UBND TỈNH GIA LAI **VĂN PHÒNG**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 26 /QĐ-VPUBND	*Gia Lai, ngày 11 tháng 7 năm 2025*

QUYẾT ĐỊNH
Ban hành Quy chế đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin tại Văn phòng Ủy ban nhân dân tỉnh

CHÁNH VĂN PHÒNG ỦY BAN NHÂN DÂN TỈNH

Căn cứ Luật an toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Luật An ninh mạng ngày 12 tháng 6 năm 2018;

Căn cứ Luật Bảo vệ bí mật nhà nước ngày 15 tháng 11 năm 2018;

Căn cứ Luật giao dịch điện tử ngày 22 tháng 6 năm 2023;

Căn cứ Luật Dữ liệu ngày 30 tháng 11 năm 2024;

Căn cứ Luật Tổ chức chính quyền địa phương ngày 16 tháng 6 năm 2025;

Căn cứ Nghị định số 147/2024/NĐ-CP ngày 9 tháng 11 năm 2024 của Chính phủ về việc ban hành Nghị định quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng;

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

Căn cứ Quyết định số 08/2023/QĐ-TTg ngày 05 tháng 4 năm 2023 của Thủ tướng Chính phủ về Mạng truyền số liệu chuyên dùng phục vụ các cơ quan Đảng, Nhà nước;

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

Căn cứ Quyết định số 01/2025/QĐ-VPUBND ngày 01 tháng 7 năm 2025 của Ủy ban nhân dân tỉnh Gia Lai quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Văn phòng Ủy ban nhân dân tỉnh Gia Lai;

Theo đề nghị của Giám đốc Trung tâm Phục vụ hành chính công.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này *"Quy chế đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin tại Văn phòng Ủy*

ban nhân dân tỉnh".

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày ký và thay thế Quyết định số 73/QĐ-VPUBND ngày 25 tháng 4 năm 2025 của Văn phòng Ủy ban nhân dân tỉnh Bình Định ban hành Quy chế đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin tại Văn phòng Ủy ban nhân dân tỉnh.

Điều 3. Giám đốc Trung tâm Phục vụ hành chính công**,** Trưởng phòng Phòng Hành chính - Tổ chức, Trưởng các phòng, ban, trung tâm thuộc Văn phòng Ủy ban nhân dân tỉnh chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- CT, các PCT UBND tỉnh (b/c);
- LĐVP UBND tỉnh;
- Lưu: VT, TTPVHCC.

CHÁNH VĂN PHÒNG

CỘNG HÒA X.H.C.N VIỆT NAM
VĂN PHÒNG ỦY BAN NHÂN DÂN
TỈNH GIA LAI

Nguyễn Xuân Vĩnh

UBND TỈNH GIA LAI
VĂN PHÒNG

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

QUY CHẾ
Bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin tại Văn phòng Ủy ban nhân dân tỉnh

(Ban hành kèm theo Quyết định số 26 /QĐ-VPUBND ngày 11 /7 /2025 của Văn phòng UBND tỉnh)

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 các chính sách quản lý và các biện pháp bảo đảm an toàn thông tin tại Văn phòng Ủy ban nhân dân tỉnh (sau đây gọi tắt là Văn phòng UBND tỉnh).

2. Đối tượng áp dụng

a) Các phòng, ban, đơn vị trực thuộc Văn phòng; cán bộ, công chức, viên chức và người lao động thuộc Văn phòng.

b) Cơ quan, tổ chức, cá nhân có sử dụng các hệ thống thông tin do Văn phòng Ủy ban nhân dân tỉnh triển khai.

c) Cơ quan, tổ chức, cá nhân có liên quan đến hoạt động ứng dụng công nghệ thông tin của Văn phòng.

Điều 2. Giải thích từ ngữ

1. Mạng được quy định tại Khoản 2 Điều 3 Luật An toàn thông tin mạng, cụ thể: 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.

2. An toàn thông tin mạng được quy định tại Khoản 1 Điều 3 Luật An toàn thông tin mạng, cụ thể: 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.

3. Hệ thống thông tin được quy định tại Khoản 3 Điều 3 Luật An toàn thông tin mạng, cụ thể: 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. Xâm phạm an toàn thông tin mạng được quy định tại Khoản 6 Điều 3 Luật An toàn thông tin mạng, cụ thể: Xâm phạm an toàn thông tin mạng là hành vi truy nhập, sử dụng, tiết lộ, làm gián đoạn, sửa đổi, phá hoại trái phép thông tin, hệ thống thông tin.

5. Sự cố an toàn thông tin mạng được quy định tại Khoản 7 Điều 3 Luật An toàn thông tin mạng, cụ thể: 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.

6. Rủi ro an toàn thông tin mạng được quy định tại Khoản 8 Điều 3 Luật An toàn thông tin mạng, cụ thể: Rủi ro an toàn thông tin mạng là những nhân tố chủ quan hoặc khách quan có khả năng ảnh hưởng tới trạng thái an toàn thông tin mạng.

7. Phần mềm độc hại được quy định tại Khoản 11 Điều 3 Luật An toàn thông tin mạng, cụ thể: 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.

8. Nguy cơ mất an toàn thông tin mạng là những nhân tố bên trong hoặc bên ngoài có khả năng ảnh hưởng tới trạng thái an toàn thông tin mạng.

9. Lỗ hổng bảo mật là điểm yếu về an toàn thông tin (sau đây gọi tắt là ATTT) trên phần mềm hoặc phần cứng, bị tin tặc khai thác để truy cập trái phép vào hệ thống thông tin.

