/NĐ-CP.

Điều 8. Kiểm tra, đánh giá an toàn an ninh mạng

1. Về kiểm tra, đánh giá việc tuân thủ quy định của pháp luật về an toàn, an ninh mạng; kiểm tra, đánh giá hiệu quả của các biện pháp bảo đảm an toàn thông tin theo phương án bảo đảm an toàn thông tin được phê duyệt.

a) Đơn vị chuyên trách an toàn, an ninh mạng thực hiện kiểm tra, đánh giá các đơn vị thuộc Bộ trong chương trình, kế hoạch kiểm tra công tác ứng dụng công nghệ thông tin hàng năm hoặc chương trình kiểm tra theo chuyên đề về an toàn, an ninh mạng được Bộ trưởng Bộ Văn hóa, Thể thao và Du lịch phê duyệt.

b) Các đơn vị thuộc Bộ tự kiểm tra, đánh giá hàng năm trong nội bộ đơn vị, trong phạm vi trách nhiệm của đơn vị đối với công tác an toàn, an ninh mạng theo quy định của pháp luật và quy định tại Quy chế này.

2. Chủ quản hệ thống thông tin (hoặc đơn vị chuyên trách an toàn, an ninh mạng của chủ quản hệ thống thông tin) lựa chọn tổ chức, doanh nghiệp có chức năng hoặc được cấp phép thực hiện kiểm tra, đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống thông tin, theo quy định tại điểm c khoản 2 Điều 20 Nghị định số 85/2016/NĐ-CP và khoản 3 Điều 11, khoản 3 Điều 12 Thông tư số 12/2022/TT-BTTTT; kiểm tra, đánh giá an ninh mạng theo quy định tại điểm c khoản 2 Điều 24 Nghị định số 53/2022/NĐ-CP và theo hướng dẫn của Bộ Công an. Tổ chức, doanh nghiệp cung cấp dịch vụ kiểm tra, đánh giá an toàn, an ninh mạng phải độc lập với tổ chức, doanh nghiệp cung cấp dịch vụ giám sát an toàn, an ninh mạng cho đơn vị.

Điều 9. Ứng phó sự cố an toàn, an ninh mạng

1. Đơn vị chuyên trách và các đơn vị, đầu mối liên quan thực hiện ứng phó sự cố an toàn thông tin mạng theo Quy chế hoạt động của Đội ứng cứu sự cố an toàn thông tin mạng của Bộ Văn hóa, Thể thao và Du lịch. Đối với nội dung (ứng phó sự cố bảo đảm an toàn thông tin mạng; phương án ứng phó, khắc phục sự cố an ninh mạng) vượt thẩm quyền quyết định của đơn vị, đơn vị lấy ý kiến của các đơn vị liên quan, báo cáo Lãnh đạo Bộ Văn hóa, Thể thao và Du lịch xem xét, quyết định.

2. Đối với hệ thống thông tin không phải hệ thống thông tin quan trọng về an ninh quốc gia, áp dụng quy trình ứng cứu sự cố thông thường theo quy định tại Điều 11 Thông tư số 20/2017/TT-BTTTT; áp dụng quy trình ứng cứu sự cố nghiêm trọng theo quy định tại Điều 14 Quyết định số 05/2017/QĐ-TTg. Đối với hệ thống thông tin quan trọng về an ninh quốc gia, áp dụng trình tự, thủ tục ứng phó, khắc phục sự cố an ninh mạng theo quy định tại Điều 17 của Nghị định số 53/2022/NĐ-CP.

3. Đơn vị chuyên trách an toàn, an ninh mạng có trách nhiệm theo dõi, nắm bắt thông tin trên phương tiện thông tin đại chúng và mạng Internet về các sự kiện mất an toàn an ninh mạng có thể tác động tới đơn vị; chủ động kiểm tra, rà soát trong nội bộ đơn vị theo các văn bản cảnh báo, hướng dẫn của các cơ quan chức năng và các tổ chức về an toàn thông tin (gửi trực tiếp cho đơn vị hoặc do Văn phòng Bộ, Đơn vị chuyên trách an toàn, an ninh mạng sao gửi chủ quản hệ thống thông tin); Thiết lập kênh trao đổi thông tin với các đối tác cung cấp thiết bị, phần mềm, giải pháp an toàn thông tin của đơn vị để nắm bắt kịp thời vấn đề, sự cố có khả năng tác động tới hệ thống thông tin của đơn vị.

4. Cán bộ tham gia đội ứng cứu sự cố của các đơn vị thuộc Bộ là đầu mối tiếp nhận cảnh báo an toàn thông tin từ đơn vị chuyên trách an toàn, an ninh mạng, các cơ quan, tổ chức có chức năng cảnh báo an toàn thông tin mạng, an ninh mạng (thông qua thư điện tử hoặc các kênh trao đổi thông tin khác).

5. 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 Điều 11 Quyết định số 05/2017/QĐ-TTg và Điều 9 Thông tư số 20/2017/TT-BTTTT, đồng thời gửi báo cáo cho đơn vị chuyên trách an toàn, an ninh mạng để tổng hợp, báo cáo Lãnh đạo Bộ. Chủ quản hệ thống thông tin phải thông báo rộng rãi về đầu mối tiếp nhận thông tin để các cá nhân, tổ chức thuộc đơn vị liên lạc trong trường hợp: nghi ngờ, phát hiện dấu hiệu tấn công, sự cố an toàn thông tin mạng; dấu hiệu, hành vi khủng bố mạng; tình huống nguy hiểm về an ninh mạng; hành vi vi phạm pháp luật về an ninh mạng liên quan đến các hệ thống thông tin do đơn vị quản lý.

