Số: 363/QĐ-SGDĐT; 04/03/2026; 15:02:49;

UBND TỈNH NINH BÌNH
SỞ GIÁO DỤC VÀ ĐÀO TẠO

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

QUY CHẾ
Bảo đảm an ninh mạng, an toàn thông tin đối với hệ thống thông tin thuộc phạm vi quản lý của Sở Giáo dục và Đào tạo

(Ban hành kèm theo Quyết định số /QĐ-SGDĐT ngày /3/2026 của Sở Giáo dục và Đào tạo tỉnh Ninh Bình)

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 việc bảo đảm an ninh mạng và an toàn thông tin đối với các hệ thống thông tin thuộc phạm vi quản lý của Sở Giáo dục và Đào tạo tỉnh Ninh Bình.

2. Đối tượng áp dụng

Cán bộ, công chức, người lao động thuộc Sở Giáo dục và Đào tạo và các tổ chức, cá nhân liên quan đến việc vận hành, khai thác hệ thống thông tin thuộc phạm vi quản lý của Sở Giáo dục và Đào tạo tỉnh Ninh Bình.

Điều 2. Giải thích từ ngữ

1. 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.

2. An toàn thông tin 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.

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. 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.

5. Đơn vị vận hành hệ thống thông tin được quy định tại Điều 5 Chương I của Thông tư 12/2022/TT-BTTTT.

6. Hạ tầng kỹ thuật là tập hợp thiết bị tính toán (máy chủ, máy trạm), thiết bị ngoại vi, thiết bị kết nối mạng, thiết bị phụ trợ, mạng nội bộ, mạng diện rộng.

7. 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.

8. 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.

9. Ứng cứu sự cố an toàn thông tin mạng là hoạt động nhằm xử lý, khắc phục sự cố gây mất an toàn thông tin mạng gồm: theo dõi, thu thập, phân tích, phát hiện, cảnh báo, điều tra, xác minh sự cố, ngăn chặn sự cố, khôi phục dữ liệu và khôi phục hoạt động bình thường của hệ thống thông tin.

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

Bảo đảm an ninh mạng, an toàn thông tin tuân thủ các nguyên tắc chung quy định tại Điều 4 Luật An ninh mạng, Điều 4 Luật An toàn thông tin mạng và Điều 4 Nghị định số 85/2016/NĐ-CP.

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.

7. Các hành vi bị nghiêm cấm quy định tại Điều 8 của Luật An ninh mạng, Điều 5 của Luật Bảo vệ bí mật nhà nước.

8. Hành vi khác bị nghiêm cấm theo quy định của pháp luật.

Chương II

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

Điều 5. Bảo đảm an ninh mạng, an toàn thông tin khi sử dụng máy tính và thiết bị ngoại vi

1. Máy tính và thiết bị ngoại vi phải được cài đặt hệ điều hành, phần mềm văn phòng, phần mềm chuyên dụng để xử lý công việc và tuân thủ các quy định sau:

a) Chỉ cài đặt phần mềm hợp lệ (phần mềm có bản quyền thương mại, phần mềm nội bộ hoặc phần mềm mã nguồn mở được đầu tư (hoặc thuê dịch vụ) có nguồn gốc rõ ràng) và thuộc danh mục phần mềm được phép sử dụng do đơn vị có thẩm quyền ban hành; thường xuyên cập nhật phần mềm và hệ điều hành.

b) Cài đặt phần mềm xử lý phần mềm độc hại và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm; thực hiện kiểm tra, rà quét phần mềm độc hại khi sao chép, mở các tập tin hoặc trước khi kết nối các thiết bị lưu trữ dữ liệu di động với máy tính của mình.

c) Khi phát hiện bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại trên máy tính (máy chạy chậm bất thường, cảnh báo từ phần mềm phòng, chống phần mềm độc hại, mất dữ liệu,...), phải cô lập máy tính (ngắt kết nối mạng vật lý, tắt máy) và báo trực tiếp cho bộ phận, cán bộ phụ trách an ninh mạng, an toàn thông tin của cơ quan (Phòng Công tác học sinh, sinh viên) để được xử lý kịp thời.

d) 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; sử dụng những trình duyệt an toàn; không truy nhập, mở các trang tin, thư điện tử không rõ nguồn gốc; không sử dụng tính năng lưu mật khẩu tự động hoặc đăng nhập tự động trên các máy tính dùng chung.