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

1. Bảo đảm an toàn thông tin mạng là yêu cầu bắt buộc, thường xuyên, liên tục, có tính xuyên suốt quá trình liên quan đến thông tin và thiết kế, xây dựng, vận hành, nâng cấp, hủy bỏ hệ thống thông tin. Bảo đảm an toàn, tuân thủ các nguyên tắc chung quy định tại Điều 4 Luật an toàn thông tin mạng và Điều 4 Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

2. Cơ quan, tổ chức, cá nhân có trách nhiệm bảo đảm ATTT mạng. Hoạt động ATTT mạng của cơ quan, tổ chức, cá nhân phải đúng các quy định của pháp luật liên quan.

3. Công tác bảo đảm ATTT mạng phải được thực hiện trên cơ sở có sự phối hợp chặt chẽ giữa các cơ quan, đơn vị và cá nhân.

4. Xử lý sự cố ATTT phải phù hợp với trách nhiệm, quyền hạn và bảo đảm lợi ích hợp pháp của cơ quan, đơn vị và theo quy định của pháp luật.

5. Phải có phương án tổ chức sao lưu dữ liệu dự phòng cho mọi dữ liệu quan trọng của tỉnh, của cơ quan, đơn vị. Lãnh đạo cơ quan, đơn vị phải chịu trách nhiệm nếu để xảy ra mất mát dữ liệu do không tiến hành sao lưu dự phòng.

6. Các thiết bị viễn thông, máy tính trong cơ quan nhà nước khi kết nối đến mạng truyền số liệu chuyên dùng của tỉnh phải tuân thủ theo Điều 8, Quyết định

số 08/2023/QĐ-TTg ngày 05/4/2023 của Thủ tướng Chính phủ về việc ban hành Quyết định về Mạng truyền số liệu chuyên dùng phục vụ các cơ quan Đảng, Nhà nước.

Điều 4. Những hành vi nghiêm cấm

1. Các hành vi bị nghiêm cấm quy định tại Điều 7 Luật An toàn thông tin mạng số 86/2015/QH13 ngày 19/11/2015.

2. Tự ý lắp đặt các thiết bị phát sóng wifi (Access Point) vào mạng máy tính của cơ quan, đơn vị và lắp đặt các thiết bị tiếp sóng wifi (Wireless card, wireless USB) trên máy tính có kết nối mạng nội bộ để truy cập mạng wifi ngoài khi chưa được phê duyệt của Lãnh đạo cơ quan, đơn vị.

3. Lợi dụng mạng để truyền bá thông tin, quan điểm, thực hiện các hành vi gây phương hại đến an ninh quốc gia; trật tự, an toàn xã hội và lợi ích quốc gia trên mạng; phá hoại khối đại đoàn kết toàn dân; tuyên truyền chiến tranh xâm lược, khủng bố; gây hận thù, mâu thuẫn giữa các dân tộc, sắc tộc, tôn giáo và bài ngoại.

4. Lợi dụng mạng để truyền bá trái phép tài liệu, hình ảnh, âm thanh hoặc dạng thông tin khác nhằm kích động bạo lực, dâm ô, đồi trụy, tội ác, tệ nạn xã hội, mê tín dị đoan; phá hoại thuần phong, mỹ tục của dân tộc; bôi nhọ, gây thù hận, xâm hại tới quyền và lợi ích hợp pháp của tổ chức, cá nhân.

5. Tự ý tải về, chia sẻ dưới mọi hình thức các dữ liệu, tài liệu, số liệu nội bộ, những văn bản chưa được cấp có thẩm quyền công khai lên mạng internet và các phương tiện thông tin đại chúng khác.

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 ATTT:

a) Văn phòng Ủy ban nhân dân tỉnh giao Trung tâm Phục vụ hành chính công tỉnh (sau đây gọi tắt là Trung tâm PVHCC tỉnh) là đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về ATTT phục vụ việc đảm bảo ATTT mạng cho các hệ thống thông tin do Văn phòng Ủy ban nhân dân tỉnh làm chủ quản.

b) Trung tâm PVHCC tỉnh làm đầu mối liên hệ, tiếp nhận, phối hợp với các cơ quan, tổ chức (có thẩm quyền quản lý về ATTT) trong công tác đảm bảo ATTT, phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm ATTT.

2. Tham gia các hoạt động, công tác bảo đảm ATTT khi có yêu cầu của tổ chức có thẩm quyền.

Điều 6. Bảo đảm nguồn nhân lực

1. Tuyển dụng

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

b) Quy trình tuyển dụng cán bộ, điều kiện tuyển dụng cán bộ và các quy trình đánh giá, kiểm tra trình độ chuyên môn tuân theo các quy định liên quan.

2. Trong quá trình làm việc

a) Đối với người dùng cuối:

- Có trách nhiệm tuân thủ các quy định, hướng dẫn bảo đảm ATTT và các quy định của pháp luật, bảo đảm ATTT đối với từng vị trí công việc.

- Thông báo ngay cho đơn vị chủ quản hệ thống thông tin khi nghi ngờ hoặc phát hiện sự cố, hiện tượng bất thường của hệ thống thông tin.

- Tham gia đầy đủ các lớp tập huấn, đào tạo và tự cập nhật kiến thức về ATTT mạng.

- Chịu trách nhiệm quản lý, sử dụng trang thiết bị CNTT được giao, bảo đảm ATTT; không được giao cho các tổ chức, cá nhân khác sử dụng trang thiết bị CNTT đã được giao sử dụng; không được sử dụng trang thiết bị CNTT cá nhân để kết nối, truy cập vào các hệ thống thông tin nội bộ nếu chưa được phép của đơn vị chủ quản; không tự thay thế, lắp mới, tráo đổi thành phần của máy tính công vụ; không mang tài sản CNTT của đơn vị ra ngoài nếu chưa được phép của thủ trưởng đơn vị; có trách nhiệm bàn giao cho đơn vị quản lý các trang thiết bị CNTT khi chuyển công tác, thay đổi vị trí việc làm hoặc nghỉ việc.

b) Định kỳ hàng năm tổ chức phổ biến, tuyên truyền nâng cao nhận thức về ATTT cho người sử dụng.

c) Tổ chức đào tạo hoặc cử đi đào tạo về ATTT hàng năm cho 03 nhóm đối tượng bao gồm: cán bộ kỹ thuật, cán bộ quản lý và người sử dụng trong hệ thống theo kế hoạch đào tạo, bồi dưỡng của đơn vị.