6. Định kỳ hàng năm, đơn vị chuyên trách an toàn, an ninh mạng chủ trì tổ chức diễn tập thực chiến an toàn an ninh mạng cho các đơn vị thuộc Bộ Văn hóa, Thể thao và Du lịch, theo kế hoạch ứng phó sự cố bảo đảm an toàn thông tin mạng và phương án ứng phó, khắc phục sự cố an ninh mạng được phê duyệt, trong phạm vi các hệ thống thông tin do Bộ Văn hóa, Thể thao và Du lịch làm chủ quản. Đơn vị là thành viên mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia tham gia đầy đủ các cuộc diễn tập quốc gia, quốc tế do Cơ quan điều phối quốc gia và các cơ quan chức năng thuộc Bộ Thông tin và Truyền thông, Bộ Công an, Bộ Quốc phòng tổ chức.

Điều 10. Phổ biến, tuyên truyền, đào tạo, bồi dưỡng về an toàn, an ninh mạng

1. Đơn vị chuyên trách an toàn, an ninh mạng với Văn phòng Bộ và các đơn vị liên quan lập kế hoạch và triển khai công tác tuyên truyền, phổ biến chủ trương, chính sách, pháp luật, biện pháp an toàn an ninh mạng, thông qua các hình thức: văn bản hướng dẫn; hội nghị, hội thảo; đăng bài trên Cổng thông tin điện tử Bộ Văn hóa, Thể thao và Du lịch, báo, tạp chí…; gửi thư điện tử và các hình thức khác phù hợp với quy định của pháp luật. Các đơn vị thuộc Bộ có trách nhiệm thực hiện quán triệt, tuyên truyền, phổ biến, nâng cao nhận thức, trách nhiệm về an toàn an ninh mạng cho cán bộ, công chức, viên chức, người lao động thuộc đơn vị.

2. Đơn vị chuyên trách an toàn, an ninh mạng tổ chức đào tạo, bồi dưỡng theo các chương trình đào tạo ngắn hạn nâng cao kiến thức, kỹ năng về an toàn an ninh mạng cho công chức, viên chức chuyên trách về công nghệ thông tin, an toàn an ninh mạng và tổ chức bồi dưỡng kiến thức cơ bản, kỹ năng về an toàn an ninh mạng cho cán bộ quản lý, nghiệp vụ cho đơn vị thuộc Bộ.

Điều 11. Báo cáo an toàn, an ninh mạng

1. Đối với báo cáo năm về an toàn thông tin mạng, chủ quản hệ thống thông tin lập báo cáo theo quy định tại khoản 3 Điều 13 và Điều 14 Thông tư số 12/2022/TT-BTTTT gửi đơn vị chuyên trách an toàn, an ninh mạng trước ngày 20 tháng 12 hàng năm. Đơn vị chuyên trách an toàn, an ninh mạng tổng hợp, xây dựng Báo cáo an toàn thông tin định kỳ hàng năm của Bộ Văn hóa, Thể thao và Du lịch, trình Lãnh đạo Bộ phê duyệt, gửi Bộ Thông tin và Truyền thông trước ngày 25 tháng 12 hàng năm.

2. Đơn vị chuyên trách an toàn, an ninh mạng lập Báo cáo hoạt động giám sát an toàn thông tin mạng của Bộ Văn hóa, Thể thao và Du lịch định kỳ 6 tháng theo quy định tại điểm k khoản 3 Điều 5 Thông tư số 31/2017/TT-BTTTT, trình Lãnh đạo Bộ phê duyệt, gửi Bộ Thông tin và Truyền thông.

3. Đơn vị chuyên trách an toàn, an ninh mạng chủ trì, phối hợp với các chủ quản hệ thống thông tin thuộc Bộ Văn hóa, Thể thao và Du lịch xây dựng các báo cáo đột xuất về an toàn, an ninh mạng theo yêu cầu của Bộ Thông tin và Truyền thông, Bộ Công an, Bộ Quốc phòng, trình Lãnh đạo Bộ Văn hóa, Thể thao và Du lịch phê duyệt.

Chương III

QUY ĐỊNH VỀ AN TOÀN, AN NINH MẠNG

Điều 12. Quy định về bảo đảm an toàn tài khoản thông tin

1. Tài khoản thông tin (gọi tắt là tài khoản) là tập hợp gồm tên đăng nhập và mật khẩu hoặc/và hình thức xác thực khác, được gắn với quyền truy cập thực

hiện một số tác vụ trên hệ thống thông tin hoặc trên thiết bị xử lý thông tin thuộc Bộ Văn hóa, Thể thao và Du lịch; bao gồm các loại sau.

a) Tài khoản định danh: Mỗi tài khoản định danh chỉ cấp cho một người dùng duy nhất và được gắn quyền truy cập các hệ thống thông tin mà người dùng đó được sử dụng.

b) Tài khoản truy cập hệ thống gắn với một nhiệm vụ cụ thể, được gắn với quyền truy cập thực hiện các tác vụ cần thiết cho nhiệm vụ đó (ví dụ: tài khoản hệ thống văn bản, tài khoản hệ thống thư điện tử công vụ,...).

c) Tài khoản quản trị gắn với quyền cài đặt, cấu hình các thông số và cấp quyền truy cập trên hệ thống thông tin; gồm: quản trị nội dung, quản trị ứng dụng, quản trị cơ sở dữ liệu, quản trị hệ điều hành, quản trị thiết bị.

2. Đơn vị chuyên trách an toàn, an ninh mạng, cơ quan, đơn vị quản lý, vận hành hệ thống thông tin cấp tài khoản định danh cho người dùng của các đơn vị thuộc Bộ trong thời gian không quá 03 ngày làm việc, tính từ thời điểm nhận được văn bản đề nghị cấp tài khoản của đơn vị quản lý người dùng; điều chỉnh quyền truy cập, thu hồi tài khoản định danh của cá nhân thay đổi vị trí việc làm trong thời gian không quá 03 ngày làm việc tính từ ngày người dùng chính thức được bổ nhiệm, điều động, chuyển công tác, thôi việc, nghỉ hưu hoặc từ thời điểm nhận được văn bản đề nghị dừng tài khoản của đơn vị quản lý người dùng. Trường hợp cần duy trì tài khoản định danh sau thời điểm người dùng dừng làm việc tại đơn vị, đơn vị quản lý người dùng phải có văn bản gửi cơ quan quản lý hệ thống, trong đó nêu rõ lý do, phạm vi các quyền cần duy trì và thời gian duy trì tài khoản.