đ) Có trách nhiệm bảo mật tài khoản truy nhập thông tin, không chia sẻ mật khẩu, thông tin cá nhân với người khác. Đặt mật khẩu với độ an toàn cao (tối thiểu 8 ký tự bao gồm: có chữ thường, có chữ in hoa, có số và ký tự đặc biệt như @, #, !,...) và thay đổi mật khẩu tối thiểu 6 tháng/lần; các tài khoản đăng nhập hệ thống phải được đăng xuất khi không sử dụng; thường xuyên xóa bộ nhớ cache và cookie trong trình duyệt trên máy tính.

e) Thực hiện thao tác khóa máy tính (sử dụng tính năng có sẵn trên máy tính) khi rời khỏi nơi đặt máy tính; tắt máy tính khi rời khỏi cơ quan.

2. 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 thực hiện xử lý công việc phải báo cáo và phải được lãnh đạo Phòng đồng ý, cho phép. Trong trường hợp này, cá nhân phải tuân thủ đầy đủ các quy định tại khoản 1 Điều này và chịu sự giám sát của bộ phận chuyên trách, được giao nhiệm vụ về an ninh mạng, an toàn thông tin của đơn vị.

3. Đối với thiết bị soạn thảo, lưu trữ bí mật nhà nước

a) Phải sử dụng máy tính độc lập, máy in (photocopy) không kết nối và không có lịch sử kết nối với mạng Internet, mạng máy tính, mạng viễn thông, trừ trường hợp lưu giữ bí mật nhà nước theo quy định của pháp luật về cơ yếu để soạn thảo, lưu trữ các văn bản có nội dung bí mật nhà nước.

b) Cá nhân được giao nhiệm vụ trong quá trình xử lý công việc, soạn thảo văn bản có nội dung bí mật nhà nước chỉ sử dụng máy tính, thiết bị theo quy định tại điểm a của khoản này; việc lưu trữ phải được thực hiện ở các thiết bị riêng biệt, bảo đảm các yêu cầu của pháp luật về bảo vệ bí mật nhà nước và cơ yếu.

Điều 6. Quản lý trang thiết bị công nghệ thông tin, an toàn, an ninh thông tin đối với cá nhân

1. Quản lý trang thiết bị công nghệ thông tin đối với cá nhân

a) Các cá nhân có trách nhiệm quản lý trang thiết bị công nghệ thông tin trong phạm vi được giao phụ trách.

b) 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 báo phòng Công tác học sinh, sinh viên thực hiện các biện pháp xóa, tiêu hủy dữ liệu đó bảo đảm 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.

c) Thiết bị tính toán 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).

d) Văn phòng có trách nhiệm định kỳ kiểm tra, sửa chữa, bảo trì thiết bị (bao gồm thiết bị đang hoạt động và thiết bị dự phòng) và Phòng Công tác học

sinh, sinh viên có trách nhiệm hướng dẫn cách sử dụng, quản lý, vận hành hệ thống hạ tầng kỹ thuật công nghệ thông tin.

2. Quản lý an ninh mạng, an toàn thông tin đối với cá nhân

a) Các phòng thuộc Sở phải xây dựng các yêu cầu, trách nhiệm bảo đảm an ninh mạng, an toàn thông tin đối với từng vị trí công việc. Sau khi tuyển dụng, tiếp nhận nhân sự mới, đơn vị phải có trách nhiệm phổ biến cho nhân sự mới các quy định về bảo đảm an ninh mạng, an toàn thông tin tại đơn vị; 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 xây dựng quy trình làm việc bao gồm nhiều lớp bảo mật đảm bảo an toàn thông tin.

b) Các phòng thuộc Sở phải thường xuyên tổ chức quán triệt các quy định về an ninh mạng, an toàn thông tin, nhằm nâng cao nhận thức về trách nhiệm bảo đảm an ninh mạng, an toàn thông tin của từng cá nhân trong đơn vị.

c) Các phòng thuộc Sở gửi yêu cầu bằng văn bản về phòng Công tác học sinh, sinh viên khi có nhu cầu 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.

d) Khi cá nhân thuộc đơn vị chấm dứt hoặc thay đổi công việc, phải lập biên bản bàn giao tài sản công nghệ thông tin và đơn vị phải thông báo bằng văn bản về phòng Công tác học sinh, sinh viên thay đổi hoặc thu hồi quyền truy cập các hệ thống thông tin.