Các đơn vị liên quan có trách nhiệm phối hợp với Sở Khoa học và Công nghệ, Công an tỉnh xây dựng, triển khai kế hoạch đào tạo, bồi dưỡng, tập huấn về công tác bảo đảm ATTT, an ninh mạng cho đội ngũ công chức, viên chức của cơ quan, đơn vị.

3. Nghỉ việc hoặc thay đổi công việc

a) Công chức, viên chức, người lao động nghỉ việc hoặc thay đổi công việc phải tuân thủ:

- Phải bàn giao lại công việc, tài khoản truy cập hệ thống thông tin, tài sản CNTT của cơ quan, đơn vị; phải có cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc;

- Quản trị viên hệ thống phải vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi công chức, viên chức, người lao động thôi việc.

b) Quy trình thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi công chức, viên chức, người lao động thôi việc:

- Thu hồi tài khoản truy cập, các trang thiết bị máy móc, phần cứng và các tài sản khác thuộc sở hữu của đơn vị quản lý;

- Vô hiệu hóa các thông tin của công chức, viên chức, người lao động thôi việc được lưu trên các phương tiện lưu trữ, phần mềm;

- Vô hiệu hóa tất cả các quyền truy cập của công chức, viên chức, người lao động thôi việc vào tài nguyên, hệ thống phần mềm của đơn vị quản lý;

- Kiểm tra lại các quyền ra vào, truy cập tài nguyên, quản trị hệ thống đã cấp cho công chức, viên chức, người lao động thôi việc để bảo đảm đã hoàn toàn được gỡ bỏ khỏi hệ thống.

c) Cán bộ, công chức, viên chức nghỉ việc hoặc thay đổi công việc phải có cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc. Các thông tin bắt buộc cần giữ bí mật, tối thiểu bao gồm:

- Không tiết lộ thông tin được tiếp xúc trong quá trình công tác tại đơn vị cho các cá nhân, tổ chức gây ảnh hưởng bất lợi đến lợi ích của đơn vị;

- Không sử dụng các thông tin được tiếp xúc trong quá trình công tác tại đơn vị vào mục đích trục lợi cá nhân.

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

Điều 7. Thiết kế an toàn hệ thống thông tin

1. Có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin.

2. Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin.

3. Có tài liệu mô tả phương án bảo đảm ATTT theo cấp độ.

4. Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm ATTT.

5. 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.

6. Có phương án quản lý và bảo vệ hồ sơ thiết kế.

7. Có bộ phận chuyên môn, tổ chuyên gia đánh giá hồ sơ thiết kế hệ thống thông tin, các biện pháp bảo đảm ATTT trước khi triển khai thực hiện.

Điều 8. Phát triển phần mềm thuê khoán

1. Đối với các nội dung liên quan đến việc phát triển phần mềm thuê khoán, nhà phát triển phải bảo đảm có các cam kết bảo đảm ATTT.

2. Kiểm thử phần mềm trên môi trường thử nghiệm trước khi đưa vào sử dụng.

3. Kiểm tra, đánh giá ATTT, trước khi đưa vào sử dụng.

4. Khi thay đổi mã nguồn, kiến trúc phần mềm thực hiện kiểm tra, đánh giá ATTT cho phần mềm.

5. Có cam kết của bên phát triển về bảo đảm tính bí mật và bản quyền của phần mềm phát triển.

Điều 9. Thử nghiệm và nghiệm thu hệ thống

Hoạt động thử nghiệm và nghiệm thu hệ thống thực hiện theo hướng dẫn tại Thông tư số 16/2024/TT-BTTTT ngày 30/12/2024 của Bộ trưởng Bộ Thông tin và Truyền thông về việc ban hành Thông tư quy định chi tiết nội dung công tác triển khai, giám sát công tác triển khai, nghiệm thu đối với dự án đầu tư ứng dụng công nghệ thông tin; xác định yêu cầu về chất lượng dịch vụ và các nội dung đặc thù của hợp đồng thuê dịch vụ đối với thuê dịch vụ công nghệ thông tin theo yêu cầu riêng.

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

Điều 10. Quản lý an toàn mạng

1. Hệ thống mạng phải được thiết kế thống nhất, cùng kết hợp và hỗ trợ, tương tác hoạt động với nhau, được tổ chức quản lý định danh, xác thực đối với tất cả người sử dụng nhằm mục đích quản lý hệ thống chặt chẽ, bảo đảm an toàn và bảo mật.

2. Hệ thống mạng nội bộ (LAN) phải được bảo vệ bằng tường lửa (có thể tích hợp tường lửa trên modem hoặc router) và phân chia hệ thống mạng thành các vùng mạng quản lý theo chính sách ATTT riêng.

3. Mạng không dây (WiFi), cần thiết lập các thông số an toàn và định kỳ ít nhất 3 tháng thay đổi mật khẩu truy cập nhằm tăng cường công tác bảo mật. Hệ thống mạng không dây phải được bảo vệ bởi mật khẩu an toàn.