3. Đơn vị chuyên trách an toàn, an ninh mạng hoặc đơn vị vận hành hệ thống, cơ quan, đơn vị quản lý, vận hành hệ thống thông tin cấp tài khoản nhiệm vụ cho người dùng được đơn vị quản lý người dùng phân công thực hiện nhiệm vụ. Khi kết thúc thời gian thực hiện nhiệm vụ, người dùng bàn giao tài khoản nhiệm vụ cho người dùng được phân công tiếp nhận nhiệm vụ hoặc giao trả tài khoản cho đơn vị quản lý người dùng.

4. Quy định về mật khẩu của tài khoản thông tin

a) Mật khẩu phải đáp ứng các yêu cầu sau: có tối thiểu 8 ký tự, gồm tối thiểu 3 trong 4 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 (` ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ I : ; " ' < > , . ? /) và dấu cách; không chứa tên tài khoản. Khuyến khích sử dụng mật khẩu có độ dài từ 12 ký tự trở lên.

b) Mật khẩu phải được giữ bí mật và được đổi ngay sau khi tài khoản được bàn giao giữa các cá nhân, đơn vị hoặc khi nghi ngờ bị lộ, tránh sử dụng chung mật khẩu cho nhiều tài khoản. Mật khẩu phải được thay đổi ít nhất một lần trong 06 tháng.

5. Cá nhân được cấp hoặc giao tài khoản chịu trách nhiệm về các hành vi của tài khoản được ghi nhận trên thiết bị xử lý thông tin, hệ thống thông tin, hệ thống giám sát an toàn, an ninh mạng.

6. Đơn vị chuyên trách an toàn, an ninh mạng, đơn vị vận hành hệ thống, cơ quan, đơn vị quản lý, vận hành hệ thống thông tin thường xuyên rà soát các tài khoản đang hoạt động, phát hiện và thu hồi các tài khoản không sử dụng hoặc không hợp lệ, điều chỉnh thông tin tài khoản chưa phản ánh chính xác thông tin thực tế tại thời điểm rà soát.

Điều 13. Quy định về máy tính của người dùng

1. Máy tính do các đơn vị thuộc Bộ trang bị có kết nối vào mạng nội bộ phải đáp ứng đầy đủ các yêu cầu sau.

a) Đặt tên máy theo quy tắc.

- Đối với máy cá nhân: Tên viết tắt của đơn vị (theo quy định của Bộ VHTTDL)- Phòng/Ban-Tên của người dùng (ví dụ: TTCNTT-QLHTDLS-DANG), trường hợp trong một phòng có người trùng tên thì thêm Họ và tên đệm (ví dụ: TTCNTT-QLHTDLS-DANGVH) và thêm số thứ tự (nếu cần thiết).

- Đối với máy dùng chung: hoặc Tên viết tắt của đơn vị-Phòng/Ban-Chức năng dùng chung (ví dụ: TTCNTT-QLHTDLS-VANBAN).

b) Sử dụng hệ điều hành được hỗ trợ bản vá lỗ hổng bảo mật; trường hợp đã hết hỗ trợ phải có kế hoạch nâng cấp, thay thế. Chỉ cài đặt tiện ích thiết yếu được cung cấp kèm theo hệ điều hành và các phần mềm phục vụ công việc, có bản quyền hoặc được các cơ quan chức năng đánh giá, xác nhận an toàn.

c) Không kết nối với mạng không dây (wifi), mạng dữ liệu di động (3G/4G/5G...) không do đơn vị cung cấp.

d) Căn cứ yêu cầu về bảo đảm an toàn, an ninh mạng, quy định về kết nối, chia sẻ thông tin giám sát từ các đơn vị của Bộ với Trung tâm giám sát không gian mạng quốc gia thuộc Cục An toàn thông tin, Bộ Thông tin và Truyền thông (được quy định tại khoản 2 Điều 9 Quy chế này), Đơn vị chuyên trách an toàn, an ninh mạng có thể cài đặt thêm phần mềm giám sát an toàn, an ninh mạng đối với các máy tính đáp ứng hiệu năng yêu cầu.

đ) Máy trước khi kết nối vào mạng nội bộ Bộ Văn hóa, Thể thao và Du lịch phải được phải đáp ứng các quy định tại điểm a, b, c của khoản này. Đơn vị chuyên trách an toàn, an ninh mạng có trách nhiệm giám sát, đảm bảo máy tính kết nối vào mạng nội bộ tuân thủ các quy định tại khoản này; ngắt kết nối mạng của máy tính không đáp ứng quy định.

e) Máy tính khi được chuyển sử dụng từ cá nhân này sang cá nhân khác hoặc không tiếp tục sử dụng cho công việc của cơ quan phải thực hiện xóa toàn

bộ dữ liệu trên ổ cứng và có biên bản về việc xóa dữ liệu. Máy tính khi mang đi bảo hành, bảo dưỡng, sửa chữa, phải tháo ổ cứng hoặc xóa dữ liệu lưu trên ổ cứng.

2. Máy tính soạn thảo văn bản chứa nội dung bí mật nhà nước, lưu trữ bí mật nhà nước.

a) Sử dụng hệ điều hành và các phần mềm soạn thảo văn bản có bản quyền. Không kết nối vào mạng Internet, mạng nội bộ, mạng không dây, mạng viễn thông, trừ trường hợp đã áp dụng các biện pháp bảo vệ theo hướng dẫn của Ban Cơ yếu Chính phủ. Không sử dụng thiết bị lưu trữ ngoài, phải là thiết bị được Ban Cơ yếu Chính phủ cung cấp, trừ trường hợp cần cài đặt hệ điều hành, sửa chữa, nâng cấp phần mềm cho máy tính hoặc phục vụ công tác kiểm tra, thanh tra về an toàn, an ninh mạng.

b) Phân quyền truy cập máy tính theo tên người hoặc đơn vị cấp phòng được giao soạn thảo bí mật nhà nước.