Điều 7. An toàn thông tin mạng đối với thuê dịch vụ công nghệ thông tin

1. Phòng Công tác học sinh, sinh viên chịu trách nhiệm chủ trì, phối hợp với các phòng thuộc Sở khi tham mưu Lãnh đạo Sở ký kết hợp đồng thuê dịch vụ công nghệ thông tin; Hợp đồng phải xác định rõ phạm vi, trách nhiệm, quyền hạn và nghĩa vụ của các bên về bảo đảm an toàn thông tin. Trong hợp đồng phải bao gồm các điều khoản về việc xử lý vi phạm quy định bảo đảm an toàn thông tin và trách nhiệm bồi thường thiệt hại do hành vi vi phạm của bên cung cấp dịch vụ gây ra.

2. Trách nhiệm của Phòng Công tác học sinh, sinh viên trong quá trình sử dụng dịch vụ công nghệ thông tin

a) Yêu cầu bên cung cấp dịch vụ phải bảo mật thông tin, dữ liệu, mã nguồn, tài liệu thiết kế; triển khai các biện pháp bảo đảm an toàn thông tin theo

quy định tại Quy chế này, Luật An toàn thông tin mạng, Luật An ninh mạng và các quy định khác có liên quan.

b) Giám sát chặt chẽ và giới hạn quyền truy cập của bên cung cấp dịch vụ khi cho phép truy cập vào hệ thống thông tin của cơ quan, đơn vị.

c) Khi phát hiện bên cung cấp dịch vụ có dấu hiệu vi phạm quy định bảo đảm an toàn thông tin

- Báo cáo Lãnh đạo Sở, tạm dừng hoặc đình chỉ hoạt động của bên cung cấp dịch vụ tùy theo mức độ vi phạm.

- Tham mưu Lãnh đạo Sở thông báo chính thức các hành vi vi phạm của bên cung cấp dịch vụ.

- Thu hồi ngay lập tức quyền truy cập hệ thống thông tin đã cấp cho bên cung cấp dịch vụ.

- Kiểm tra, xác định, lập báo cáo mức độ vi phạm và thiệt hại xảy ra; Tham mưu Lãnh đạo Sở thông báo cho bên cung cấp dịch vụ và tiến hành các thủ tục xử lý vi phạm và bồi thường thiệt hại.

3. Trách nhiệm các phòng thuộc Sở khi kết thúc sử dụng dịch vụ

a) Thông báo bằng văn bản cho Phòng Công tác học sinh, sinh viên thu hồi quyền truy cập hệ thống thông tin và các tài sản khác liên quan đã cấp cho bên cung cấp dịch vụ; thay đổi các khóa, mật khẩu truy cập hệ thống thông tin.

b) Phối hợp Phòng Công tác học sinh, sinh viên yêu cầu bên cung cấp dịch vụ chuyển giao đầy đủ các thông tin, dữ liệu, mã nguồn, tài liệu thiết kế và các công cụ cần thiết để bảo đảm đơn vị vẫn có thể khai thác sử dụng dịch vụ được liên tục kể cả trong trường hợp thay đổi bên cung cấp dịch vụ.

Điều 8. Xác định cấp độ và phương án bảo đảm an ninh mạng, an toàn thông tin hệ thống thông tin

Phòng Công tác học sinh, sinh viên tham mưu thực hiện bảo đảm an ninh mạng, an toàn thông tin cấp độ cho các hệ thống thông tin theo quy định tại Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ; Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 của Chính phủ quy định chi tiết một số điều của Luật An ninh mạng và Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Chính phủ quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

Điều 9. Ứng cứu sự cố an toàn hệ thống thông tin

1. Nguyên tắc ứng cứu xử lý sự cố

a) Chủ động, kịp thời, nhanh chóng, chính xác, đồng bộ và hiệu quả.

b) Phối hợp chặt chẽ, tuân thủ quy định của pháp luật về điều phối, ứng cứu sự cố an toàn thông tin mạng.

c) Ưu tiên ứng cứu, xử lý sự cố bằng lực lượng tại chỗ và trách nhiệm chính của chủ quản hệ thống thông tin, đơn vị vận hành hệ thống thông tin.

d) Việc xử lý sự cố an toàn thông tin mạng phải bảo đảm quyền và lợi ích hợp pháp của tập thể, cá nhân; bảo mật thông tin cá nhân, thông tin riêng của cơ quan khi tham gia các hoạt động ứng cứu xử lý sự cố.