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

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. Các bản quyền phần mềm cần được thống kê, quản lý thời gian phục vụ cho việc gia hạn.

g. Triển khai hệ thống phát hiện phòng chống xâm nhập giữa các vùng mạng quan trọng.

h. Sử dụng thêm các phương pháp xác thực đa nhân tố đối với các thiết bị mạng quan trọng.

i. Triển khai phương án cảnh báo thời gian thực trực tiếp đến người quản trị hệ thống thông qua hệ thống giám sát khi phát hiện sự cố trên các thiết bị mạng.

k. Duy trì ít nhất 02 kết nối mạng Internet từ các ISP sử dụng hạ tầng kết nối trong nước khác nhau (nếu hệ thống buộc phải có kết nối mạng Internet).

5. 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; 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.

b. Triển khai phương án dự phòng nóng cho các thiết bị mạng chính bảo đảm khả năng vận hành liên tục của hệ thống; năng lực của thiết bị dự phòng phải đáp ứng theo quy mô hoạt động của hệ thống.

c. Triển khai hệ thống/phương tiện lưu trữ nhật ký độc lập và phù hợp với hoạt động của các thiết bị mạng. Dữ liệu nhật ký phải được lưu tối thiểu 06 tháng.

d. Triển khai hệ thống/phương tiện chống thất thoát dữ liệu trong hệ thống.

6. Truy cập và quản lý cấu hình hệ thống

a. Cán bộ quản lý, vận hành truy cập, khai thác thông tin tại hệ thống 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.

b. Cán bộ quản lý, vận hành có trách nhiệm theo dõi và phát hiện các trường hợp truy cập hệ thống trái phép hoặc thao tác vượt quá giới hạn, báo cáo cho cấp có thẩm quyền để tiến hành ngăn chặn, thu hồi, khóa quyền truy cập của các tài khoản vi phạm.

c. Quy trình kết nối thiết bị đầu cuối của người sử dụng vào hệ thống mạng; truy nhập và quản lý cấu hình hệ thống; cấu hình tối ưu, tăng cường bảo mật cho thiết bị mạng, bảo mật (cứng hóa) trong hệ thống và thực hiện quy trình trước khi đưa hệ thống vào vận hành khai thác.

7. 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.

8. Các thiết bị mạng phải được cấu hình chức năng xác thực; Chỉ cho phép sử dụng các kết nối mạng an toàn (nếu hỗ trợ) khi truy cập, quản trị thiết bị từ xa; Giới hạn các địa chỉ mạng có thể kết nối, quản trị thiết bị từ xa; Hạn chế được số lần đăng nhập sai; Phân quyền truy cập, quản trị; Nâng cấp, xử lý điểm yếu ATTT của thiết bị hệ thống trước khi đưa vào sử dụng.

9. Việc thanh lý, tiêu hủy thiết bị, vật mang thông tin trong mạng phải đảm bảo yêu cầu không để lộ, lọt thông tin Nhà nước. Phải có quy trình cụ thể và phải lưu giữ hồ sơ, biên bản việc thanh lý, tiêu hủy.

10. Tệp tin cấu hình, sơ đồ mạng logic và vật lý phải được cập nhật, sao lưu dự phòng.

11. Có biện pháp bảo vệ, dự phòng, phòng chống các nguy cơ do mất cắp, cháy nổ, ngập lụt, động đất và các thảm họa khác do thiên nhiên hoặc con người gây ra và các phương án khôi phục hệ thống sau thảm họa.

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

1. Quy định với máy chủ

a) Hệ thống máy chủ phải có tính năng sẵn sàng cao, cơ chế dự phòng linh hoạt để bảo đảm hoạt động liên tục.

b) Có biện pháp bảo vệ, dự phòng, phòng chống các nguy cơ do mất cắp, cháy nổ, ngập lụt, động đất và các thảm hoạ khác do thiên nhiên hoặc do con người gây ra và các phương án khôi phục sau thảm hoạ cho hệ thống máy chủ.

c) Máy chủ phải được thiết lập chính sách xác thực; kiểm soát truy cập; kết nối về hệ thống giám sát tập trung; thực hiện biện pháp phòng chống xâm nhập; phòng chống phần mềm độc hại và xử lý dữ liệu trên máy chủ khi chuyển giao.

d) Máy chủ phải được nâng cấp, xử lý điểm yếu ATTT trên máy chủ trước khi đưa vào sử dụng.

đ) Việc kết nối, gỡ bỏ máy chủ khỏi hệ thống phải được sự cho phép của thủ trưởng đơn vị và thực hiện theo quy trình đã được phê duyệt.

e) Phần mềm hệ điều hành cài lên máy chủ ưu tiên là phần mềm hệ điều hành có bản quyền hoặc phần mềm mã nguồn mở được sử dụng rộng rãi trong nước và quốc tế.

g) Ghi nhật ký, quy định thời gian về hoạt động tác động vào các máy chủ, người sử dụng, lỗi phát sinh và các sự cố nhằm trợ giúp cho việc điều tra giám sát về sau.

2. Quy định với ứng dụng

a) Các yêu cầu, thiết kế về an toàn bảo mật của phần mềm ứng dụng cần được xác định rõ trong tài liệu phân tích, thiết kế. Trong quá trình triển khai, vận hành các phần mềm ứng dụng cần bảo đảm nghiêm ngặt theo các yêu cầu, thiết kế về an toàn bảo mật.

b) Ứng dụng phải được thiết lập chính sách xác thực; kiểm soát truy cập; kết nối về hệ thống giám sát tập trung; có phương án bảo mật thông tin liên lạc, chống chối bỏ và biện pháp bảo đảm an toàn ứng dụng và mã nguồn.

c) Có phương án xác định và khắc phục rủi ro trước, trong quá trình triển khai và khi vận hành các phần mềm ứng dụng.

d) Ứng dụng phải kiểm tra, thử nghiệm và có biên bản đánh giá tính an toàn, bảo mật đối với phần mềm ứng dụng theo yêu cầu khi nghiệm thu các phần mềm này. Việc tiến hành thử nghiệm phải bảo đảm trên môi trường riêng biệt, không ảnh hưởng tới hoạt động và dữ liệu của đơn vị.

