UBND TỈNH KHÁNH HÒA **SỞ NỘI VỤ** Số: 238 /QĐ-SNV	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc** *Khánh Hòa, ngày 03 tháng 6 năm 2026*

QUYẾT ĐỊNH
Bảo đảm an toàn, an ninh mạng
Hệ thống thông tin phục vụ hoạt động nội bộ tại Sở Nội vụ

GIÁM ĐỐC SỞ NỘI VỤ TỈNH KHÁNH HÒA

Căn cứ Quyết định số 01/2025/QĐ-UBND ngày 11/7/2025 của Ủy ban nhân dân tỉnh về việc quy định chức năng, nhiệm vụ, quyền hạn của Sở Nội vụ tỉnh Khánh Hòa; Quyết định số 01/QĐ-UBND ngày 01 tháng 7 năm 2025 của UBND tỉnh Khánh Hòa về cơ cấu tổ chức của Sở Nội vụ tỉnh Khánh Hòa;

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

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

Căn cứ Nghị định số 356/2025/NĐ-CP ngày 31/12/2025 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Bảo vệ dữ liệu cá nhân;

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

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

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ trưởng Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Quyết định số 11/2026/QĐ-UBND ngày 31/01/2026 của Ủy ban nhân dân tỉnh Khánh Hòa về ban hành Quy chế bảo đảm an ninh mạng, an toàn thông tin trên địa bàn tỉnh Khánh Hòa;

Theo đề nghị của Chánh Văn phòng Sở Nội vụ.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn, an ninh mạng Hệ thống thông tin phục vụ hoạt động nội bộ tại Sở Nội vụ tỉnh Khánh Hòa, gồm 05 chương, 23 Điều.

Điều 2. Quyết định này có hiệu lực kể từ ngày ký và thay thế Quyết định số 83/QĐ-SNV ngày 29/7/2025 của Sở Nội vụ về việc ban hành Quy chế bảo đảm

an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin tại Sở Nội vụ Khánh Hòa.

Điều 3. Chánh Văn phòng Sở; Thủ trưởng các cơ quan, đơn vị trực thuộc Sở; công chức, viên chức và người lao động Sở Nội vụ chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận: (VBĐT)
- Như điều 3;
- UBND tỉnh *(báo cáo)*;
- Công an tỉnh *(phối hợp)*;
- Sở KHCN *(phối hợp)*;
- Lãnh đạo Sở;
- Các CQĐV trực thuộc Sở *(thực hiện)*;
- Lưu: VT, VP, TL.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ NỘI VỤ
TỈNH KHÁNH HÒA

Huỳnh Mạnh Thắng

UBND TỈNH KHÁNH HÒA
SỞ NỘI VỤ

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

QUY CHẾ
Bảo đảm an toàn, an ninh mạng
Hệ thống thông tin phục vụ hoạt động nội bộ tại Sở Nội vụ

(Kèm theo Quyết định số 238 /QĐ-SNV ngày 03/6/2026 của Sở Nội vụ)

Chương I
QUY ĐỊNH CHUNG

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

1. Phạm vi điều chỉnh

Quy chế này quy định các chính sách quản lý và các biện pháp nhằm bảo đảm an toàn thông tin cho Hệ thống thông tin phục vụ hoạt động nội bộ tại Sở Nội vụ bao gồm:

- Phạm vi quản lý về vật lý và logic của tổ chức;
- Các ứng dụng, dịch vụ hệ thống cung cấp;
- Nguồn nhân lực bảo đảm an toàn thông tin.

2. Đối tượng áp dụng

a) Tất cả công chức, viên chức; Các cơ quan, đơn vị trực thuộc Sở Nội vụ;

b) Cơ quan, đơn vị, tổ chức, cá nhân có kết nối, sử dụng Hệ thống thông tin phục vụ hoạt động nội bộ tại Sở Nội vụ.

c) Cơ quan, đơn vị, tổ chức, cá nhân cung cấp dịch vụ quản lý, vận hành, duy trì, phát triển và bảo đảm an toàn thông tin mạng phục vụ hoạt động của Hệ thống thông tin phục vụ hoạt động nội bộ tại Sở Nội vụ.

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. 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.

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.

