



Đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin tại Văn phòng Ủy ban nhân dân tỉnh Hưng Yên

(Ban hành kèm theo Quyết định số 123/QĐ-VPUB ngày 15/2026 của Văn phòng UBND tỉnh Hưng Yên)

CHƯƠNG I. QUY ĐỊNH CHUNG

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

1.1. 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 các hệ thống thông tin tại Văn phòng Ủy ban nhân dân tỉnh (sau đây gọi tắt là Văn phòng)

1.2. Đối tượng áp dụng

Quy chế này áp dụng thống nhất đối với:

- Các phòng chuyên môn, đơn vị trực thuộc Văn phòng; cán bộ, công chức, viên chức, người lao động thuộc Văn phòng;
- Các cơ quan, tổ chức, cá nhân có sử dụng các hệ thống thông tin do Văn phòng UBND tỉnh triển khai.
- Các 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 và thuật ngữ chuyên môn

Để đảm bảo tính thống nhất trong việc thực thi, các thuật ngữ dưới đây được hiểu như sau:

2.1. An toàn thông tin mạng (ATTT) 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.

2.2. Hệ thống thông tin (HTTT): Được quy định tại Khoản 3 Điều 3 Luật An toàn thông tin mạng, cụ thể: Hệ thống thông tin là tập hợp các thành phần bao gồm phần cứng, phần mềm, dữ liệu và mạng kết nối được tổ chức để thu thập, xử lý, lưu trữ và truyền đưa thông tin phục vụ hoạt động của Văn phòng.

2.3. 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

2.4. Sự cố an toàn thông tin mạng (Incident): 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.

2.5. 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.

2.6. Phần mềm độc hại (Malware) được quy định tại Khoản 11 Điều 3 Luật An toàn thông tin mạng. Bao gồm nhưng không giới hạn ở: Virus, Worm (sâu máy tính), Trojan, Ransomware (mã độc tống tiền), Spyware (phần mềm gián điệp), và các loại mã độc được thiết kế để xâm nhập, phá hoại hoặc đánh cắp thông tin.

2.5. Tấn công từ chối dịch vụ (DoS/DDoS): Là hành vi sử dụng các kỹ thuật tấn công nhằm làm quá tải tài nguyên hệ thống (băng thông, CPU, RAM), khiến người dùng hợp pháp không thể truy cập vào dịch vụ hoặc hệ thống thông tin.

2.6. Kỹ thuật xã hội (Social Engineering): Là các hình thức tấn công dựa trên việc lừa đảo, thao túng tâm lý con người để lấy được thông tin mật, mật khẩu hoặc quyền truy cập hệ thống (ví dụ: lừa đảo qua email - Phishing, gọi điện mạo danh...).

2.7. Tài sản thông tin (Information Asset): Là bất kỳ thông tin hoặc vật mang tin nào (văn bản giấy, tệp tin số, cơ sở dữ liệu, thiết bị lưu trữ...) có giá trị đối với hoạt động của Văn phòng.

2.8. Truy cập trái phép (Unauthorized Access): Là việc một cá nhân hoặc tổ chức tiếp cận vào hệ thống, dữ liệu hoặc mạng mà không có sự cho phép bằng văn bản hoặc quyền hạn được phân cấp chính thức.

2.9. 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 đảm bảo an toàn thông tin

Việc triển khai Quy chế này nhằm đạt được các mục tiêu chiến lược sau:

1. Bảo vệ hạ tầng số: Đảm bảo hệ thống mạng, máy chủ và các ứng dụng của Văn phòng hoạt động liên tục, không bị gián đoạn bởi các cuộc tấn công mạng.

2. Bảo vệ tài sản dữ liệu: Ngăn chặn tuyệt đối việc lộ lọt thông tin bí mật nhà nước, thông tin nội bộ và dữ liệu cá nhân của cán bộ, công chức.

3. Nâng cao năng lực số: Xây dựng môi trường làm việc số an toàn, chuyên nghiệp, tạo nền tảng vững chắc cho lộ trình chuyển đổi số của tỉnh Hưng Yên.

4. Tuân thủ pháp luật: Đảm bảo mọi hoạt động ứng dụng CNTT của Văn phòng đều đáp ứng đầy đủ các quy định pháp luật hiện hành của Việt Nam.

Điều 4. Nguyên tắc đảm bảo an toàn thông tin

1. Nguyên tắc Phòng ngừa chủ động (Proactive Defense): An toàn thông tin không chỉ là việc ứng phó khi có sự cố, mà phải là hoạt động được lồng ghép ngay từ khâu lập kế hoạch, thiết kế và vận hành các hệ thống thông tin.