2. Phân loại sự cố an toàn thông tin mạng

a) Sự cố do bị tấn công mạng: tấn công từ chối dịch vụ; tấn công giả mạo; tấn công sử dụng mã độc; tấn công truy cập trái phép, chiếm quyền điều khiển; tấn công thay đổi giao diện; tấn công mã hóa phần mềm, dữ liệu, thiết bị; tấn công phá hoại thông tin, dữ liệu, phần mềm; tấn công nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu; các hình thức tấn công khác.

b) Sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật.

c) Sự cố do lỗi của cán bộ quản trị, vận hành hệ thống.

d) Sự cố do các thảm họa tự nhiên.

3. Phân loại mức độ sự cố

a) Thấp: sự cố gây ảnh hưởng cá nhân và không làm gián đoạn hay đình trệ hoạt động chính của cơ quan.

b) Trung bình: sự cố ảnh hưởng đến một nhóm người dùng nhưng không gây gián đoạn hay đình trệ hoạt động chính của cơ quan.

c) Cao: sự cố tác động đến khả năng vận hành của hệ thống thông tin, ảnh hưởng đến dữ liệu, thiết bị, gây ảnh hưởng đến hoạt động chung của cơ quan và hoạt động cung cấp dịch vụ công cho người dân, doanh nghiệp.

d) Nghiêm trọng: sự cố gây gián đoạn hoặc đình trệ hệ thống trong một khoảng thời gian ngắn, ảnh hưởng nghiêm trọng đến dữ liệu, thiết bị của hệ thống, gây thiệt hại nghiêm trọng cho cơ quan, người dân, doanh nghiệp.

đ) Đặc biệt nghiêm trọng: sự cố làm tê liệt toàn bộ hoạt động của hệ thống, gây thiệt hại đặc biệt nghiêm trọng cho cơ quan, người dân, doanh nghiệp, đe dọa trật tự an toàn xã hội.

4. Quy trình ứng cứu sự cố thực hiện theo Điều 11 Thông tư số 20/2017/TT-BTTTT.

5. Trường hợp có sự cố ở mức độ cao trở lên hoặc vượt quá khả năng khắc phục của đơn vị, lãnh đạo phòng thuộc Sở phải báo cáo khẩn cấp cho Lãnh đạo Sở (qua Phòng Công tác học sinh, sinh viên) để được hướng dẫn, hỗ trợ hoặc điều phối ứng cứu sự cố an toàn thông tin mạng.

6. Quá trình xử lý sự cố phải được ghi chép và lưu trữ tại đơn vị; bảo toàn bằng chứng, chứng cứ phục vụ cho việc kiểm tra, xử lý, khắc phục và phòng ngừa sự cố. Trong trường hợp sự cố có liên quan đến các vi phạm pháp luật, đơn vị có trách nhiệm thu thập và cung cấp chứng cứ cho cơ quan có thẩm quyền theo quy định của pháp luật.

Điều 10. Quản lý rủi ro, lỗ hổng, điểm yếu an ninh mạng, an toàn thông tin

1. Phòng Công tác học sinh, sinh viên làm đầu mối chủ trì, phối hợp với các tổ chức, cá nhân có liên quan để tổ chức quản lý lỗ hổng, điểm yếu an toàn an ninh mạng

a) Lập danh sách toàn bộ thiết bị, phần mềm công nghệ thông tin đang sử dụng trong phạm vi quản lý của Sở Giáo dục và Đào tạo, bao gồm: nhãn hiệu phần cứng, tên phần mềm và phiên bản (hệ điều hành, cơ sở dữ liệu, ứng dụng, các tiện ích khác).

b) Tiếp nhận thông tin về lỗ hổng, điểm yếu an toàn an ninh mạng từ các cơ quan, tổ chức có chức năng cảnh báo về an toàn an ninh mạng.

c) Quản lý, giám sát việc cài đặt bản vá lỗ hổng, điểm yếu an toàn an ninh mạng. Triển khai cài đặt bản vá lỗ hổng, điểm yếu an toàn an ninh mạng sau khi bản vá được phát hành; Áp dụng các biện pháp bảo vệ tạm thời trong trường hợp bản vá bảo mật chưa được phát hành hoặc chưa đủ điều kiện để triển khai.

2. Các phòng thuộc Sở phối hợp với Phòng Công tác học sinh, sinh viên triển khai quản lý rủi ro an toàn, an ninh mạng trên cơ sở quản lý lỗ hổng, điểm yếu an toàn an ninh mạng theo quy định tại khoản 1 Điều này và theo hướng dẫn của các cơ quan có liên quan.