đ) Quản lý và phần quyền truy cập phần mềm ứng dụng và cơ sở dữ liệu phù hợp với chức năng, nhiệm vụ của người sử dụng. Quyền truy cập phải được phân ra theo từng cấp độ tương ứng với từng nhiệm vụ của nhân viên và phải được phê duyệt từ cấp trên.

3. Quy định với ứng dụng thư điện tử

a) Sử dụng thư điện tử công vụ phục vụ (có dạng xyz@vpub.gialai.gov.vn) cho công việc của cơ quan; không sử dụng thư điện tử công cộng vào mục đích công vụ.

b) Mỗi cá nhân cần đặt mật khẩu theo quy định tại Điểm d, Điều 19 của quy chế này cho hộp thư điện tử của mình.

4. Khi công chức, viên chức, người lao động nghỉ việc hoặc chuyển công tác thì tài khoản truy cập phần mềm ứng dụng và tài khoản thư điện tử công vụ sẽ bị khoá.

Điều 12. Quản lý an toàn dữ liệu

1. Thực hiện quản lý, lưu trữ dữ liệu quan trọng trong hệ thống cùng với mã tính kiểm tra tính nguyên vẹn.

2. Có cơ chế sao lưu dữ liệu dự phòng, lưu trữ dữ liệu tại nơi an toàn đồng thời thường xuyên kiểm tra để bảo đảm sẵn sàng phục hồi nhằm ngăn ngừa và hạn chế khi sự cố ATTT mạng xảy ra.

3. Tiến hành cập nhật đồng bộ thông tin, dữ liệu giữa hệ thống sao lưu dự phòng chính và hệ thống phụ được thực hiện theo yêu cầu của đơn vị vận hành hệ thống.

4. Quản lý chặt chẽ các thiết bị lưu trữ dữ liệu, nghiêm cấm việc di chuyển, thay đổi vị trí khi chưa được phép của người có thẩm quyền.

5. Quản lý và phân quyền truy cập phần mềm ứng dụng và cơ sở dữ liệu phù hợp với chức năng, nhiệm vụ của người sử dụng. Quyền truy cập phải được phân ra theo từng cấp độ tương ứng với từng nhiệm vụ của nhân viên và phải được phê duyệt từ cấp trên.

6. 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.

7. Lưu trữ có mã hoá các thông tin, dữ liệu (không phải là thông tin, dữ liệu công khai) trên hệ thống lưu trữ, phương tiện lưu trữ.

8. Kiểm tra, giám sát các hoạt động liên quan đến các nơi lưu trữ mật khẩu và cảnh báo khi có những hành động bất thường (Ví dụ: user không có quyền nhưng cố tình truy xuất đến các file lưu mật khẩu…).

Điều 13. Quản lý an toàn thiết bị đầu cuối

Các thiết bị đầu cuối khi kết nối vào hệ thống phải được quản lý như sau:

1. Việc sử dụng các thiết bị lưu trữ ngoài như ổ cứng di động, các loại thẻ nhớ, thiết bị lưu trữ USB,... phải thường xuyên quét virus trước khi đọc hoặc sao chép dữ liệu.

2. Thông tin về thiết bị đầu cuối (tên, chủng loại, địa chỉ MAC, địa chỉ IP) phải được quản lý và cập nhật.

3. Các thiết bị đầu cuối phải được quản lý khi kết nối vào hệ thống mạng theo địa chỉ MAC, IP.

4. Khi truy cập và sử dụng thiết bị đầu cuối từ xa phải có cơ chế xác thực và sử dụng giao thức mạng an toàn.

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

6. Cấu hình tối ưu và tăng cường bảo mật cho máy tính người sử dụng và thực hiện quy trình trước khi đưa vào hệ thống sử dụng:

a) Máy tính người dùng trước khi đưa vào sử dụng phải được đánh giá, rà soát các điểm yếu ATTT, bảo đảm sử dụng hệ điều hành có bản quyền, còn trong hạn được hỗ trợ cập nhật của hãng phát hành. Trong trường hợp có thông báo hết hỗ trợ cập nhật bản vá từ hãng, phải có kế hoạch nâng cấp, thay thế. Cập nhật bản vá hệ điều hành đầy đủ tại thời điểm đưa vào sử dụng và trong quá trình sử dụng.

b) Gỡ bỏ các phần mềm không cần thiết, cài đặt chương trình diệt virus có bản quyền. Không cấp tài khoản quản trị máy tính cho người dùng, không để người dùng tự ý cài đặt các phần mềm độc hại trên máy tính.

7. Kiểm tra, đánh giá, xử lý điểm yếu ATTT cho thiết bị đầu cuối trước khi đưa vào sử dụng.

Điều 14. 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. Các phần mềm phòng chống mã độc phải được thiết lập chế độ tự động cập nhật; chế độ tự động quét mã độc khi sao chép, mở các tập tin.

2. Khi gửi văn bản điện tử gửi qua hệ thống thư điện tử phải có định dạng theo Danh mục tiêu chuẩn kỹ thuật về ứng dụng CNTT trong cơ quan nhà nước như: (.txt), (.doc), (.odt), (.pdf) và các định dạng khác theo quy định, không được gửi các file thực thi (.com), (.bat), (.exe)....

3. Các cán bộ, công chức, viên chức và người lao động trong cơ quan phải được hướng dẫn về phòng chống mã độc, các rủi ro do mã độc gây ra; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm trên máy tính PC, Tablet, Laptop của cơ quan khi chưa có sự đồng ý của người có thẩm quyền theo quy định của cơ quan.

4. Tất cả các máy tính của đơn vị phải được cấu hình nhằm vô hiệu hóa tính năng tự động thực thi (autoplay) các tập tin trên các thiết bị lưu trữ di động.