c) Trường hợp ổ cứng lỗi cần mang đi bảo hành, phải thực hiện biện pháp xóa dữ liệu vĩnh viễn trước khi mang ổ cứng ra khỏi đơn vị và có biên bản ghi nhận về việc xóa dữ liệu giữa đơn vị sử dụng máy tính và đơn vị nhận ổ cứng. Việc sửa chữa, nâng cấp phần mềm cho máy tính (sau khi đã đưa vào sử dụng), nếu yêu cầu phải tiếp cận các tệp tin trên ổ cứng, phải thực hiện dưới sự giám sát của đơn vị sử dụng máy tính, đảm bảo không lộ lọt dữ liệu trên ổ cứng máy tính ra bên ngoài trong quá trình này (có biên bản giữa đơn vị sử dụng máy tính và đơn vị sửa chữa, nâng cấp phần mềm).

d) Đơn vị được cấp sử dụng máy tính soạn thảo, lưu trữ bí mật nhà nước chịu trách nhiệm giám sát, đảm bảo việc sử dụng máy tính tuân thủ đúng quy định tại khoản này.

3. Trường hợp máy tính xách tay được cơ quan trang bị để sử dụng bên ngoài phạm vi cơ quan, đơn vị thuộc Bộ, nếu kết nối Internet, phải cài đặt hệ điều hành được hỗ trợ bản vá lỗ hổng bảo mật và phần mềm phòng diệt mã độc, phải cập nhật thường xuyên bản vá cho hệ điều hành và mẫu nhận diện mã độc do nhà sản xuất cung cấp.

4. Đối với máy tính bảng được cơ quan trang bị để phục vụ công việc phải sử dụng hệ điều hành được hỗ trợ bản vá lỗ hổng bảo mật; chỉ cài đặt phần mềm phục vụ công việc và các phần mềm bảo đảm an toàn an, ninh mạng do đơn vị chuyên trách về an toàn, an ninh thông tin mạng cung cấp hoặc các đơn vị về an toàn, an ninh mạng được Bộ Thông tin và Truyền thông cấp phép.

5. Máy tính do người dùng tự trang bị, khi kết nối vào mạng nội bộ hoặc chạy ứng dụng của Bộ Văn hóa, Thể thao và Du lịch từ địa điểm bên ngoài mạng nội bộ của Bộ Văn hóa, Thể thao và Du lịch, phải đáp ứng đầy đủ các điều kiện dưới đây.

a) Cài đặt đầy đủ các bản vá lỗ hổng bảo mật của hệ điều hành; cài đặt phần mềm phòng diệt mã độc và cập nhật mẫu nhận diện mã độc mới nhất.

b) Không cài đặt, sử dụng phần mềm, công cụ có tính năng hoặc tạo rủi ro mất an toàn an ninh mạng (cấp phát địa chỉ mạng, dò quét mật khẩu, dò quét cổng mạng, giả lập tấn công...).

c) Khi kết nối vào mạng nội bộ Bộ Văn hóa, Thể thao và Du lịch, người dùng cần thực hiện: ngắt các kết nối vào các hệ thống mạng khác (mạng không dây, mạng dữ liệu di động...), không sử dụng máy tính như một điểm phát sóng không dây.

6. Đối với các máy tính, thiết bị được cài đặt phần mềm giám sát an toàn an ninh mạng (quy định tại điểm d khoản 1 Điều này), không được tự ý gỡ bỏ phần mềm an toàn thông tin, khi có sự cố mất kết nối, trục trặc phần mềm hoặc có thay đổi về thiết bị, phụ kiện thay thế dẫn đến mất phần mềm an toàn thông tin cần thông báo/phản ánh tới đầu mối cài đặt để tiến hành xử lý khắc phục hoặc cài đặt lại phần mềm.

Điều 14. Quy định đối với người dùng

Người dùng tại đơn vị thuộc Bộ Văn hóa, Thể thao và Du lịch có trách nhiệm

1. Đảm bảo an toàn mật khẩu các tài khoản thông tin mà người dùng được cấp, theo quy định tại khoản 4 Điều 14 của Quy chế này. Nếu phát hiện có dấu hiệu lộ mật khẩu, thực hiện các việc sau: đổi mật khẩu tại máy tính làm việc tại cơ quan; quét mã độc trên các thiết bị của cá nhân đã từng được sử dụng để truy cập thư điện tử công vụ hoặc các ứng dụng của Bộ Văn hóa, Thể thao và Du lịch trước đó; cung cấp thông tin về sự việc, hiện tượng cho bộ phận hỗ trợ kỹ thuật của đơn vị chuyên trách an toàn, an ninh mạng.

2. Sử dụng tài khoản định danh cá nhân khi đăng nhập vào máy tính có kết nối vào mạng nội bộ.

3. Không lưu thông tin ngoài phạm vi công việc và hoạt động của đơn vị trên ổ đĩa mạng. Xóa thông tin trên ổ đĩa mạng do bản thân tạo ra sau khi thông tin hết giá trị sử dụng.

4. Nếu nghi ngờ hoặc phát hiện thư điện tử nhận được là thư rác, thư giả mạo, người dùng chuyển tiếp thư này cho bộ phận hỗ trợ kỹ thuật của Đơn vị chuyên trách an toàn, an ninh mạng để áp dụng biện pháp ngăn chặn. Không mở các địa chỉ trong nội dung thư, mở tệp đính kèm hoặc thực hiện theo hướng dẫn của thư điện tử có địa chỉ nhận không rõ nguồn gốc. Không mở thư điện tử công vụ và các phần mềm nội bộ của Bộ Văn hóa, Thể thao và Du lịch trên máy tính công cộng hoặc máy tính không đáp ứng các yêu cầu quy định tại khoản 3, 4, 5 Điều 15 của Quy chế này. Không sử dụng địa chỉ thư điện tử công vụ để đăng ký sử dụng các ứng dụng, dịch vụ ngoài phạm vi công việc. Mã hóa (đặt mật

khẩu) các tệp tin có nội dung nhạy cảm trước khi gửi qua thư điện tử và gửi mật khẩu cho người nhận bằng phương thức khác.

