Số: 68/QĐ-SGDĐT; 14/02/2025; 10:34:39;

UBND TỈNH NAM ĐỊNH
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 TOÀN HỆ THỐNG THÔNG TIN MẠNG NỘI BỘ CỦA SỞ GIÁO DỤC VÀ ĐÀO TẠO TỈNH NAM ĐỊNH

(Kèm theo Quyết định /QĐ-SGDĐT ngày / /2025 của Sở GDĐT)

CHƯƠNG I
NHỮNG QUY ĐỊNH CHUNG

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

1. Phạm vi điều chỉnh:

Quy chế này quy định về bảo đảm an toàn hệ thống thông tin Mạng máy tính, mạng nội bộ, Email công vụ. Áp dụng cho hệ thống mạng của Sở và các đơn vị thuộc Sở.

2. Đối tượng áp dụng:

Quy chế này áp dụng đối với công chức, viên chức và người lao động công tác tại các phòng, đơn vị thuộc Sở trong việc quản lý, sử dụng hệ thống mạng nội bộ (LAN), mạng Internet, Hệ thống Email công vụ của Sở.

Điều 2. Giải thích từ ngữ:

1. Thiết bị công nghệ thông tin: Là toàn bộ các trang thiết bị có liên quan đến công nghệ thông tin (CNTT) như: Máy tính (PC, Laptop, Sever), máy in, máy quét, máy chiếu, các loại ổ ghi đĩa CD, VCD, DVD, ổ cứng, thẻ nhớ (USB), camera số, máy ảnh số, thiết bị chuyển mạch (hub, switch), tường lửa (firewall), modem, hệ thống cáp mạng.

2. Tài nguyên mạng: Là toàn bộ các phần mềm dùng chung chạy trên mạng nội bộ của Sở, gồm: Trang thông tin điện tử, các phần mềm dùng chung của UBND tỉnh và Bộ GDĐT (nếu có), Email công vụ, các phần mềm được cài đặt trên hệ thống máy tính, các phần mềm chuyên môn, chuyên ngành...

3. Email: là thông điệp dữ liệu được gửi đến một hoặc nhiều địa chỉ Email thông qua cơ sở hạ tầng thông tin.

4. Người sử dụng: Công chức, viên chức và người lao động Sở Giáo dục và Đào tạo, sử dụng các thiết bị CNTT; được cấp tài khoản (Account) gồm tên người

sử dụng (Username) và mật khẩu (Password) để khai thác mạng LAN và các tài nguyên mạng nội bộ của Sở thông qua mạng LAN, mạng Internet.

5. Quản trị mạng: Là công chức/viên chức được giao nhiệm vụ quản lý hệ thống thiết bị CNTT, duy trì sự hoạt động mạng máy tính nội bộ tại Phòng Giáo dục Chính trị và Công tác học sinh, sinh viên thuộc Sở Giáo dục và Đào tạo; hướng dẫn người sử dụng thiết bị CNTT và khai thác tài nguyên mạng phục vụ công tác.

Điều 3. Mục tiêu, nguyên tắc bảo đảm an toàn thông tin

1. Mục tiêu:

Mục tiêu bảo đảm an toàn thông tin là bảo vệ thông tin, hệ thống thông tin tránh bị truy cập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của hệ thống thông tin.

2. Nguyên tắc:

a) Hoạt động ứng dụng công nghệ thông tin thực hiện các nguyên tắc bảo đảm an toàn thông tin mạng được quy định tại Điều 4 Luật an toàn thông tin mạng năm 2015 và Điều 41 Nghị định số 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước.

b) Bảo đảm an toàn thông tin (ATTT) là yêu cầu bắt buộc, phải được thực hiện thường xuyên, liên tục, kịp thời và hiệu quả.

c) Thu thập, tạo lập, xử lý, truyền tải, lưu trữ và sử dụng thông tin, dữ liệu; Thiết kế, thiết lập và vận hành, nâng cấp, hủy bỏ 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 tổ chức, cá nhân, không xâm phạm đến đời sống riêng tư, bí mật cá nhân, bí mật gia đình của cá nhân, thông tin riêng của tổ chức.