5. Khi phát hiện ra bất kỳ dấu hiệu 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.

6. 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.

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

Công tác triển khai: Hệ thống giám sát trung tâm; thông tin giám sát và danh mục các đối tượng giám sát; thực thi nhiệm vụ giám sát; nâng cao năng lực hoạt động giám sát; trách nhiệm giám sát ATTT của các Hệ thống thông tin của Văn phòng được thực hiện theo 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.

Điều 16. Quản lý điểm yếu an toàn hệ thống thông tin

1. Đơn vị/bộ phận chuyên trách về ATTT có trách nhiệm:

a) Quản lý thông tin điểm yếu ATTT 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.

b) Báo cáo Lãnh đạo/Cán bộ quản lý ngay khi phát hiện điểm yếu ATTT ở mức độ nghiêm trọng. Thực hiện cảnh báo và xử lý điểm yếu ATTT theo chỉ đạo. Việc xử lý điểm yếu ATTT phải bảo đảm không gây ảnh hưởng/gián đoạn hoạt động của hệ thống.

c) Xây dựng phương án xử lý tạm thời đối với trường hợp điểm yếu ATTT chưa được khắc phục và phương án khôi phục hệ thống trong trường hợp xử lý điểm yếu thất bại.

d) 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 ATTT đối với các điểm yếu khi cần thiết.

2. Đối với hệ thống/hệ thống thành phần được đề xuất là cấp độ 3 trở lên phải thực hiện kiểm tra, đánh giá và xử lý điểm yếu ATTT cho thiết bị hệ thống, máy chủ, dịch vụ trước khi đưa vào sử dụng.

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

4. Hoạt động đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống thực hiện theo quy định tại điểm c khoản 2 Điều 20 Nghị định số 85/2016/NĐ-CP và Điều 13 Thông tư số 03/2017/TT-BTTTT.

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

1. Quản lý truy cập, sử dụng tài nguyên nội bộ và trên Internet

a) Người sử dụng khi truy cập, sử dụng tài nguyên nội bộ phải tuân thủ các quy định của pháp luật về bảo đảm ATTT 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 ATTT.

2. Cài đặt và sử dụng máy tính an toàn

a) Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác của pháp luật về ATTT mạng. Chịu trách nhiệm bảo đảm ATTT 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 ATTT mạng phải báo ngay với cấp trên và bộ phận phụ trách công nghệ thông tin của cơ quan, đơn vị để kịp thời ngăn chặn, xử lý.

d) Tham gia các chương trình đào tạo, hội nghị về ATTT mạng được cơ quan chức năng, đơn vị chuyên môn tổ chức.

Điều 18. Quản lý sự cố an toàn thông tin

1. Phân nhóm sự cố an toàn thông tin:

a) Thấp: sự cố gây ảnh hưởng cá nhân và không làm gián đoạn hay đình trệ hoạt động chính của cơ quan, đơn vị như: máy tính trạm bị nhiễm phần mềm độc hại, phần mềm hệ điều hành, các phần mềm ứng dụng cài đặt trên máy tính cá nhân phát sinh lỗi;

b) Trung bình: sự cố ảnh hưởng đến một nhóm người dùng nhưng không gây gián đoạn hay đình trệ hoạt động chính của đơn vị như: hệ thống mạng của 01 (một) phòng, ban thuộc đơn vị bị ngưng hoạt động, phần mềm độc hại lây nhiễm tất cả các máy tính trạm trong 01 phòng, ban;

c) Cao: sự cố làm cho thiết bị, phần mềm hay hệ thống không thể sử dụng được và gây ảnh hưởng đến một trong các hoạt động chính của cơ quan như: hệ thống quản lý văn bản và điều hành, hồ sơ cấp phép, một cửa điện tử của đơn vị bị ngưng hoạt động, một số thiết bị công nghệ thông tin quan trọng (bộ chuyển mạch trung tâm, thiết bị định tuyến, thiết bị tường lửa, máy chủ quản lý tập tin chung,) bị hư hỏng;

d) Khẩn cấp: sự cố ảnh hưởng đến sự liên tục của nhiều hoạt động chính của cơ quan, đơn vị như: toàn bộ hệ thống thiết bị công nghệ thông tin, hệ thống cung cấp điện ngừng hoạt động, hệ thống trang thông tin điện tử bị tin tặc (hacker) tấn công, xâm nhập, thay đổi nội dung...

2. Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố ATTT:

Khi có sự cố hoặc nguy cơ mất ATTT mạng xảy ra như: hệ thống hoạt động chậm bất thường, không truy cập được hệ thống, nội dung thông tin bị thay đổi

không chủ động hoặc các dấu hiệu bất thường khác thì tiến hành quy trình ứng cứu sự cố theo các bước sau:

a) Bước 1: Nếu hệ thống có nguy cơ mất ATTT mạng thuộc thẩm quyền cơ quan, đơn vị trực tiếp quản lý thì thực hiện tiếp Bước 2. Nếu hệ thống có nguy cơ mất ATTT mạng thuộc Sở Khoa học và Công nghệ quản lý (các hệ thống được triển khai tập trung tại Trung tâm Dữ liệu tỉnh) thì thực hiện tiếp Bước 3.

b) Bước 2: Tiến hành xử lý sự cố theo quy chế nội bộ của cơ quan, đơn vị. Nếu sự cố được khắc phục thì lập biên bản ghi nhận và kết thúc quy trình phối hợp xử lý sự cố. Khi sự cố vượt quá khả năng xử lý của cơ quan, lập biên bản ghi nhận và thực hiện tiếp Bước 3;

c) Bước 3: Báo sự cố đến Sở Khoa học và Công nghệ và thực hiện tiếp Bước 4;

d) Bước 4: Phối hợp với Sở Khoa học và Công nghệ và các cơ quan, tổ chức có liên quan để tiến hành khắc phục sự cố và thực hiện tiếp Bước 5;

đ) Bước 5: Lập biên bản ghi nhận và kết thúc quy trình phối hợp xử lý sự cố, lãnh đạo cơ quan, đơn vị phải chỉ đạo kịp thời để khắc phục và hạn chế thiệt hại, báo cáo bằng văn bản cho cơ quan cấp trên trực tiếp quản lý và Sở Khoa học và Công nghệ.