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

1. Mục tiêu bảo đảm an toàn thông tin

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 Hệ thống thông tin phục vụ hoạt động nội bộ tại Sở Nội vụ

2. Nguyên tắc

a) Cơ quan, tổ chức thuộc đối tượng áp dụng Quy chế này có trách nhiệm bảo đảm an toàn thông tin và hệ thống thông tin trong phạm vi xử lý công việc của mình theo quy định của pháp luật, hướng dẫn của cơ quan, đơn vị có thẩm quyền và các quy định tại Quy chế này.

b) Bảo đảm an toàn thông tin (ATTT) là yêu cầu bắt buộc, phải được thực hiện thường xuyên, liên tục trong quá trình:

- 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.

c) Việc bảo đảm an toàn Hệ thống thông tin phục vụ hoạt động nội bộ tại Sở Nội vụ được thực hiện một cách tổng thể, đồng bộ, tập trung trong việc đầu tư các giải pháp bảo vệ, có sự dùng chung, chia sẻ tài nguyên để tối ưu hiệu năng, tránh đầu tư thừa, trùng lặp.

Điều 4. Những hành vi nghiêm cấm

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

Điều 5. Phối hợp với những cơ quan/tổ chức có thẩm quyền

1. Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin:

Văn phòng Sở là đầu mối liên hệ, phối hợp các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin phục vụ việc bảo đảm an toàn, an ninh mạng cho Hệ thống thông tin phục vụ hoạt động nội bộ tại Sở.

2. Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin:

a) Đội Ứng cứu sự cố an toàn thông tin mạng tỉnh:

- Số điện thoại hotline 24/7: 0694401575 hoặc 0917532787

- Số điện thoại trong giờ hành chính: 0694401575 hoặc 0917532787

- Thư điện tử: tbatanm@khanhhoa.gov.vn.

b) Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT)

- Số điện thoại hotline 24/7 Ban ứng cứu sự cố: 0692205199

- Email báo cáo sự cố: report@vncert.vn

- Báo cáo sự cố qua nền tảng điều phối, xử lý sự cố an toàn thông tin mạng quốc gia: Hệ thống điều hành an ninh mạng quốc gia: soar.soc.gov.vn

3. Tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của các cơ quan, tổ chức có thẩm quyền.

Điều 6. Bảo đảm nguồn nhân lực

1. Tuyển dụng

Cán bộ được tuyển dụng vào vị trí làm về an toàn thông tin có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, an toàn thông tin, phù hợp với vị trí tuyển dụng.

2. Trong quá trình làm việc

a) Trách nhiệm bảo đảm an toàn thông tin cho người sử dụng, công chức, viên chức quản lý và vận hành hệ thống:

- Với người sử dụng:

+ Người sử dụng có trách nhiệm đảm bảo ATTT đối với từng vị trí công việc.

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

+ 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.

- Với công chức, viên chức quản lý và vận hành hệ thống:

Công chức, viên chức quản lý và vận hành hệ thống 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 hóa để bảo vệ truy cập không dây tới hệ thống thông tin; phải tổ chức quản lý định danh đối với tất cả người dùng tham gia sử dụng hệ thống thông tin.

b) Định kỳ hàng năm tổ chức hoặc tham gia phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin cho người sử dụng do đơn vị chức năng tổ chức.

3. Chấm dứt hoặc thay đổi vị trí công tác

a) Khi công chức, viên chức, người lao động nghỉ việc, nghỉ hưu, chuyển công tác hoặc được điều động, bổ nhiệm sang vị trí khác không còn nhu cầu sử dụng quyền truy cập hệ thống, đơn vị quản lý trực tiếp có trách nhiệm phối hợp với bộ phận chuyên trách công nghệ thông tin *(hoặc an toàn thông tin, an ninh mạng)* thực hiện đầy đủ thủ tục thu hồi, bàn giao và kiểm tra các tài sản, tài nguyên thông tin đã được cấp, bao gồm:

- Tài khoản thư điện tử công vụ, tài khoản hệ thống thông tin, phần mềm nghiệp vụ, chữ ký số, thiết bị xác thực đa yếu tố (nếu có);

- Dữ liệu, hồ sơ, tài liệu điện tử được lưu trữ trên máy tính, thiết bị lưu trữ di động, tài khoản dùng chung, dùng riêng;

- Máy tính để bàn, máy tính xách tay, thiết bị lưu trữ, thiết bị mạng và các trang thiết bị công nghệ thông tin khác được cơ quan cấp phát;

- Các phần mềm, bản quyền, khóa mã hóa, tài khoản quản trị và các tài sản số khác thuộc phạm vi quản lý của cơ quan, đơn vị.