5. Thực hiện quét mã độc thiết bị lưu trữ ngoài (thẻ nhớ, ổ đĩa ngoài,...) trước khi sử dụng. Bảo vệ thiết bị lưu trữ ngoài, không để thất thoát thông tin, tài liệu của cơ quan. Mã hóa (đặt mật khẩu) các tệp tin có nội dung nhạy cảm khi lưu trữ trên thiết bị lưu trữ ngoài và xóa thông tin, tài liệu của cơ quan trên thiết bị lưu trữ ngoài sau khi hoàn thành xử lý công việc cần sử dụng thiết bị lưu trữ ngoài.

6. Thực hiện soạn thảo văn bản chứa nội dung bí mật nhà nước, lưu trữ tài liệu mật tại máy tính được trang bị cho việc soạn thảo, lưu trữ văn bản mật theo quy định. Không sử dụng thiết bị lưu trữ ngoài để lưu thông tin, tài liệu mật, trừ trường hợp có áp dụng các biện pháp mã hóa do Ban Cơ yếu Chính phủ cung cấp.

7. Đối với bí mật công tác, bí mật hoạt động nghiệp vụ, dữ liệu cá nhân do người dùng được phân công xử lý: áp dụng mã hóa dữ liệu trong trường hợp cần lưu trữ, truyền đưa trên môi trường mạng hoặc thiết bị lưu trữ ngoài; giới hạn phạm vi truy cập trong phạm vi các cá nhân có trách nhiệm tham gia xử lý.

8. Khóa máy tính (sử dụng tính năng của hệ điều hành) khi rời khỏi nơi đặt máy tính; tắt máy tính khi rời khỏi cơ quan.

9. Cập nhật bản vá hệ điều hành và quét mã độc thường xuyên máy tính xách tay hoặc máy do người dùng tự trang bị và sử dụng để truy cập ứng dụng của Bộ Văn hóa, Thể thao và Du lịch từ Internet.

10. Phối hợp với Trung tâm Công nghệ thông tin trong việc triển khai các biện pháp an toàn, an ninh mạng trên máy tính của người dùng, gỡ mã độc (nếu phát hiện có mã độc mà phần mềm phòng diệt mã độc không có khả năng xử lý), điều tra nguyên nhân mất an toàn an ninh mạng liên quan đến người dùng hoặc máy tính của người dùng.

Điều 15. Quy định về hệ thống mạng nội bộ của đơn vị thuộc Bộ

1. Hệ thống mạng nội bộ đơn vị thuộc Bộ Văn hóa, Thể thao và Du lịch phải được tổ chức thành các vùng mạng theo chức năng gồm: vùng mạng người dùng; vùng mạng kết nối Internet; mạng truyền số liệu chuyên dùng Chính phủ; vùng mạng máy chủ cung cấp ứng dụng, dịch vụ ra Internet; vùng mạng máy chủ nội bộ, máy chủ cơ sở dữ liệu; vùng mạng hệ thống quản lý tập trung, quản trị thiết bị; vùng mạng phục vụ công tác quản trị; vùng mạng hệ thống giám sát an toàn an ninh mạng. Sử dụng tường lửa mạng để kiểm soát truy cập giữa các vùng mạng: Chỉ cho phép truy cập các ứng dụng, dịch vụ theo từng ứng dụng, dịch vụ cụ thể; chặn tất cả truy cập tới các dịch vụ, ứng dụng không sử dụng hoặc không phục vụ công việc. Thiết lập phòng chống xâm nhập và phòng chống phần mềm độc hại trên môi trường mạng cho các vùng mạng máy chủ.

2. Các kết nối mạng để xác thực, truy cập thông tin, trao đổi thông tin, quản trị ứng dụng/thiết bị/hệ thống phải áp dụng mã hóa.

3. Các thiết bị mạng lõi, thiết bị mạng các vùng mạng máy chủ, thiết bị an toàn an ninh mạng phải được cấu hình gửi nhật ký hệ thống tới hệ thống giám sát an toàn an ninh mạng. Nhật ký hệ thống của các thiết bị mạng phải được lưu trữ tối thiểu 03 tháng.

4. Các thiết bị mạng phải được cấu hình xác thực để xác thực truy cập quản trị. Chỉ cho phép truy cập quản trị thiết bị mạng từ vùng mạng phục vụ công tác quản trị.

5. Truy cập quản trị hệ thống từ Internet phải thông qua cổng truy cập SSL VPN và thực hiện xác thực 02 yếu tố; Thiết lập giới hạn thời gian chờ để đóng phiên kết nối khi cổng SSL VPN không nhận được tín hiệu từ người truy cập (tối đa 60 phút).

6. Các thiết bị kết nối vào mạng nội bộ phải đồng bộ thời gian với máy chủ thời gian (được đồng bộ với nguồn thời gian tin cậy trên Internet).

7. Thiết bị mạng, thiết bị an toàn, an ninh mạng phải được xử lý lỗ hổng, điểm yếu đã công bố trước khi đưa vào sử dụng và khi có cảnh báo về lỗ hổng bảo mật mới. Thực hiện kiểm tra, đánh giá an toàn, an ninh mạng đối với hệ thống mạng nội bộ định kỳ hàng năm.

8. Tài liệu mô tả hệ thống mạng phải được cập nhật thường xuyên, phản ánh chính xác thực tế các cấu hình, chính sách đang áp dụng cho hệ thống mạng.

Điều 16. Quy định về kết nối Internet

1. Tất cả các kết nối Internet từ mạng nội bộ phải thông qua hệ thống bảo vệ truy cập Internet (VD: Tường lửa, hệ thống IPS/IDS…có tính năng lọc bỏ, không cho phép truy nhập các trang tin có nghi ngờ chứa mã độc hoặc các nội dung không phù hợp).

2. Từ máy trạm có kết nối mạng nội bộ, người sử dụng truy cập Internet thông qua hệ thống Internet an toàn (gồm các máy chủ trung gian ngăn cách máy trạm của người dùng và mạng Internet).