3. Trên cơ sở báo cáo kết quả kiểm tra, đánh giá an toàn thông tin mạng hoặc cảnh báo nguy cơ gây mất an toàn thông tin mạng từ Công an tỉnh hoặc các cơ quan có thẩm quyền khác, Phòng Công tác học sinh, sinh viên có trách nhiệm tự khắc phục hoặc lựa chọn đơn vị đủ năng lực để triển khai các phương án khắc phục. Kết thúc xử lý, tham mưu Lãnh đạo Sở báo cáo kết quả thực hiện về cấp có thẩm quyền để theo dõi, tổng hợp theo quy định.

Điều 11. Đào tạo, bồi dưỡng nghiệp vụ, tuyên truyền, phổ biến nâng cao nhận thức về an ninh mạng, an toàn thông tin

1. Phòng Công tác học sinh, sinh viên chủ trì tổ chức đào tạo, bồi dưỡng nghiệp vụ về an ninh mạng, an toàn thông tin cho cán bộ công nghệ thông tin, an ninh mạng, an toàn thông tin, cán bộ phụ trách chuyển đổi số các đơn vị trực thuộc; đào tạo cơ bản về an toàn thông tin cho cán bộ quản lý, người sử dụng máy tính thuộc cơ quan Sở.

2. Các đơn vị phải thường xuyên tổ chức các hoạt động tuyên truyền, phổ biến nâng cao nhận thức về bảo đảm an ninh mạng, an toàn thông tin đến toàn thể cán bộ, công chức, viên chức và người lao động tại đơn vị.

Chương III

TRÁCH NHIỆM BẢO ĐẢM AN NINH MẠNG, AN TOÀN THÔNG TIN

Điều 12. Trách nhiệm của các phòng thuộc Sở

1. Trưởng các phòng có trách nhiệm tổ chức thực hiện các quy định tại Quy chế này và chịu trách nhiệm trước Giám đốc Sở trong công tác bảo đảm an ninh mạng, an toàn thông tin của đơn vị.

2. Thường xuyên tổ chức quán triệt các quy định về an ninh mạng, an toàn thông tin trong đơn vị; xác định các yêu cầu, trách nhiệm bảo đảm an ninh mạng, an toàn thông tin đối với các vị trí việc làm tại đơn vị.

3. Phối hợp, cung cấp thông tin và tạo điều kiện cho các đơn vị có thẩm quyền triển khai công tác kiểm tra khắc phục sự cố an ninh mạng, an toàn thông tin kịp thời, nhanh chóng và đạt hiệu quả.

4. Phối hợp chặt chẽ với các đơn vị liên quan trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an ninh mạng, an toàn thông tin.

5. Phòng Công tác học sinh, sinh viên

- Tham mưu hồ sơ, văn bản gửi cơ quan có thẩm quyền xác định cấp độ an toàn hệ thống thông tin theo quy định tại Nghị định số 85/2016/NĐ-CP.

- Thực hiện bảo vệ hệ thống thông tin theo Quy chế này, các quy định của pháp luật và hướng dẫn, tiêu chuẩn, quy chuẩn an toàn thông tin.

- Định kỳ hoặc đột xuất báo cáo công tác thực thi bảo đảm an toàn hệ thống thông tin theo yêu cầu của Ủy ban nhân dân tỉnh và cơ quan quản lý nhà nước chuyên ngành có thẩm quyền.

- Chủ trì tham mưu Lãnh đạo Sở thực hiện theo yêu cầu của cơ quan chức năng liên quan trong công tác bảo đảm an ninh mạng, an toàn thông tin.

- Kịp thời thông báo sự cố an ninh mạng, an toàn thông tin và phối hợp ứng cứu xử lý sự cố an ninh mạng, an toàn thông tin với các cơ quan, đơn vị liên quan.

Điều 13. Trách nhiệm của cán bộ, công chức, viên chức và người lao động

1. Trách nhiệm của cán bộ, công chức, viên chức và người lao động

a) Chấp hành Quy chế này và các quy định của pháp luật về an ninh mạng, an toàn thông tin. Chịu trách nhiệm bảo đảm an ninh mạng, an toàn thông tin trong phạm vi trách nhiệm và quyền hạn được giao.

b) Cán bộ, công chức, viên chức và người lao động có trách nhiệm tự quản lý, bảo quản, bảo đảm an ninh mạng, an toàn thông tin cho tài khoản, các thiết bị mà mình được giao sử dụng;

c) Khi phát hiện sự cố mất an ninh mạng, an toàn thông tin phải thông báo ngay với Lãnh đạo Phòng để kịp thời ngăn chặn, xử lý;

d) Tham gia nghiêm túc các chương trình đào tạo, tập huấn về an ninh mạng, an toàn thông tin do cơ quan chuyên trách về an ninh mạng, an toàn thông tin tổ chức.