2. Nguyên tắc Phân cấp quản lý (Decentralization): Việc bảo đảm an toàn thông tin là trách nhiệm của toàn thể cán bộ, công chức. Trong đó, lãnh đạo đơn vị chịu trách nhiệm quản lý chung, bộ phận chuyên trách chịu trách nhiệm kỹ thuật, và cá nhân người dùng chịu trách nhiệm trực tiếp trên tài khoản và thiết bị được giao.

3. Nguyên tắc Quyền hạn tối thiểu (Least Privilege): Người dùng và các tài khoản hệ thống chỉ được cấp quyền truy cập vừa đủ để hoàn thành nhiệm vụ chuyên môn được giao. Mọi quyền hạn vượt mức phải được phê duyệt bằng văn bản.

4. Nguyên tắc Kiểm soát đa lớp (Defense in Depth): Áp dụng đồng bộ các biện pháp bảo mật từ lớp vật lý (phòng máy chủ, khóa cửa), lớp mạng (tường lửa, VLAN), lớp máy chủ (cập nhật bản vá, chống virus) đến lớp ứng dụng và lớp con người.

5. Nguyên tắc Lưu vết (Accountability): Mọi hoạt động truy cập, thay đổi dữ liệu và cấu hình hệ thống quan trọng phải được ghi lại nhật ký (log) để phục vụ công tác kiểm tra, giám sát và truy vết khi có sự cố xảy ra.

Điều 5. Những hành vi nghiêm cấm

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. Để duy trì kỷ luật an toàn thông tin, nghiêm cấm các hành vi sau đây:

5.1. Vi phạm về hạ tầng và kết nối:

a) Tự ý lắp đặt, kết nối các thiết bị phát sóng không dây (Wifi, Access Point), các thiết bị tiếp sóng, bộ kích sóng hoặc các thiết bị có chức năng định tuyến, chuyển tiếp gói tin không thuộc danh mục quản lý của Văn phòng vào hệ thống mạng nội bộ.

5.2. Vi phạm về dữ liệu và thông tin:

a) Truy cập, sao chép, phát tán, hoặc chia sẻ các tài liệu, dữ liệu thuộc danh mục Bí mật nhà nước hoặc thông tin nội bộ của Văn phòng ra bên ngoài (qua Email cá nhân, mạng xã hội, USB, đám mây công cộng...) khi chưa được sự cho phép của cấp có thẩm quyền.

b) Sử dụng các công cụ, phần mềm để can thiệp, thay đổi trái phép nội dung của các văn bản, dữ liệu trên hệ thống quản lý văn bản và điều hành.

c) Nghiêm cấm việc truy cập, sao chép, cung cấp, phát tán trái phép tài liệu, dữ liệu thuộc danh mục bí mật nhà nước hoặc thông tin nội bộ chưa được phép công khai của Văn phòng cho tổ chức, cá nhân không có thẩm quyền.

Việc trao đổi tài liệu phục vụ công tác qua các nền tảng điện tử, mạng xã hội hoặc ứng dụng nhắn tin chỉ được thực hiện đối với các thông tin phục vụ xử lý công việc thông thường, không thuộc phạm vi bí mật nhà nước và phải bảo đảm an toàn thông tin, đúng đối tượng nhận, không phát tán ra bên ngoài

5.3. Vi phạm về quản lý tài khoản và thiết bị:

a) Chia sẻ tài khoản/chứng thư, mật khẩu của cá nhân cho người khác hoặc cho phép người khác sử dụng máy tính công vụ đang đăng nhập tài khoản của mình.

b) Sử dụng mật khẩu yếu, dễ đoán hoặc không thực hiện thay đổi mật khẩu theo định kỳ quy định.

c) Tự ý cài đặt các phần mềm không rõ nguồn gốc, phần mềm bẻ khóa (crack), phần mềm chuyên dụng không phục vụ mục đích công việc lên máy tính công vụ.

d) Cắm các thiết bị lưu trữ ngoài (USB, ổ cứng di động, thẻ nhớ...) đã nhiễm mã độc hoặc chưa được kiểm định, kiểm tra trước khi sử dụng trong hệ thống thông tin tại Văn phòng.

5.4. Vi phạm về ý thức và trách nhiệm:

a) Cố ý bỏ qua các cảnh báo bảo mật của hệ thống hoặc không báo cáo kịp thời khi phát hiện các dấu hiệu bất thường về an toàn thông tin.

b) Sử dụng mạng nội bộ của Văn phòng vào các mục đích vi phạm pháp luật, truy cập các trang web chứa nội dung độc hại hoặc tham gia vào các hoạt động tấn công mạng.