3. Đối với máy chủ và thiết bị xử lý thông tin khác, chỉ thiết lập kết nối Internet cho các hệ thống được thiết kế có giao tiếp với Internet.

Điều 17. Quy định về hệ thống thông tin

1. Phần mềm ứng dụng của Bộ Văn hóa, Thể thao và Du lịch phải đáp ứng các yêu cầu sau.

a) Áp dụng Khung phát triển phần mềm an toàn theo hướng dẫn của Bộ Thông tin và Truyền thông.

b) Sử dụng hệ điều hành, cơ sở dữ liệu, công cụ phát triển phần mềm có bản quyền hoặc được các cơ quan chức năng đánh giá, xác nhận an toàn; được cung cấp bản vá lỗ hổng, điểm yếu bảo mật trong thời gian hoạt động.

c) Truy cập ứng dụng web phải thông qua tường lửa ứng dụng web; sử dụng chứng thư số SSL đặt trên tường lửa ứng dụng web để mã hóa kết nối giữa người dùng, người quản trị và hệ thống thông tin. Tách riêng địa chỉ truy cập dành cho người dùng và truy cập dành cho quản trị ứng dụng.

d) Có khả năng tích hợp với hệ thống quản lý người dùng tập trung để xác thực người dùng tại cơ quan Bộ. Có tính năng cho phép người dùng đổi mật khẩu. Cho phép cấu hình đảm bảo an toàn mật khẩu người sử dụng đối với tài khoản xác thực tại ứng dụng: Yêu cầu thay đổi mật khẩu mặc định; Cho phép thiết lập quy tắc đặt mật khẩu về số ký tự, loại ký tự; Cho phép thiết lập thời gian yêu cầu thay đổi mật khẩu; Cho phép thiết lập thời gian mật khẩu hợp lệ; Hạn chế số lần đăng nhập sai trong khoảng thời gian nhất định với tài khoản nhất định. Mã hóa thông tin xác thực đối với tài khoản xác thực tại ứng dụng theo tiêu chuẩn mã hóa do Bộ Thông tin và Truyền thông quy định. Cho phép cấu hình giới hạn thời gian chờ để đóng phiên kết nối khi ứng dụng không nhận được yêu cầu từ người dùng (cấu hình ban đầu 60 phút và điều chỉnh trong quá trình hoạt động để phù hợp với yêu cầu thực tế của từng ứng dụng).

đ) Có tính năng kiểm tra tính hợp lệ của dữ liệu đầu vào, đầu ra; lọc bỏ, ngăn chặn dữ liệu không hợp lệ.

e) Có tính năng ghi nhật ký hệ thống và gửi nhật ký hệ thống tới hệ thống giám sát an toàn an ninh mạng. Giới hạn kích thước tệp nhật ký hệ thống lưu trên máy chủ ở mức độ phù hợp để không làm ảnh hưởng đến hiệu năng của ứng dụng. Nhật ký hệ thống của ứng dụng phải được lưu trữ tối thiểu 03 tháng.

g) Có phương án sao lưu dự phòng sự cố sử dụng hệ thống sao lưu dữ liệu.

h) Có thiết kế đáp ứng yêu cầu bảo đảm an toàn hệ thống thông tin theo cấp độ. Khi có thay đổi thiết kế, phải đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống.

i) Áp dụng biện pháp bảo vệ theo hướng dẫn của Ban Cơ yếu Chính phủ đối với ứng dụng có xử lý bí mật nhà nước.

2. Dữ liệu xử lý trong hệ thống thông tin.

a) Trường hợp hệ thống thông tin cần thu thập, xử lý, lưu trữ dữ liệu cá nhân, phải đáp ứng các yêu cầu sau: Chỉ thu thập các dữ liệu cá nhân được phép thu thập theo quy định của pháp luật; Thông báo tới người dùng các loại dữ liệu cá nhân được thu thập, xử lý, lưu trữ thông tin trong hệ thống thông tin và biện pháp bảo vệ; Chỉ cơ quan, đơn vị có trách nhiệm được phân quyền truy cập, sử dụng dữ liệu cá nhân.

b) Thông tin bí mật nhà nước phải được mã hóa bằng giải pháp do Ban Cơ yếu Chính phủ cung cấp.

c) Áp dụng chữ ký số trong trường hợp cần đảm bảo chống từ chối nguồn gốc dữ liệu.

3. Máy chủ thuộc các hệ thống thông tin phải đáp ứng các yêu cầu sau.

a) Sử dụng hệ điều hành được cung cấp bản vá lỗ hổng, điểm yếu. Chỉ cài đặt các dịch vụ, tiện ích thiết yếu được cung cấp kèm theo hệ điều hành và các phần mềm phục vụ hoạt động của máy chủ, có nguồn gốc an toàn và không nhiễm mã độc. Cài đặt phần mềm phòng diệt mã độc và cập nhật mẫu nhận diện mã độc; Cài đặt phần mềm giám sát an toàn an ninh mạng, cấu hình tự động tải bản vá lỗ hổng bảo mật mức hệ điều hành từ hệ thống quản lý bản vá lỗ hổng bảo mật tập trung (đối với máy chủ sử dụng hệ điều hành Windows).

c) Thiết lập chính sách xác thực trên máy chủ đáp ứng quy định về mật khẩu của tài khoản thông tin quy định tại khoản 5 Điều 14 của Quy chế này; yêu cầu thay đổi mật khẩu mặc định. Cấu hình giới hạn thời gian chờ để đóng phiên kết nối khi máy chủ không nhận được yêu cầu từ người dùng (tối đa 60 phút).

d) Cấu hình gửi nhật ký hệ thống tới hệ thống giám sát an toàn, an ninh mạng. Nhật ký hệ thống của máy chủ phải được lưu trữ tối thiểu 03 tháng.