2. Trách nhiệm của cán bộ phụ trách công nghệ thông tin/an toàn thông tin: Ngoài các quy định tại Khoản 1 Điều này, cán bộ phụ trách công nghệ thông tin/an toàn thông tin có trách nhiệm

a) Chủ trì tham mưu với Lãnh đạo Sở thực hiện các quy định của Quy chế này và các quy định pháp luật có liên quan đến an ninh mạng, an toàn thông tin.

b) Tham mưu Lãnh đạo Sở ban hành các quy định nội bộ và triển khai các giải pháp kỹ thuật bảo đảm an ninh mạng, an toàn thông tin.

c) Trực tiếp thiết lập hoặc tham mưu các biện pháp kỹ thuật bảo đảm an toàn cho hạ tầng kỹ thuật, hệ thống thông tin trong cơ quan; hướng dẫn cán bộ, công chức, viên chức và người lao động trong cơ quan tuân thủ các biện pháp bảo đảm an ninh mạng, an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin;

d) Thực hiện việc giám sát, đánh giá, ghi nhật ký và báo cáo ngay Lãnh đạo Sở các sự cố mất an ninh mạng, an toàn thông tin và mức độ nghiêm trọng của các sự cố đó;

đ) Phối hợp với cá nhân, đơn vị có liên quan trong việc kiểm soát, phát hiện và khắc phục các sự cố an ninh mạng, an toàn thông tin.

Chương IV

TỔ CHỨC THỰC HIỆN

Điều 14. Kinh phí thực hiện

Kinh phí bảo đảm an ninh mạng, an toàn thông tin được bố trí từ nguồn ngân sách nhà nước theo phân cấp ngân sách hiện hành; lồng ghép với kinh phí thực hiện các Chương trình, Kế hoạch, Đề án khác có liên quan và các nguồn kinh phí huy động hợp pháp khác (nếu có) theo quy định của pháp luật.

Điều 15. Chế độ, nội dung báo cáo, khen thưởng, kỷ luật

1. Phòng Công tác học sinh, sinh viên chủ trì, tham mưu báo cáo tình hình an ninh mạng, an toàn thông tin theo quy định tại Khoản 1, Khoản 2 Điều 20 Quy chế bảo đảm an ninh mạng, an toàn thông tin đối với hệ thống thông tin trên địa bàn tỉnh Ninh Bình ban hành kèm theo Quyết định số 14/2026/QĐ-UBND ngày 30/01/2026 của Ủy ban nhân dân tỉnh Ninh Bình.

2. Hàng năm, Văn phòng căn cứ kết quả kiểm tra, đánh giá, báo cáo công tác bảo đảm an ninh mạng, an toàn thông tin của các cơ quan, đơn vị đề xuất Giám đốc Sở xem xét khen thưởng cho các cá nhân, đơn vị có nhiều thành tích trong công tác bảo đảm an ninh mạng, an toàn thông tin theo quy định hiện hành.

3. Các tập thể, cá nhân có hành vi vi phạm quy chế này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý theo quy định hiện hành.

Điều 16. Công tác kiểm tra

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

Điều 17. Tổ chức thực hiện

1. Trưởng các phòng thuộc Sở có trách nhiệm triển khai thực hiện, phổ biến, quán triệt đến toàn bộ cán bộ, công chức, viên chức, người lao động trong đơn vị Quy chế này; thường xuyên kiểm tra việc thực hiện Quy chế tại đơn vị; chịu trách nhiệm trước pháp luật và trước Giám đốc Sở về các vi phạm, thất thoát thông tin, dữ liệu thuộc phạm vi quản lý của đơn vị.

2. Phòng Công tác học sinh, sinh viên có trách nhiệm theo dõi, đôn đốc, kiểm tra, đánh giá việc thực hiện Quy chế, tham mưu báo cáo UBND tỉnh định kỳ hằng năm hoặc đột xuất theo yêu cầu.

Điều 18. Sửa đổi, bổ sung Quy chế

Trong quá trình thực hiện Quy chế, nếu có khó khăn, vướng mắc, phát sinh cần sửa đổi, bổ sung, đề nghị các đơn vị kịp thời báo cáo Giám đốc Sở (qua phòng Công tác học sinh, sinh viên) để xem xét, điều chỉnh cho phù hợp./.