Điều 6: 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. Các đơn vị được giao quản lý vận hành hệ thống thông tin phối hợp với Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh và các cơ quan, tổ chức có thẩm quyền quản lý về ATTT đảm bảo ATTT mạng cho các hệ thống thông tin do Văn phòng UBND tỉnh làm chủ quản.

b. Cán bộ phụ trách Công nghệ thông tin thuộc Văn phòng UBND tỉnh tham gia 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. Tham gia các hoạt động, công tác bảo đảm ATTT khi có yêu cầu của tổ chức có thẩm quyền.

Điều 7. 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, 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 8. 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 9. Quản lý nhà cung cấp sản phẩm, dịch vụ

1. Lập và cập nhật danh sách các nhà cung cấp sản phẩm, dịch vụ định kỳ. Đơn vị vận hành xây dựng quy trình đánh giá nhà cung cấp sản phẩm, dịch vụ an ninh mạng sau đó đánh giá và cập nhật danh sách tối thiểu 01 lần/năm hoặc khi xảy ra thay đổi ảnh hưởng đến danh sách.

2. Rà soát vấn đề bảo mật khi kết thúc hợp đồng với các nhà cung cấp dịch vụ.

Điều 10. 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. Yêu cầu 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) Bộ phận chuyên trách có trách nhiệm quản lý và lưu trữ mã nguồn an toàn.
 - c) Khi thay đổi mã nguồn, kiến trúc phần mềm thực hiện kiểm tra, đánh giá ATTT cho phần mềm.
 - d) Có cam kết của bên phát triển về bảo đảm tính bí mật và bản quyền của phần mềm phát triển.

Điều 11. 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. 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. Bộ phận chuyên trách và bên triển khai hệ thống xây dựng kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống, trình lãnh đạo đơn vị phê duyệt trước khi đưa hệ thống vào vận hành, khai thác.
4. Bộ phận 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.

ĐẢM BẢO AN TOÀN THÔNG TIN

TRONG QUẢN LÝ VẬN HÀNH HỆ THỐNG THÔNG TIN

Điều 12. Quản lý tài sản Công nghệ thông tin

1. Quản lý tài sản phần cứng và phần mềm: Lập danh sách, kiểm kê, rà soát và cập nhật danh sách cho tất cả tài sản thuộc hệ thống thông tin định kỳ tối thiểu 02 lần/năm.

2. Xây dựng quy trình xử lý tài sản chưa được quản lý: Rà soát, xử lý tài sản phần cứng không có trong danh sách định kỳ tối thiểu 01 lần/tháng và phần mềm trái phép định kỳ tối thiểu 01 lần/quý.

3. Quản lý tài sản thông tin: Mức độ nhạy cảm của tài sản thông tin phải được phân loại thành: Công khai, Nội bộ, Hạn chế truy cập, và Bí mật nhà nước. Định kỳ kiểm tra cấp độ phân quyền dữ liệu tối thiểu 01 lần/tháng.

Điều 13. Quản lý tài khoản

1. Quản lý tách biệt giữa các loại tài khoản dùng trong hệ thống thông tin (quản trị, nghiệp vụ, kỹ thuật, dịch vụ).

2. Xoá hoặc vô hiệu hoá các tài khoản không hoạt động sau 45 ngày hoặc ngay khi có thay đổi về nhân sự quản lý tài khoản. Định kỳ rà soát và cập nhật quy định quản lý tài khoản tối thiểu 01 lần/năm.

Điều 13. 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. Tập 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 cấp, 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 14. 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 cấp, cháy nổ, ngập lụt, động đất và các thảm họa khác do thiên nhiên hoặc do con người gây ra và các phương án khôi phục sau thảm họa 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 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.

e) Ứng dụng phải được định kỳ kiểm tra đánh giá an toàn thông tin 01 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 máy chủ và ứng dụng cho cán bộ 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 nguyên vẹn.

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

Điều 15. Quản lý lỗ hổng bảo mật và nhật ký an ninh mạng bảo mật

1. Lỗ hổng bảo mật: Rà soát và cập nhật quy trình đánh giá, xử lý lỗ hổng tối thiểu 01 lần/năm hoặc khi xảy ra thay đổi lớn.

2. Nhật ký (Log): Đảm bảo duy trì không gian lưu trữ nhật ký tối thiểu 12 tháng để tránh thất thoát dữ liệu. Định kỳ thực hiện rà soát nhật ký an ninh mạng tối thiểu 01 lần/tuần.