đ) Không kết nối với mạng không dây, mạng dữ liệu di động.

e) Thực hiện cài đặt bản vá lỗ hổng bảo mật mức hệ điều hành trong vòng 07 ngày làm việc sau khi bản vá được phát hành.

g) Không lưu mã nguồn ứng dụng; tài liệu thiết kế, cài đặt, quản trị, vận hành, bảo đảm an toàn an ninh mạng hệ thống thông tin trên máy chủ không có chức năng lưu trữ mã nguồn và tài liệu về hệ thống thông tin.

4. Hệ thống thông tin phải được triển khai, cấu hình và duy trì hoạt động đáp ứng các quy định tại Điều này và theo phương án bảo đảm an toàn thông tin đã được phê duyệt theo hồ sơ đề xuất cấp độ; được kiểm tra, đánh giá an toàn, an ninh mạng trước khi đưa vào sử dụng và định kỳ hàng năm trong quá trình vận hành.

5. Tài liệu về hệ thống thông tin phải được cập nhật trong quá trình vận hành, đảm bảo phản ánh chính xác hiện trạng của hệ thống. Tài liệu về hệ thống thông tin phải được lưu giữ an toàn, chỉ được cung cấp cho các đối tượng có trách nhiệm đối với hệ thống thông tin.

Điều 18. Quy định về kết thúc sử dụng hệ thống thông tin

1. Hệ thống thông tin phải kết thúc sử dụng khi: đã được thay thế hoàn toàn bằng hệ thống thông tin khác; hoặc không còn giá trị sử dụng; hoặc sử dụng phiên bản phần mềm có lỗ hổng bảo mật nghiêm trọng và không có biện pháp ngăn chặn việc khai thác các lỗ hổng bảo mật này; hoặc các thành phần tài sản của hệ thống thông tin đã hết thời gian khấu hao sử dụng theo quy định pháp

luật về quản lý, sử dụng tài sản công và được cấp có thẩm quyền cho phép dừng sử dụng.

2. Thủ tục kết thúc vận hành, khai thác, hủy bỏ hệ thống thông tin.

a) Đơn vị vận hành hệ thống thông tin báo cáo chủ quản hệ thống thông tin cho phép kết thúc vận hành, khai thác hệ thống thông tin.

b) Chủ quản hệ thông tin và đơn vị vận hành thực hiện sao lưu dữ liệu hệ thống thông tin; dừng hoạt động của hệ thống; thu hồi tài nguyên máy chủ ảo hóa (nếu hệ thống thông tin sử dụng nền tảng ảo hóa) hoặc xóa bỏ hoàn toàn (không có khả năng phục hồi) nội dung thông tin, dữ liệu trên thiết bị vật lý trước khi chuyển sang bộ phận quản lý tài sản chờ thanh lý; thu hồi địa chỉ mạng, cấu hình trên hệ thống mạng, hệ thống an toàn, an ninh mạng áp dụng cho hệ thống thông tin.

Điều 19. Quy định về sao lưu dữ liệu phòng ngừa sự cố

1. Đơn vị quản lý, vận hành hệ thống thực hiện sao lưu thông tin, dữ liệu của hệ thống thông tin như sau.

a) Loại dữ liệu cần sao lưu: Cơ sở dữ liệu, thông tin về cấu hình của phần mềm nội bộ, thông tin cấu hình thiết bị, hệ điều hành của thiết bị và những thông tin, dữ liệu khác (nếu có) phục vụ công tác quản lý, khai thác sử dụng.

b) Đối với cơ sở dữ liệu, thông tin về cấu hình của phần mềm nội bộ: Thực hiện sao lưu ngoài giờ hành chính.

c) Đối với thông tin cấu hình thiết bị, hệ điều hành của thiết bị và những thông tin, dữ liệu khác (nếu có): Thực hiện sao lưu 01 bản sao lưu sau mỗi lần cài đặt, thay đổi cấu hình.

d) Lưu giữ tối thiểu 03 bản sao lưu gần nhất.

2. Dữ liệu sao lưu được khôi phục trong các trường hợp: có yêu cầu khôi phục dữ liệu từ người dùng; ứng dụng, cơ sở dữ liệu đang hoạt động bị sự cố, cần khôi phục từ bản sao lưu; hoặc theo yêu cầu của cơ quan có thẩm quyền.

Điều 20. Kiểm tra, đánh giá, chế độ báo cáo an toàn, an ninh thông tin mạng

1. Nội dung kiểm tra, đánh giá

a) Kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn, an ninh thông tin theo cấp độ.

b) Đánh giá hiệu quả của biện pháp bảo đảm an toàn, an ninh hệ thống thông tin.

c) Đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống.

d) Kiểm tra, đánh giá khác do chủ quản hệ thống thông tin quy định.

2. Hình thức kiểm tra, đánh giá:

a) Kiểm tra, đánh giá định kỳ theo kế hoạch của chủ quản hệ thống thông tin.

b) Kiểm tra, đánh giá đột xuất theo yêu cầu của cấp có thẩm quyền.

3. Công tác kiểm tra.

a) 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.

b) Giao đơn vị chuyên trách an toàn, an ninh mạng kiểm tra và báo cáo Bộ việc thực hiện Quy chế này tại các đơn vị trực thuộc Bộ.

4. Chế độ báo cáo.

a) Đơn vị vận hành hệ thống thông tin hàng năm định kỳ hoặc đột xuất báo cáo công tác thực thi bảo đảm an toàn hệ thống thông tin theo chủ quản hệ thống thông tin hoặc đơn vị chuyên trách có thẩm quyền. Nội dung báo cáo thực hiện theo Điều 14 Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông.

b) Báo cáo định kỳ gửi về Cục Thống kê tội phạm và Trung tâm Công nghệ thông tin trước ngày 30 tháng 11 hàng năm để tổng hợp báo cáo Bộ Văn hóa, Thể thao và Du lịch.