- Việc bàn giao, thu hồi phải được lập biên bản, xác nhận đầy đủ giữa cá nhân bàn giao, đơn vị quản lý trực tiếp và bộ phận chuyên trách có liên quan nhằm bảo đảm an toàn thông tin, tránh thất thoát dữ liệu và ngăn ngừa truy cập trái phép.

b) Ngay sau khi có quyết định chấm dứt công tác, điều chuyển hoặc thay đổi vị trí việc làm của công chức, viên chức, bộ phận chuyên trách công nghệ

thông tin có trách nhiệm rà soát, cập nhật và thực hiện vô hiệu hóa, thu hồi hoặc điều chỉnh toàn bộ quyền truy cập của cá nhân đối với hệ thống thông tin của cơ quan, đơn vị bao gồm:

- Quyền đăng nhập, truy cập mạng nội bộ, thư điện tử công vụ, phần mềm nghiệp vụ, cơ sở dữ liệu và các nền tảng số;

- Quyền quản trị hệ thống, quản trị cơ sở dữ liệu, quản trị thiết bị mạng, ứng dụng và các hệ thống dùng chung khác;

- Quyền truy cập từ xa (nếu có), chia sẻ dữ liệu, tài khoản dùng chung và các quyền truy cập đặc biệt khác;

- Các chứng thư số, khóa bảo mật, mã xác thực và thông tin định danh điện tử đã cấp;

Đồng thời, công chức chuyên trách về quản lý công nghệ thông tin hoặc an toàn thông tin, an ninh mạng *(sau đây gọi tắt là công chức chuyên trách)* phải kiểm tra, bảo đảm cá nhân không còn khả năng truy cập trái phép vào hệ thống thông tin, dữ liệu và tài nguyên số của cơ quan sau khi thôi việc hoặc thay đổi nhiệm vụ; trường hợp cần thiết phải thực hiện thay đổi mật khẩu quản trị, thu hồi khóa truy cập và cập nhật nhật ký quản lý tài khoản theo quy định.

Chương II
BẢO ĐẢM AN TOÀN THÔNG TIN TRONG QUẢN LÝ THIẾT KẾ, XÂY DỰNG HỆ THỐNG

Điều 7. Quản lý thiết kế an toàn hệ thống thông tin

1. Công chức chuyên trách 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;

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;

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;

Xô 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.

2. Khi có thay đổi thiết kế, công chức chuyên trách 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.

Điều 8. Phát triển phần mềm thuê khoán

1. Yêu cầu có biên bản, hợp đồng và các cam kết đối với bên thuê khoán các nội dung liên quan đến việc phát triển phần mềm thuê khoán.

2. Yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm:

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

b) Công chức chuyên trách có trách nhiệm quản lý và lưu trữ mã nguồn an toàn.

Điều 9. Thử nghiệm và nghiệm thu hệ thống

1. Bên triển khai xây dựng kế hoạch, nội dung thử nghiệm hệ thống trước khi thực hiện thử nghiệm và nghiệm thu hệ thống.

2. Cơ quan, đơn vị vận hành thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác theo phương án thiết kế được phê duyệt trong Hồ sơ đề xuất cấp độ.

3. Công chức chuyên trách và bên triển khai hệ thống xây dựng kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống, trình Lãnh đạo Sở phê duyệt trước khi đưa hệ thống vào vận hành, khai thác.

4. Công chức chuyên trách phối hợp với bên triển khai hệ thống thực hiện thử nghiệm và nghiệm thu hệ thống, trước khi đưa vào vận hành, khai thác.

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

Điều 10. Quản lý an toàn mạng

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

2. 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.

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

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

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

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

b) Các dữ liệu sau yêu cầu 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.

6. Truy cập và quản lý cấu hình hệ thống:

a) Cấu hình hệ thống từ xa phải sử dụng các giảo 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.