3. Tài nguyên thông tin cần đảm bảo an toàn thông tin

3.1. Hệ thống hạ tầng kỹ thuật:

a) Thiết bị lưu trữ (máy chủ, máy trạm, ...).

b) Thiết bị ngoại vi (máy in, máy quét và các thiết bị số hoá, camera, thiết bị lưu trữ dữ liệu di động, ...).

c) Đường truyền dữ liệu, đường kết nối Internet.

d) Mạng nội bộ (LAN), thiết bị kết nối mạng, thiết bị bảo mật và thiết bị phụ trợ.

đ) Thiết bị công nghệ thông tin khác được kết nối mạng trong các cơ quan, đơn vị.

3.2. Hệ thống thông tin, phần mềm, ứng dụng và cơ sở dữ liệu:

a) Hệ thống thông tin, nền tảng số, cơ sở dữ liệu dùng chung (email, quản lý văn bản và điều hành, thông tin nội bộ, quản lý nhân sự và thi đua khen thưởng, quản lý tài sản, hồ sơ hành chính điện tử, dữ liệu thống kê tổng hợp, ...).

b) Phần mềm, ứng dụng cung cấp dịch vụ công trực tuyến.

c) Cổng trang thông tin điện tử của Sở.

d) Hệ thống thông tin nghiệp vụ và các cơ sở dữ liệu chuyên ngành.

đ) Phần mềm, ứng dụng phục vụ công tác quản lý, điều hành hoạt động của cơ quan Nhà nước.

3.3. Thông tin, dữ liệu được trao đổi, truyền tải, xử lý và lưu trữ tại hệ thống thông tin của Sở.

Điều 4. Nguồn nhân lực bảo đảm an toàn thông tin

1. Quy định đối với công tác tuyển dụng:

Cán bộ được tuyển dụng vào vị trí làm về an toàn thông tin cần 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 về việc thực hiện đảm bảo an toàn thông tin trong quá trình làm việc:

Trách nhiệm bảo đảm an toàn thông tin đối với người sử dụng, cán bộ quản lý và vận hành hệ thống.

a) Với người sử dụng:

- Người sử dụng có trách nhiệm đảm bảo ATTT đối với từng vị trí công việc. Trước khi tham gia vào hệ thống phải được kiểm tra khả năng đáp ứng các yêu cầu về ATTT.

- Phải được thường xuyên tổ chức quán triệt các quy định về ATTT, nhằm nâng cao nhận thức về trách nhiệm đảm bảo ATTT.

- Cá nhân, tổ chức phải có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng; không tự ý thay đổi, tháo lắp thiết bị.

b) Với cán bộ quản lý và vận hành hệ thống

- Cán bộ chuyên trách phải thiết lập phương pháp hạn chế truy cập mạng không dây, giám sát và điều khiển truy cập không dây, tổ chức sử dụng chứng thực và mã hoá để bảo vệ truy cập không dây tới hệ thống thông tin.

- Các phòng ban, đơn vị và các tổ chức, cá nhân tham gia sử dụng các dịch vụ của hệ thống phải tuân thủ các quy định về bảo đảm an toàn, an ninh thông tin và

chịu trách nhiệm đối với mọi hoạt động trên tài khoản truy cập của mình đã được cấp trên hệ thống.

3. Quy định đối với công chức, viên chức và người lao động nghỉ chế độ hoặc thay đổi công việc:

a) Khi công chức, viên chức và người lao động chấm dứt hoặc thay đổi công việc, các tài khoản truy cập hệ thống, thông tin lưu trữ trên phương tiện lưu trữ (Email công vụ) sẽ được đóng và các thiết bị, máy móc, tài sản có liên quan được phân cho cán bộ khác tiếp quản.

b) Cán bộ quản trị phải vô hiệu hoá tất cả các quyền ra, vào, truy cập tài khoản, quản trị hệ thống sau khi cán bộ thôi việc.