Trường hợp có sự cố nghiêm trọng ở mức độ cao, khẩn cấp hoặc vượt quá khả năng khắc phục của cơ quan, đơn vị, lãnh đạo cơ quan, đơn vị phải báo cáo ngay cho cơ quan cấp trên quản lý trực tiếp và Sở Khoa học và Công nghệ để được hướng dẫn, hỗ trợ.

3. Bộ phận chuyên trách về ATTT có trách nhiệm

a) Phân nhóm sự cố ATTT mạng theo quy định tại Quyết định số 05/2017/NĐ-CP của Thủ tướng Chính phủ ngày 16/3/2017 quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm ATTT mạng quốc gia (Quyết định số 05); Xây dựng phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố ATTT mạng, ứng phó sự cố ATTT mạng;

b) Xây dựng quy trình ứng cứu sự cố ATTT mạng thông thường và nghiêm trọng theo quy định tại Điều 13, 14 Quyết định số 05/2017/QĐ-TTg.

c) Phối hợp với các đơn vị chức năng xây dựng và triển khai kế hoạch ứng phó sự cố ATTT theo quy định tại Điều 16 Quyết định số 05/2017/QĐ-TTg;

d) Có phương án và điều động nhân lực có kinh nghiệm thực hiện giám sát và cảnh báo sự cố ATTT, phối hợp với các đơn vị chuyên trách về ATTT đưa ra cảnh báo sớm về nguy cơ mất ATTT trong hệ thống.

đ) Xây dựng quy trình ứng cứu sự cố ATTT mạng thông thường và nghiêm trọng theo quy định tại Điều 13, 14 Quyết định số 05/2017/QĐ-TTg;

e). 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 ATTT; 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;

g) 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 dừng 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 ATTT theo chỉ đạo của Lãnh đạo;

h) 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 ATTT; 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.

4. Trách nhiệm của người dùng:

Thông tin, báo cáo kịp thời cho cán bộ chuyên trách về ATTT của cơ quan khi phát hiện các sự cố gây mất ATTT trong quá trình tham gia vào hệ thống thông tin của đơn vị; Phối hợp tích cực trong suốt quá trình giải quyết và khắc phục sự cố.

Điều 19. Quản lý truy cập

1. Đối với phòng, ban, trung tâm trực thuộc Văn phòng; cá nhân có trách nhiệm:

a) Bảo vệ bí mật thông tin tài khoản cá nhân, hoặc tài khoản của cơ quan, đơn vị khi được phân công nắm giữ đồng thời phải thay đổi ngay mật khẩu tài khoản khi mới được cấp và tự chịu trách nhiệm trong việc quản lý, bảo vệ mật khẩu của tài khoản, không được cho người khác sử dụng tài khoản cá nhân hoặc của cơ quan, đơn vị;

b) Không đặt chế độ tự động ghi nhớ mật khẩu của các trình duyệt trong mọi trường hợp sử dụng;

c) Thiết lập mật mã truy cập và chế độ tự động bảo vệ màn hình sau 10 phút không sử dụng cho tất cả hệ thống máy chủ, máy trạm của người sử dụng;

d) Hệ thống mạng không dây (WiFi) của Văn phòng và các đơn vị phải được đặt mật khẩu (password) khi truy cập. Thiết lập phương pháp hạn chế người dùng truy cập mạng không dây, giám sát và điều khiển truy cập mạng không dây;

đ) Đặt mật khẩu đăng nhập, truy cập hệ thống thông tin có độ phức tạp cao (có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự hoa, ký tự số hoặc ký tự đặc biệt như: !, @, #, $, %) và phải được thay đổi tối thiểu 03 tháng/lần cho tất cả các tài khoản truy cập vào hệ thống máy chủ, thiết bị mạng, máy tính, các ứng dụng.

2. Đối với các hệ thống thông tin

a) Bảo đảm mỗi tài khoản của tổ chức, cá nhân truy cập vào hệ thống thông tin là duy nhất.

b) Các hệ thống thông tin cần giới hạn số lần đăng nhập sai liên tiếp vào hệ thống (từ 03 đến 05 lần). Hệ thống tự động khóa tài khoản trong một khoảng thời gian nhất định nếu liên tục đăng nhập sai vượt quá số lần quy định trước khi tiếp tục cho đăng nhập và có phương thức hỗ trợ cấp lại mật khẩu tài khoản.

c) Đơn vị quản lý, vận hành các hệ thống dùng chung sẽ không chịu trách nhiệm về những thiệt hại do phía người dùng không tuân thủ các quy định về bảo vệ bí mật tài khoản dẫn đến thông tin cá nhân bị đánh cắp hay bị sửa đổi, các ứng dụng bị sử dụng mạo danh hay các hậu quả tiêu cực khác.

Điều 20. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ

1. Thực hiện việc huỷ bỏ toàn bộ thông tin, dữ liệu trên hệ thống với sự xác nhận của đơn vị chủ quản hệ thống thông tin khi kết thúc vận hành, khai thác, thanh lý, huỷ bỏ hệ thống thông tin.

2. Đối với các hệ thống thông tin có dữ liệu được lưu trữ trên tài sản vật lý cần phải mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài thì phải được sự phê duyệt của cấp có thẩm quyền và thực hiện các biện pháp bảo vệ dữ liệu; có cam kết bảo mật thông tin giữa bên có dữ liệu và bên cung cấp dịch vụ sửa chữa thiết bị lưu trữ dữ liệu.