Điều 11. Quản lý an toàn máy chủ và ứng dụng

Quy định về quản lý an toàn máy chủ và ứng dụng:

1. Quy định với máy chủ

a) Hoạt động của máy chủ phải được giám sát thường xuyên, liên tục, bảo đảm tính khả dụng của ứng dụng.

b) Ảnh hệ điều hành phải được sao lưu dự phòng trên hệ thống lưu trữ độc lập định kỳ 01 tháng/lần.

c) Máy chủ phải được nâng cấp, xử lý điểm yếu an toàn thông tin trên máy chủ trước khi đưa vào sử dụng.

d) Việc kết nối, gỡ bỏ máy chủ khỏi hệ thống phải được sự cho phép của Thủ trưởng đơn vị và xóa sạch dữ liệu.

đ) Có tài liệu liệt kê, cài đặt với những phần mềm hệ thống cài trong máy chủ.

2. Quy định với ứng dụng:

a) Hoạt động của ứng dụng phải được giám sát thường xuyên, liên tục, bảo đảm tính khả dụng của ứng dụng.

b) Ứng dụng phải được thiết lập chính sách xác thực; Kiểm soát truy cập; Có phương án bảo mật thông tin liên lạc và biện pháp bảo đảm an toàn ứng dụng và mã nguồn.

c) Ứng dụng phải được định kỳ kiểm tra đánh giá an toàn thông tin 2 năm/lần hoặc khi thay đổi, nâng cấp mở rộng.

3. Truy cập mạng của máy chủ:

a) Kết nối, truy cập máy chủ phải được kiểm soát bởi tường lửa hệ thống.

b) Chỉ mở cổng quản trị hệ thống từ vùng mạng LAN hoặc vùng mạng quản trị (nếu có).

c) Truy cập quản trị máy chủ từ bên ngoài mạng phải qua kênh kết nối VPN.

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

a) Định kỳ 03 tháng thay đổi các tài khoản, mật khẩu mặc định ngay khi đưa hệ điều hành, phần mềm vào sử dụng.

b) Chỉ cấp quyền quản lý ứng dụng cho công chức, viên chức quản trị theo chức năng, nhiệm vụ được giao.

c) Truy cập quản trị máy chủ và ứng dụng phải qua giao thức mã hóa như SSL, TLS, SSH và VPN.

d) Truy cập quản trị máy chủ và ứng dụng từ bên ngoài mạng phải qua kênh kết nối VPN.

5. Quy định về cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố:

a) Định kỳ hàng tháng hoặc khi nâng cấp ứng dụng phải sao lưu, dự phòng mã nguồn ứng dụng và cơ sở dữ liệu trên thiết bị hoặc hệ thống độc lập.

b) Dữ liệu lưu trữ phải được mã hóa cùng mã kiểm tra tính toàn vẹn.

c) Dữ liệu lưu trữ phải được quản lý theo phiên bản và có quản lý truy cập.

Điều 12. Quản lý an toàn dữ liệu

1. Quy định dự phòng và khôi phục dữ liệu:

a) Định kỳ hàng tuần phải sao lưu, dự phòng cơ sở dữ liệu và dữ liệu nghiệp vụ (nếu có) trên thiết bị hoặc hệ thống độc lập.

b) Dữ liệu lưu trữ phải được mã hóa cùng mã kiểm tra tính toàn vẹn.

c) Dữ liệu lưu trữ phải được quản lý theo phiên bản và có quản lý truy cập.

2. Định kỳ hàng tháng 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.

3. Bản sao lưu được lưu trữ trên thiết bị hoặc hệ thống độc lập.

Điều 13. Quản lý sự cố an toàn thông tin

1. Thực hiện cô lập hệ thống, ngắt kết nối với các hệ thống liên quan khác.

2. Khi có sự cố an toàn thông tin xảy ra, công chức chuyên trách phải sao lưu, dự phòng toàn bộ hiện trạng hệ thống trước khi xử lý sự cố.

3. Liên hệ với đầu mối ứng cứu sự cố theo thông tin tại khoản 2, Điều 5 Quy chế này.

Điều 14. Quản lý an toàn người sử dụng đầu cuối

1. Khi kết nối thiết bị lưu trữ ngoài như ổ cứng di động, các loại thẻ nhớ, thiết bị lưu trữ USB, ... phải quét virus trước khi đọc hoặc sao chép dữ liệu.