CHƯƠNG II
ĐẢM BẢO AN TOÀN THÔNG TIN TRONG THIẾT KẾ, XÂY DỰNG HỆ THỐNG THÔNG TIN

Điều 5. Thiết kế, xây dựng hệ thống thông tin cần bảo đảm các yêu cầu:

1. Xây dựng tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin và thuyết minh trong hồ sơ đề xuất cấp độ của hệ thống.

2. Xây dựng tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin thuyết minh trong hồ sơ đề xuất cấp độ của hệ thống.

3. Bộ phận chuyên trách xây dựng tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ của hệ thống thông tin thuyết minh trong hồ sơ đề xuất cấp độ của hệ thống.

4. Bộ phận chuyên trách xây dựng tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin của hệ thống thông tin thuyết minh trong hồ sơ đề xuất cấp độ của hệ thống.

5. Bộ phận chuyên trách khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống, báo cáo Lãnh đạo quyết định trước khi thực hiện thay đổi.

6. Các yêu cầu về mặt kỹ thuật để bảo đảm việc thiết kế, xây dựng và thiết lập hệ thống thông tin bảo đảm an toàn. Các yêu cầu kỹ thuật được chia thành các nhóm yêu cầu: bảo đảm an toàn mạng; bảo đảm an toàn máy chủ; bảo đảm an toàn ứng dụng; bảo đảm an toàn dữ liệu.

Điều 6. Đối với phát triển phần mềm thuê khoán cần đáp ứng:

1. Có điều khoản hợp đồng, biên bản và các cam kết đối với bên thuê khoán khi thực hiện các nội dung liên quan đến việc phát triển phần mềm thuê khoán.

2. Bộ phận chuyên trách có trách nhiệm quản lý và lưu trữ mã nguồn an toàn.

3. Các nhà phát triển cung cấp mã nguồn phần mềm.

a) Các nhà phát triển cung cấp mã nguồn phần mềm cho bộ phận chuyên trách.

b) Phần mềm thuê khoán phải được kiểm thử phần mềm trên môi trường thử nghiệm trước khi đưa vào sử dụng.

c) Phần mềm thuê khoán phải được kiểm tra, đánh giá an toàn thông tin, trước khi đưa vào sử dụng.

Điều 7. Thử nghiệm và nghiệm thu hệ thống

1. Thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng;

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

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

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

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

CHƯƠNG III
ĐẢM BẢO AN TOÀN THÔNG TIN TRONG QUẢN LÝ, VẬN HÀNH HỆ THỐNG THÔNG TIN

Điều 8. Hệ thống Email công vụ của Sở

1. Hệ thống Email công vụ của Sở là hệ thống thông tin dùng chung cung cấp dịch vụ Email phục vụ công vụ cho các đơn vị, cá nhân thuộc Sở.

2. Hệ thống Email công vụ của tỉnh Nam Định có tên miền là @namdinh.gov.vn và địa chỉ truy cập trên Internet là https: //mail.namdinh.gov.vn.

Điều 9. Quản lý an toàn mạng

1. Quản lý, vận hành hoạt động bình thường của hệ thống:

a) Việc bật, tắt máy tính, máy in,... phải thực theo hướng dẫn sử dụng thiết bị, hạn chế tối đa việc tắt đột ngột thiết bị.

b) Cấu hình mạng, vị trí thiết bị, quy định địa chỉ IP, tên máy trạm, máy chủ, nhóm làm việc (Workgroup), vùng làm việc (Domain) được quy định và thống nhất tại đơn vị mình quản lý do cán bộ quản trị mạng thiết lập.

c) Các thông tin khi di chuyển từ ổ đĩa ngoài, USB, đĩa CD, VCD, DVD và các thư điện tử trước khi tải về phải kiểm tra, quét virus.

d) Không truy cập các trang web không biết rõ nguồn gốc. Nghiêm cấm mọi hành vi cài đặt hoặc phát tán virus vào hệ thống máy tính.