Điều 16. 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 thích hợp theo các chuẩn quốc gia hoặc quốc tế đã được công nhận để bảo vệ thông tin cùng mã kiểm tra tính nguyên 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. Sao lưu dự phòng và khôi phục dữ liệu

a) Lập danh sách các dữ liệu, phần mềm cần được sao lưu, có phân loại theo thời gian lưu trữ, thời gian sao lưu, phương pháp sao lưu và thời gian kiểm tra phục hồi hệ thống từ dữ liệu sao lưu.

b) Đơn vị vận hành xây dựng tài liệu, quy trình hướng dẫn sao lưu/phục hồi dữ liệu của hệ thống: 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....

Điều 17. Quản lý sự cố an toàn thông tin

1. Phân nhóm sự cố an toàn thông tin theo quy định tại Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ quy định về hệ

thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng Quốc gia (Quyết định 05/2017/QĐ-TTg).

2. Phương án tiếp nhận, phát hiện, phân loại và quy trình xử lý ban đầu sự cố an toàn thông tin mạng: Đơn vị được giao quản lý vận hành hệ thống xây dựng quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng theo quy định tại Điều 13,14 Quyết định số 05/2017/QĐ-TTg.

3. Kế hoạch ứng phó sự cố an toàn thông tin mạng: Phòng Hành chính - tổ chức phối hợp với Trung tâm Thông tin - Hội nghị, Trung tâm Phục vụ hành chính công xây dựng và triển khai kế hoạch ứng phó sự cố an toàn thông tin theo quy định tại Điều 16 Quyết định số 05/2017/QĐ-TTg.

4. Giám sát, phát hiện và cảnh báo sự cố an toàn thông tin

a. Đơn vị quản lý vận hành hệ thống thông tin thực hiện giám sát, phát hiện và cảnh báo sự cố an toàn thông tin, phối hợp với các đơn vị chuyên trách về ATTT đưa ra cảnh báo sớm về nguy cơ mất ATTT trong hệ thống.

b. Đối với người dùng: Thông tin, báo cáo kịp thời cho cán bộ chuyên trách về ATTT của đơn vị 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.

5. Bộ phận chuyên trách về ATTT có trách nhiệm quyết định toàn diện về mặt kỹ thuật trong quá trình khắc phục sự cố về ATTT; hỗ trợ, phối hợp và hướng dẫn các đơn vị khắc phục sự cố mất ATTT; yêu cầu dừng hoạt động một phần hoặc toàn bộ hệ thống thông tin của đơn vị nhằm phục vụ công tác khắc phục sự cố về ATTT; phối hợp với đơn vị trong điều tra các nguyên nhân gây ra sự cố mất ATTT theo chỉ đạo của Lãnh đạo;

6. 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.

7. Tổ chức diễn tập phương án xử lý sự cố an toàn thông tin theo chỉ đạo của lãnh đạo.

Điều 18. 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 19. 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 20. Quản lý điểm yếu an toàn hệ thống thông tin

1. Đơn vị vận hành hệ thống thông tin 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 21. 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 22. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ

1. Thực hiện việc hủy 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, hủy 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, hủy bỏ hệ thống thông tin được thực hiện theo quy định của pháp luật hiện hành.

CHƯƠNG IV. TRÁCH NHIỆM TỔ CHỨC THỰC HIỆN

Điều 23. Trách nhiệm của Lãnh đạo Văn phòng

1. Chịu trách nhiệm cao nhất trước UBND tỉnh về việc bảo đảm an toàn thông tin mạng trong mọi hoạt động của Văn phòng.

2. Phê duyệt các kế hoạch, phương án đầu tư, nâng cấp hạ tầng và các quy trình ứng phó sự cố.

3. Chỉ đạo điều động nguồn lực, nhân sự và kinh phí để xử lý kịp thời các sự cố khẩn cấp.

Điều 24. Trách nhiệm của Phòng Hành chính - Quản trị

1. Chủ trì tham mưu lãnh đạo Văn phòng UBND tỉnh xây dựng, sửa đổi, bổ sung và tổ chức thực hiện Quy chế này.

2. Chủ trì tham mưu xây dựng kế hoạch, chương trình, phương án bảo đảm an toàn thông tin mạng tại Văn phòng UBND tỉnh.

3. Chủ trì tham mưu bố trí kinh phí, mua sắm, nâng cấp trang thiết bị, phần mềm và các giải pháp phục vụ công tác bảo đảm an toàn thông tin mạng.

4. Phối hợp với Trung tâm Thông tin Hội nghị tỉnh tổ chức kiểm tra việc thực hiện Quy chế; tổng hợp, báo cáo tình hình an toàn thông tin mạng theo quy định.