2. Không sử dụng các máy tính thuộc sở hữu cá nhân (máy xách tay của cá nhân, PDA) hoặc những thiết bị lưu trữ di động cá nhân vào mạng quản trị hoặc nghiệp vụ. Hạn chế tối đa việc sử dụng các thiết bị lưu trữ ngoài để sao chép, di chuyển dữ liệu.

3. Thiết lập mạng công cộng cho các máy tính thuộc sở hữu cá nhân (máy xách tay của cá nhân, PDA) hoặc những thiết bị lưu trữ di động cá nhân và có quản lý truy cập vùng mạng này với các vùng mạng khác trong hệ thống.

4. Máy tính người sử dụng phải được thiết lập chế độ cập nhật bản vá tự động và phần mềm phòng chống mã độc.

Điều 15. Quản lý rủi ro an toàn thông tin mạng

Đơn vị vận hành xây dựng và ban hành Hồ sơ Quản lý rủi ro an toàn thông tin bao gồm các nội dung sau:

1. Danh mục tài sản thông tin, dữ liệu có trong hệ thống.

2. Đánh giá các rủi ro an toàn thông tin đối với mỗi loại tài sản.

3. Có phương án dự phòng và khôi phục sau sự cố đối với thông tin, dữ liệu và ứng dụng.

Điều 16. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ

Quy định, quy trình về Kết thúc vận hành, khai thác, thanh lý, hủy bỏ bao gồm các nội dung sau:

1. Thiết bị công nghệ thông tin có chứa dữ liệu (máy tính, thiết bị lưu trữ, ...) khi bị hỏng phải được công chức chuyên trách 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 trang thiết bị công nghệ thông tin: Máy tính cá nhân (PC), máy tính xách tay, máy chủ, các thiết bị mạng, phương tiện lưu trữ như thẻ

nhớ, ổ cứng phải xóa sạch dữ liệu khi chuyển giao hoặc thay đổi mục đích sử dụng.

Chương IV
TỔ CHỨC BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 17. Trách nhiệm của Văn phòng Sở.

Thực hiện trách nhiệm theo quy định tại Điều 22 Nghị định 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về về bảo đảm an toàn hệ thống thông tin theo cấp độ.

Điều 18. Trách nhiệm của công chức chuyên trách về công nghệ thông tin, an toàn thông tin, an ninh mạng

1. Giao Văn phòng Sở bố trí công chức chuyên trách thực hiện nhiệm vụ quản lý, vận hành, giám sát và bảo đảm an toàn cho hệ thống thông tin phục vụ hoạt động nội bộ của Sở.

2. Tuân thủ các quy định về trách nhiệm của công chức chuyên trách về an toàn thông tin được giao tại Quy chế này.

Điều 19. Trách nhiệm của người dùng

Thực hiện nghiêm túc các quy định về quản lý, vận hành hệ thống tại cơ quan, đơn vị theo đúng các quy định hiện hành. Chấp hành đúng các quy định về an toàn thông tin tại Điều 14 Quy chế này.

Chương V
TỔ CHỨC THỰC HIỆN

Điều 20. Rà soát, cập nhật, bổ sung Quy chế

1. Định kỳ 03 năm hoặc khi có thay đổi Quy chế bảo đảm an toàn thông tin kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung.

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.

Điều 21. Quy chế này được áp dụng thực hiện trong nội bộ Sở Nội vụ. Thủ trưởng các cơ quan, đơn vị trực thuộc Sở và công chức, viên chức, người lao động của Sở có trách nhiệm thực hiện nghiêm túc Quy chế này.

Điều 22. Trong quá trình thực hiện nếu có vấn đề phát sinh, vướng mắc hoặc chưa phù hợp; Thủ trưởng các cơ quan, đơn vị trực thuộc Sở cần phản hồi về Văn phòng Sở để phối hợp thực hiện hoặc tổng hợp báo cáo Giám đốc Sở xem xét chỉ đạo thực hiện.

Điều 23. Giao Văn phòng Sở có trách nhiệm theo dõi, kiểm tra các cơ quan, đơn vị, công chức, viên chức, người lao động thuộc Sở thực hiện nghiêm Quy chế này./.