đ) Hoạt động của hệ thống phải được giám sát thường xuyên, liên tục, bảo đảm tính khả dụng của hệ thống.

e) Toàn bộ cấu hình hệ thống phải được sao lưu, dự phòng trên thiết bị hoặc hệ thống lưu trữ độc lập, định kỳ 01 tháng/lần.

g) Khi thực hiện nâng cấp, thay đổi cấu hình hệ thống phải thực hiện ngoài giờ làm việc.

h) Phải kiểm tra hoạt động tổng thể của hệ thống sau khi thay đổi cấu hình hoặc nâng cấp hệ thống.

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

a) Định kỳ hàng tháng hoặc khi có thay đổi, bộ phận chuyên trách thực hiện sao lưu, dự phòng hệ thống trên hệ thống độc lập như USB, DVD hoặc SAN.

b) Các dữ liệu cần sao lưu, dự phòng: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

3. Truy cập và quản lý cấu hình hệ thống.

a) Cấu hình hệ thống từ xa phải sử dụng các giao thức bảo mật có mã hóa thông tin như SSL, TSL, SSH, VPN.

b) Khi cấu hình hệ thống từ bên ngoài phải thông qua kết nối VPN.

c) Toàn bộ cấu hình hệ thống phải được lưu trên thiết bị hoặc hệ thống lưu trữ độc lập.

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

đ) Hệ thống mạng phải được thiết lập cấu hình để: Kiểm soát truy cập từ bên ngoài mạng; Kiểm soát truy cập từ bên trong mạng; Kết nối về hệ thống giám sát tập trung; Phòng chống xâm nhập giữa các vùng mạng; Phòng chống phần mềm độc hại trên môi trường mạng.

e) Việc cài đặt, kết nối và gỡ bỏ thiết bị mạng trong hệ thống phải được cho phép bởi người có thẩm quyền và thực hiện theo quy trình được phê duyệt.

4. Các thiết bị trong hệ thống cần được cấu hình tối ưu, tăng cường bảo mật, ưu tiên sử dụng thiết bị chuyên dụng trước khi đưa vào vận hành, khai thác.

Điều 10. Quản lý an toàn máy chủ và ứng dụng

1. Quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ:

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

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

c) Quản lý các thay đổi cấu hình kỹ thuật của hệ điều hành, phần mềm.

d) Thường xuyên cập nhật các bản vá lỗi hệ điều hành, phần mềm từ nhà cung cấp.

đ) Loại bỏ các thành phần của hệ điều hành, phần mềm không cần thiết hoặc không còn nhu cầu sử dụng.

e) Phần mềm bản quyền cần được theo dõi quản lý thời gian sử dụng đảm bảo cho việc gia hạn đúng thời gian.

2. Truy cập mạng của máy chủ:

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

3. Truy cập và quản trị máy chủ và ứng dụng:

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

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

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

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

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

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

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

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

a) Triển khai hệ thống/phương tiện lưu trữ độc lập với hệ thống lưu trữ trên các máy chủ dịch vụ để sao lưu dự phòng.

b) 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.

5. Cài đặt, gỡ bỏ hệ điều hành, dịch vụ, phần mềm trên hệ thống máy chủ và ứng dụng.

6. Kết nối và gỡ bỏ hệ thống máy chủ và dịch vụ khỏi hệ thống.

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

Điều 11. Quản lý an toàn dữ liệu

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

a) Đơn vị phải áp dụng quy định sử dụng các phương thức mã hóa thích hợp

theo các chuẩn quốc gia hoặc quốc tế đã được công nhận để bảo vệ thông tin.

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

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

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

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

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

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

7. Định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ và các thông tin, dữ liệu quan trọng khác trên hệ thống (nếu có).

Điều 12. Quản lý an toàn thiết bị đầu cuối

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

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

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

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

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

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

Điều 13. Quản lý phòng chống phần mềm độc hại

1. Tất cả các máy trạm, máy chủ phải được trang bị phần mềm phòng chống mã độc đáp ứng yêu cầu tại Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ.