5. Phối hợp tổ chức tuyên truyền, tập huấn, nâng cao nhận thức về an toàn thông tin cho cán bộ, công chức, viên chức và người lao động.

Điều 25. Trách nhiệm của Trung tâm Thông tin Hội nghị tỉnh

1. Trực tiếp quản lý, vận hành hạ tầng mạng, máy chủ, hệ thống thông tin, thiết bị bảo mật và các nền tảng kỹ thuật dùng chung của Văn phòng UBND tỉnh.

2. Triển khai các biện pháp kỹ thuật nhằm bảo đảm an toàn thông tin mạng; tổ chức giám sát, phát hiện, cảnh báo và xử lý nguy cơ mất an toàn thông tin.

3. Thực hiện rà soát lỗ hổng bảo mật, sao lưu dữ liệu, cập nhật bản vá, kiểm tra an toàn hệ thống định kỳ theo quy định.

4. Chủ trì hoặc phối hợp xử lý sự cố an toàn thông tin; phối hợp với cơ quan chức năng trong công tác điều tra, truy vết, khắc phục sự cố an toàn thông tin mạng.

5. Hướng dẫn kỹ thuật, hỗ trợ người sử dụng trong việc bảo đảm an toàn thông tin khi khai thác, sử dụng hệ thống thông tin.

Điều 26. Trách nhiệm của Trung tâm Phục vụ hành chính công tỉnh

1. Tổ chức thực hiện các quy định về bảo đảm an toàn thông tin mạng đối với hệ thống, thiết bị và tài khoản được giao quản lý, sử dụng tại Trung tâm.

2. Phối hợp với Trung tâm Thông tin Hội nghị tỉnh trong công tác quản lý, vận hành, xử lý sự cố và bảo đảm an toàn thông tin đối với các hệ thống phục vụ giải quyết thủ tục hành chính.

3. Quản lý cán bộ, công chức, viên chức, người lao động thuộc phạm vi quản lý trong việc chấp hành Quy chế này.

Điều 27. Trách nhiệm của các Phòng, Ban, Đơn vị trực thuộc

1. Phổ biến và đôn đốc cán bộ, công chức thuộc đơn vị mình thực hiện nghiêm túc các quy định trong Quy chế này.

2. Chịu trách nhiệm về an toàn thông tin đối với các tài sản, dữ liệu và thiết bị được giao quản lý tại đơn vị.

3. Phối hợp chặt chẽ với bộ phận chuyên trách trong việc cung cấp thông tin và thực hiện các biện pháp khắc phục khi có sự cố xảy ra tại đơn vị.

Điều 28. Trách nhiệm của cán bộ, công chức, viên chức và người lao động

1. Thực hiện đúng các quy định về mật khẩu, quản lý thiết bị, sử dụng phần mềm và bảo mật dữ liệu.

2. Chủ động nhận diện các dấu hiệu bất thường và báo cáo ngay cho bộ phận chuyên trách theo đúng quy trình.

3. Có ý thức bảo vệ thiết bị công vụ, không tự ý can thiệp vào cấu hình kỹ thuật hoặc cài đặt các phần mềm không được phép.

4. Chịu trách nhiệm trước pháp luật và trước Lãnh đạo Văn phòng nếu để xảy ra mất an toàn thông tin do vi phạm các quy định đã được ban hành.

Điều 29. Khen thưởng và xử lý vi phạm

1. Những cá nhân, tập thể có thành tích xuất sắc trong việc phát hiện sớm các nguy cơ, ngăn chặn hiệu quả các cuộc tấn công mạng hoặc có sáng kiến nâng cao tính an toàn cho hệ thống sẽ được xem xét khen thưởng theo quy định.

2. Các hành vi vi phạm Quy chế này, tùy theo tính chất, mức độ và hậu quả gây ra, sẽ bị xử lý theo các hình thức: nhắc nhở, phê bình tại đơn vị; kỷ luật cán bộ, công chức theo quy định của Luật Cán bộ, công chức; truy cứu trách nhiệm dân sự; truy cứu trách nhiệm hình sự nếu có dấu hiệu tội phạm theo quy định của pháp luật.

Điều 30. Tổ chức triển khai Quy chế

1. Quy định trong Quy chế này có hiệu lực thi hành kể từ ngày ký ban hành.

2. 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.

3. Trong quá trình thực hiện, nếu có vấn đề phát sinh hoặc không còn phù hợp với thực tế, Phòng Hành chính - Quản trị có trách nhiệm tổng hợp, báo cáo Lãnh đạo Văn phòng để xem xét sửa đổi, bổ sung cho phù hợp./.