3. Việc thực hiện kết thúc vận hành, khai thác, thanh lý, huỷ bỏ hệ thống thông tin được thực hiện theo quy định của pháp luật hiện hành.

Chương IV

TRÁCH NHIỆM ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 21. Trách nhiệm của lãnh đạo các phòng, ban, đơn vị

1. Lãnh đạo các phòng, ban, đơn vị thuộc Văn phòng chịu trách nhiệm trong việc cập nhật, triển khai thực hiện Quy chế này và các chỉ dẫn, hướng dẫn đảm bảo an toàn, an ninh thông tin của cơ quan và cấp trên tại phòng, ban, đơn vị mình.

2. Tuyên truyền chấp hành tốt các quy định, quy trình nội bộ về xử lý văn bản và hồ sơ công việc trên môi trường mạng, cập nhật và cung cấp thông tin trên các phần mềm ứng dụng, Cổng/trang thông tin điện tử.

3. Việc thanh lý, tiêu huỷ thiết bị, phần mềm, vật mang thông tin thuộc phòng, ban, đơn vị mình phải theo quy định, quy trình cụ thể của pháp luật, không để lộ, lọt thông tin nhà nước và phải lưu giữ hồ sơ, biên bản, tiêu huỷ thanh lý.

Điều 22. Trách nhiệm của Trung tâm Phục vụ hành chính công

1. Tham mưu Văn phòng Ủy ban nhân dân tỉnh về công tác bảo đảm ATTT tại Văn phòng và chịu trách nhiệm trước Văn phòng UBND tỉnh trong việc bảo đảm an toàn cho các hệ thống thông tin cấp tỉnh do Văn phòng UBND tỉnh quản lý.

2. Xây dựng và triển khai các Kế hoạch, chương trình, đào tạo về ATTT trong ứng dụng CNTT tại Văn phòng UBND tỉnh.

3. Tuỳ theo mức độ sự cố, phối hợp với các cơ quan, đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố ATTT tại Văn phòng UBND tỉnh; cảnh báo các vấn đề về ATTT trong hoạt động ứng dụng CNTT tại Văn phòng UBND tỉnh.

4. Triển khai các biện pháp bảo đảm an toàn, an ninh thông tin cho tất cả cán bộ công chức viên chức của cơ quan; tham mưu, đề xuất đầu tư, nâng cấp, mua sắm trang thiết bị công nghệ thông tin, các thiết bị phần cứng, phần mềm và giải pháp liên quan đến công tác bảo đảm an toàn an ninh thông tin mạng và Trung tâm tích hợp dữ liệu Văn phòng.

5. Hướng dẫn người sử dụng trong công tác đảm bảo an toàn, an ninh thông tin, thay đổi mật khẩu cá nhân theo quy định. Tham mưu Văn phòng tạo điều kiện cho cán bộ, công chức, viên chức tham gia chương trình nâng cao an toàn, an ninh thông tin.

6. Phối hợp chặt chẽ với cơ quan Công an trong công tác phòng ngừa, đấu tranh, truy vết, ngăn chặn các hoạt động xâm phạm an toàn, an ninh thông tin. Tạo điều kiện thuận lợi cho các cơ quan chức năng tham gia khắc phục sự cố và điều tra.

Điều 23. Trách nhiệm của cán bộ, công chức, viên chức và người lao động

1. Nghiêm túc chấp hành các quy định tại quy chế này và các quy định khác của pháp luật về bảo đảm ATTT.

2. Khi phát hiện sự cố ảnh hưởng đến an toàn hệ thống thông tin, phải thông báo ngay cho Trung tâm Phục vụ hành chính công.

3. Các thông tin, tài liệu, văn bản có tính mật theo quy định, phải dự thảo, lưu trữ đúng theo quy định về bảo mật và ATTT.

4. Cán bộ, công chức, viên chức chuyên trách CNTT:

a) Theo nhiệm vụ được Lãnh đạo văn phòng phân công, chịu trách nhiệm tham mưu chuyên môn và vận hành bảo đảm an toàn hệ thống thông tin tại cơ quan, đơn vị.

b) Hướng dẫn, hỗ trợ người dùng tại Văn phòng giải pháp phòng, chống virus, mã độc máy tính. Thực hiện việc đánh giá, báo cáo các rủi ro và mức độ các rủi ro ảnh hưởng đến hoạt động hệ thống thông tin của đơn vị, các giải pháp cơ bản khắc phục các rủi ro.

c) Phối hợp với các cá nhân, tổ chức có liên quan trong việc kiểm tra, phát hiện, phòng ngừa, đấu tranh, ngăn chặn xâm phạm ATTT; tham gia khắc phục các sự cố mất ATTT.

Chương V
TỔ CHỨC THỰC HIỆN

Điều 24. Điều khoản thi hành

1. Giao Trung tâm Phục vụ hành chính công chủ trì tham mưu, theo dõi và giám sát việc thực hiện Quy chế này. Định kỳ tổng hợp báo cáo tình hình an toàn, an ninh thông tin của cơ quan theo quy định.

2. Quy chế này được phổ biến đến tất cả cán bộ, công chức, viên chức, người lao động. Trưởng các phòng, ban, đơn vị trực thuộc tổ chức triển khai thực hiện nghiêm các quy định trong Quy chế này.

3. Trong quá trình thực hiện, nếu có vấn đề phát sinh, vướng mắc cần điều chỉnh, sửa đổi, bổ sung; các phòng, ban, đơn vị trực thuộc Văn phòng phản ánh về Trung tâm Phục vụ hành chính công để tổng hợp trình Lãnh đạo Văn phòng UBND tỉnh xem xét, sửa đổi, bổ sung cho phù hợp./.