2. Khi phát hiện ra bất kỳ dấu hiện nào liên quan đến việc bị nhiễm mã độc trên máy trạm (ví dụ: máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống mã độc, mất dữ liệu, …), người sử dụng phải báo trực tiếp cho bộ phận có trách nhiệm của đơn vị để xử lý.

3. Phần mềm ứng dụng trước khi được cài đặt, sử dụng phải được kiểm tra xem có phần mềm độc hại tồn tại hay không? Tất cả các tập tin, thư mục phải được quét mã độc trước khi sao chép, sử dụng.

4. Định kỳ hàng năm thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống; thực hiện kiểm tra và xử lý phần mềm độc hại khi phát hiện dấu hiệu hoặc cảnh báo về dấu hiệu phần mềm độc hại xuất hiện trên hệ thống.

Điều 14. Quản lý điểm yếu an toàn thông tin

1. Thường xuyên phổ biến, quán triệt và cập nhật những quy định về an toàn thông tin và hướng dẫn công chức, viên chức, người lao động thực hiện đúng hướng dẫn về an toàn, an ninh thông tin nhằm nâng cao nhận thức và trách nhiệm về an toàn thông tin.

2. Hạn chế việc sử dụng chức năng chia sẻ tài nguyên, khi sử dụng chức năng này cần bật thuộc tính bảo mật bằng mật khẩu và thu hồi chức năng này khi đã sử dụng xong. Đối với các đơn vị có mạng máy tính thuộc mạng cục bộ (LAN) thì tuyệt đối không được tự ý kết nối thêm các máy tính, thiết bị ngoại vi (máy tính xách tay, thiết bị lưu trữ di động, bộ phát sóng wifi…) vào hệ thống mạng của cơ quan đơn vị khi chưa đảm bảo điều kiện an ninh. Không được sử dụng các loại thiết bị lưu trữ ngoài để sao chép, lưu trữ các tài liệu quan trọng, đặc biệt là các thiết bị lạ, chưa được kiểm soát.

3. Các máy tính cá nhân khi không sử dụng trong thời gian dài (quá 4 giờ làm việc) cần tắt máy để tránh bị các tin tặc lợi dụng tấn công vào hệ thống thông tin của máy tính. Máy tính cá nhân phải được cài đặt phần mềm diệt virus có bản quyền.

4. Khai thác tài nguyên Internet có chọn lọc, không vào các trang web lạ, không bấm vào các đường liên kết, biểu tượng quảng cáo không rõ nội dung và không cài đặt phần mềm không rõ nguồn gốc.

5. Phải đặt mật khẩu cho máy tính (mật khẩu đăng nhập, mật khẩu bảo vệ màn hình), Sử dụng các thiết bị lưu trữ thông tin (USB, Thẻ nhớ…) đảm bảo an toàn, đúng cách để phòng ngừa vi rút, phần mềm gián điệp xâm nhập máy tính phá hoại, đánh cắp thông tin.

6. Quản lý thông tin điểm yếu an toàn thông tin đối với từng thành phần có trong hệ thống (hệ điều hành, máy chủ, ứng dụng, dịch vụ…); phân loại mức độ nguy hiểm của điểm yếu; xây dựng phương án và quy trình xử lý đối với từng mức độ nguy hiểm của điểm yếu.

7. Báo cáo Lãnh đạo/Cán bộ quản lý ngay khi phát hiện điểm yếu an toàn

thông tin ở mức độ nghiêm trọng. Thực hiện cảnh báo và xử lý điểm yếu an toàn thông tin theo chỉ đạo. Việc xử lý điểm yếu an toàn thông tin phải bảo đảm không làm ảnh hưởng/gián đoạn hoạt động của hệ thống.

8. Có trách nhiệm phối hợp với các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục điểm yếu an toàn thông tin đối với các điểm yếu khi cần thiết.