Chương IV

TỔ CHỨC THỰC HIỆN

Điều 21. Thủ trưởng cơ quan, đơn vị thuộc Bộ

1. Tổ chức triển khai thực hiện Quy chế này và các quy định của pháp luật, văn bản chỉ đạo và hướng dẫn của các cơ quan có thẩm quyền về an toàn an ninh mạng; Ban hành quy định về an toàn, an ninh mạng của đơn vị mình phù hợp với Quy chế này và các quy định của pháp luật về an toàn, an ninh mạng; Xây dựng kế hoạch, báo cáo định kỳ, đột xuất về an toàn, an ninh mạng và gửi Trung tâm Công nghệ thông tin tổng hợp, báo cáo lãnh đạo Bộ.

2. Chỉ đạo cán bộ chuyên trách an toàn, an ninh mạng trực thuộc đơn vị phối hợp chặt chẽ với Trung tâm Công nghệ thông tin trong quá trình triển khai công tác an toàn an ninh mạng tại đơn vị.

3. Trong trường hợp mua sắm trang bị thiết bị hạ tầng công nghệ thông tin, xây dựng phần mềm có liên quan hoặc ảnh hưởng tới hạ tầng công nghệ, phần mềm dùng chung của Bộ phải có tư vấn, thông qua của đơn vị chuyên trách thẩm định để không gây ảnh hưởng tới hạ tầng công nghệ chung của Bộ.

4. Cử cán bộ công chức, viên chức, người lao động tham gia chương trình đào tạo, tập huấn của Bộ Văn hóa, Thể thao và Du lịch về an toàn thông tin mạng, an ninh mạng.

Điều 22. 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 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 23. Công chức, viên chức, người lao động

1. Trách nhiệm của cán bộ, công chức, viên chức phụ trách an toàn thông tin mạng, an ninh mạng của đơn vị.

a) Chịu trách nhiệm bảo đảm an toàn thông tin mạng, an ninh mạng của đơn vị.

b) Tham mưu lãnh đạo đơn vị ban hành quy định, quy chế bảo đảm an toàn, an ninh thông tin mạng của đơn vị và là đầu mối để triển khai thực hiện các giải pháp kỹ thuật bảo đảm an toàn, anh ninh mạng.

c) Giám sát, đánh giá, kịp thời báo cáo thủ trưởng đơn vị các nguy cơ gây mất an toàn thông tin của đơn vị.

d) Định kỳ báo cáo, đánh giá với thủ trưởng đơn vị về tình hình đảm bảo an toàn thông tin và đề xuất các biện pháp khắc phục, nâng cao an toàn, an ninh thông tin.

đ) Phối hợp với các cá nhân, đơn vị được giao đầu mối trong việc kiểm soát, phát hiện và khắc phục các sự cố an toàn, an ninh thông tin.

2. Trách nhiệm của cán bộ, công chức, viên chức, người lao động trong các cơ quan, đơn vị.

a) Nghiêm túc chấp hành các quy định, quy trình nội bộ của đơn vị, Quy chế này và các quy định khác của pháp luật về an toàn thông tin.

b) Chịu trách nhiệm bảo đảm an toàn thông tin trong phạm vi trách nhiệm và quyền hạn được giao; tự quản lý, bảo quản thiết bị mà mình được giao sử dụng.

c) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin phải báo cáo ngay với bộ phận phụ trách an toàn thông tin của đơn vị để kịp thời ngăn chặn và xử lý.

Điều 24. Trung tâm Công nghệ thông tin

1. Tham mưu cho Lãnh đạo Bộ về việc triển khai công tác an toàn thông tin mạng, an ninh mạng; Hướng dẫn các quy định của pháp luật, văn bản chỉ đạo trong phạm vi các cơ quan, đơn vị, tổ chức thuộc Bộ Văn hóa, Thể thao và Du lịch; Tổ chức triển khai Quy chế này và các quy định của pháp luật về an toàn, an ninh mạng tại đơn vị thuộc Bộ.

2. Tổng hợp kế hoạch, báo cáo định kỳ, đột xuất về an toàn an ninh mạng, trình Lãnh đạo Bộ Văn hóa, Thể thao và Du lịch gửi các cơ quan quản lý về an toàn an ninh mạng; Xử lý các việc đột xuất về an toàn, an ninh mạng (chưa quy định tại Quy chế này) theo phân công của Lãnh đạo Bộ.

3. Định kỳ hàng năm, tổ chức rà soát, kiểm tra tính phù hợp của Quy chế này với các quy định của pháp luật về an toàn thông tin mạng, an ninh mạng và các quy định, tiêu chuẩn liên quan; kiểm tra tính đáp ứng của Quy chế này với yêu cầu thực tế của Bộ Văn hóa, Thể thao và Du lịch; báo cáo Bộ về việc sửa đổi, bổ sung Quy chế trong trường hợp cần thiết.

Điều 25. Khen thưởng và xử lý vi phạm

1. Trung tâm Công nghệ thông tin tiến hành kiểm tra, đánh giá, xếp hạng an toàn, an ninh thông tin mạng, trên cơ sở đó tham mưu, đề xuất Lãnh đạo Bộ xem xét khen thưởng hàng năm theo quy định.

2. Kết quả thực hiện Quy chế này là một trong những tiêu chí có thể sử dụng để đánh giá kết quả thực hiện hàng năm của cá nhân, đơn vị.

3. Các cơ quan, đơn vị và các cán bộ, công chức, viên chức người lao động trực thuộc Bộ có hành vi vi phạm quy chế này tùy theo mức độ vi phạm bị xử lý theo quy định.

Điều 26. 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 Văn hóa, Thể thao và Du lịch.

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 Trung tâm Công nghệ thông tin để tổng hợp, gửi Văn phòng Bộ phối hợp với Vụ Kế hoạch - Tài chính thẩm định, trình lãnh đạo Bộ phê duyệt.

Điều 27. Điều khoản thi hành

1. Thủ trưởng các cơ quan, đơn vị 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 Quy chế, nếu có khó khăn, vướng mắc, các cơ quan, đơn vị có liên quan phản ánh kịp thời về Bộ Văn hóa, Thể thao và Du lịch (qua Trung tâm Công nghệ thông tin) để tổng hợp báo cáo trình Lãnh đạo Bộ sửa đổi, bổ sung cho phù hợp./.