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

10. Định kỳ 1 năm kiểm tra, đánh giá điểm yếu an toàn thông tin cho toàn bộ hệ thống thông tin; Thực hiện quy trình kiểm tra, đánh giá, xử lý điểm yếu an toàn thông tin khi có thông tin hoặc nhận được cảnh báo về điểm yếu an toàn thông tin đối với thành phần cụ thể trong hệ thống.

Điều 15. Quản lý giám sát an toàn hệ thống thông tin

1. Triển khai hệ thống giám sát trung tâm phải đáp ứng yêu cầu tại khoản 1, Điều 5 Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ Thông tin và truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin.

2. Thông tin giám sát và danh mục các đối tượng giám sát phải đáp ứng yêu cầu tại khoản 2, Điều 5 Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ Thông tin và truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin

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

4. Thực thi nhiệm vụ giám sát theo quy định tại khoản 3, Điều 5 Thông tư số 31/2017/TT-BTTTT.

Điều 16. Quản lý sự cố an toàn thông tin

1. Phân nhóm sự cố an toàn thông tin mạng theo quy định tại Quyết định số 05/2017/QĐ-TTg của Thủ tướng Chính phủ ngày 16/3/2017 quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia (Quyết định 05).

2. Quyết định toàn diện về mặt kỹ thuật đối với các cơ quan trong quá trình khắc phục sự cố về ATTT; Hỗ trợ, phối hợp và hướng dẫn các cơ quan khắc phục sự cố mất ATTT; Yêu cầu ngưng hoạt động một phần hoặc toàn bộ các hệ thống thông tin của các cơ quan nhằm phục vụ công tác khắc phục sự cố về ATTT; Phối hợp với đơn vị chức năng trong điều tra các nguyên nhân gây ra sự cố mất an toàn thông tin theo chỉ đạo của Lãnh đạo.

3. Phòng Giáo dục Chính trị và Công tác học sinh sinh viên phối hợp với cơ

quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an toàn thông tin; Yêu cầu bên cung cấp, hỗ trợ cung cấp quy trình xử lý sự cố cho các dịch vụ do bên cung cấp, hỗ trợ cung cấp liên quan đến hệ thống.

Điều 17. Quản lý an toàn người sử dụng đầu cuối

1. Kết nối máy tính/thiết bị đầu cuối của người sử dụng vào hệ thống

a) Người sử dụng khi truy cập, sử dụng tài nguyên nội bộ, truy cập mạng và tài nguyên trên Internet phải tuân thủ các quy định của pháp luật về bảo đảm an toàn thông tin và các quy định của cơ quan, tổ chức.

b) Khi cài đặt, kết nối máy tính/thiết bị đầu cuối phải thực hiện theo hướng dẫn/quy trình dưới sự giám sát của bộ phận chuyên trách về an toàn thông tin.

c) Máy tính/thiết bị đầu cuối phải được xử lý điểm yếu an toàn thông tin, cấu hình cứng hóa bảo mật trước khi kết nối vào hệ thống.

2. Trong quá trình sử dụng

a) Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác của pháp luật về an toàn thông tin mạng. Chịu trách nhiệm bảo đảm an toàn thông tin mạng trong phạm vi trách nhiệm và quyền hạn được giao.

b) Có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng.

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

d) Tham gia các chương trình đào tạo, hội nghị về an toàn thông tin mạng được tỉnh hoặc đơn vị chuyên môn tổ chức.

Điều 18. Các hành vi nghiêm cấm khi sử dụng mạng nội bộ, Email công vụ:

1. Nghiêm cấm cắm các thiết bị lạ, truyền mạng wifi cá nhân.

2. 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.

3. 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.

4. 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.

5. Không sử dụng Email công vụ vào việc riêng.

Điều 19. Kiểm tra, đánh giá và quản lý rủi ro an toàn thông tin

1. Nội dung kiểm tra, đánh giá và quản lý rủi ro an toàn thông tin

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

b) Đánh giá hiệu quả của biện pháp bảo đảm an toàn 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 và quản lý rủi ro an toàn thông tin

a) Định kỳ theo quy định của pháp luật và kế hoạch của chủ quản hệ thống thông tin.

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

Điều 20. Phương án Kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin

1. Thiết bị CNTT có chứa dữ liệu (máy tính, thiết bị lưu trữ, ...) khi bị hỏng phải được cán bộ vận hành kiểm tra, sửa chữa, khắc phục. Phải có biện pháp kiểm tra, giám sát đảm bảo không để lọt lộ thông tin hay lây nhiễm mã độc đối với máy tính mang ra bên ngoài sửa chữa, bảo hành.

2. Trước khi tiến hành thanh lý/loại bỏ thiết bị công nghệ thông tin cũ, phải áp dụng các biện pháp kỹ thuật xoá bỏ hoàn toàn dữ liệu người dùng đã tạo ra, đảm bảo không thể phục hồi.

3. Các phương tiện và thiết bị CNTT: Máy tính cá nhân (PC), máy tính xách tay, máy chủ, các thiết bị mạng, phương tiện lưu trữ như CD/DVD, thẻ nhớ, ổ cứng phải xóa sạch dữ liệu khi chuyển giao hoặc thay đổi mục đích sử dụng.

CHƯƠNG IV
TỔ CHỨC THỰC HIỆN

Điều 21. Đơn vị chuyên trách về an toàn thông tin

1. Giao Phòng Giáo dục Chính trị và Công tác học sinh, sinh viên chịu trách nhiệm chuyên trách về an toàn thông tin, có trách nhiệm bảo đảm an toàn thông tin cho hệ thống thông tin toàn Sở. Giao Văn phòng Sở chịu trách nhiệm quản lý trang thiết bị Công nghệ thông tin tại Sở.

2. Phòng Giáo dục Chính trị và Công tác học sinh, sinh viên là đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin xử lý khi xảy ra sự cố.

a) Sở Thông tin và Truyền thông tỉnh Nam Định

- Người liên hệ/bộ phận: Trung tâm Chuyển đổi số và Truyền thông

+ Số điện thoại: 0228. 363 1116

+ Email: trungtamcntttt.nd@gmail.com

b) Cục An toàn thông tin/Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC)

- Người liên hệ/bộ phận: Phòng Ứng cứu sự cố

- Số điện thoại: 0869 100 317

- Email: ir@vncert.vn

- Báo cáo sự cố qua nền tảng điều phối, xử lý sự cố an toàn thông tin mạng quốc gia: https://irlab.vn

- Báo cáo sự cố qua website của VNCERT/CC: https://vncert.vn

3. Hướng dẫn triển khai quy chế này và các quy định về an toàn thông tin có liên quan.

4. Tham mưu thực hiện chế độ báo cáo định kỳ theo quy định của pháp luật, báo cáo đột xuất theo yêu cầu của cấp trên.

Điều 22. Tổ chức triển khai quy chế

Các đơn vị thuộc Sở có trách nhiệm triển khai thực hiện và giao Phòng Giáo dục Chính trị và Công tác học sinh, sinh viên có trách nhiệm hướng dẫn, kiểm tra, đôn đốc các đơn vị thuộc Sở tham gia sử dụng mạng máy tính thực hiện đúng theo Quy chế này. Trong quá trình thực hiện, nếu có vướng mắc, các đơn vị thuộc Sở cần phản ánh kịp thời về Văn phòng Sở và Phòng Giáo dục Chính trị và Công tác học sinh, sinh viên xem xét trước khi trình Lãnh đạo Sở cho phép bổ sung, sửa đổi Quy chế cho phù hợp với tình hình thực tế.

Điều 23. Rà soát, cập nhật, bổ sung quy chế

1. Định kỳ hàng năm hoặc khi có thay đổi chính sách an toàn thông tin Phòng Giáo dục Chính trị và Công tác học sinh, sinh viên kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung Quy chế bảo đảm an toàn thông tin.

2. Có hồ sơ lưu lại thông tin phản hồi của đối tượng áp dụng chính sách trong quá trình triển khai, áp dụng chính sách an toàn thông tin./.