ỦY BAN NHÂN DÂN TỈNH GIA LAI	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 02 /2026/QĐ-UBND	*Gia Lai, ngày 08 tháng 01 năm 2026*

QUYẾT ĐỊNH

Ban hành Quy chế bảo đảm an toàn thông tin, an ninh mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Gia Lai

Căn cứ Luật Tổ chức Chính quyền địa phương số 72/2025/QH15;

Căn cứ Luật Ban hành văn bản quy phạm pháp luật số 64/2025/QH15 được sửa đổi, bổ sung một số điều theo Luật số 87/2025/QH15;

Căn cứ Luật Công nghệ thông tin số 67/2006/QH11;

Căn cứ Luật An toàn thông tin mạng số 86/2015/QH13;

Căn cứ Luật An ninh mạng số 24/2018/QH14;

Căn cứ Luật Bảo vệ bí mật nhà nước số 29/2018/QH14;

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 Nghị định số 142/2016/NĐ-CP ngày 14 tháng 10 năm 2016 của Chính phủ về ngăn chặn xung đột thông tin trên mạng;

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

Căn cứ Nghị định số 13/2023/NĐ-CP ngày 17 tháng 4 năm 2023 của Chính phủ về bảo vệ dữ liệu cá nhân;

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 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 tháng 9 năm 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 16/2024/TT-BTTTT ngày 30 tháng 12 năm 2024 của Bộ trưởng Bộ Thông tin và Truyền thông 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;

Căn cứ Thông tư số 31/2017/TT-BTTTT ngày 15 tháng 11 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị

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

Căn cứ Thông tư số 19/2023/TT-BTTTT ngày 25 tháng 12 năm 2023 của Bộ trưởng Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của 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;

Theo đề nghị của Giám đốc Công an tỉnh;

Ủy ban nhân dân tỉnh Quyết định ban hành Quy chế bảo đảm an toàn thông tin, an ninh mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Gia Lai.

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn thông tin, an ninh mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Gia Lai.

Điều 2. Quyết định này có hiệu lực thi hành từ ngày 20 tháng 01 năm 2026.

Quyết định số 22/2021/QĐ-UBND của Ủy ban nhân dân tỉnh Bình Định ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Bình Định; Quyết định số 41/2016/QĐ-UBND của Ủy ban nhân dân tỉnh Gia Lai ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước trên địa bàn tỉnh Gia Lai hết hiệu lực kể từ ngày Quyết định này có hiệu lực thi hành.

Điều 3. Chánh Văn phòng Ủy ban nhân dân tỉnh, Giám đốc Công an tỉnh, Thủ trưởng các sở, ban, ngành; Chủ tịch Ủy ban nhân dân các xã, phường; các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Văn phòng Chính phủ;
- Cục A05 - Bộ Công an;
- Cục KTVB&QLXLVPHC;
- Thường trực Tỉnh ủy;
- Thường trực HĐND tỉnh;
- CT, các PCT UBND tỉnh;
- Ủy ban MTTQ Việt Nam tỉnh;
- Đoàn ĐBQH tỉnh;
- Văn phòng Tỉnh ủy;
- Lãnh đạo VPUBND tỉnh;
- Trung tâm PVHCC;
- Lưu: VT, V9.

TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Lâm Hải Giang

ỦY BAN NHÂN DÂN **TỈNH GIA LAI**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**

QUY CHẾ

Bảo đảm an toàn thông tin, an ninh mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Gia Lai

(Ban hành kèm theo Quyết định số /2026/QĐ-UBND ngày / /2026 của Ủy ban nhân dân tỉnh Gia Lai)

Chương I
QUY ĐỊNH CHUNG

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

1. Phạm vi điều chỉnh: Quy chế này quy định về công tác bảo đảm an toàn thông tin, an ninh mạng trong hoạt động ứng dụng công nghệ thông tin (CNTT) của các cơ quan nhà nước trên địa bàn tỉnh Gia Lai.

2. Đối tượng áp dụng:

a) Các sở, ban, ngành; Ban Quản lý Khu kinh tế tỉnh; các đơn vị trực thuộc Ủy ban nhân dân tỉnh; các đơn vị trực thuộc sở, ban, ngành; Ủy ban nhân dân cấp xã và các đơn vị trực thuộc Ủy ban nhân dân cấp xã.

b) Các tổ chức chính trị - xã hội do ngân sách nhà nước bảo đảm kinh phí hoạt động, có sử dụng các hệ thống thông tin do Ủy ban nhân dân tỉnh triển khai.

c) Cán bộ, công chức, viên chức, người lao động đang làm việc trong các cơ quan, đơn vị quy định tại điểm a, b khoản này.

d) Các tổ chức, cá nhân cung cấp dịch vụ công nghệ thông tin, an toàn thông tin, an ninh mạng tham gia kết nối vào các hệ thống thông tin của tỉnh hoặc có liên quan trực tiếp đến công tác bảo đảm an toàn thông tin, an ninh mạng trên địa bàn tỉnh.

3. Các văn bản quy phạm pháp luật được viện dẫn trong Quy chế này khi được sửa đổi, bổ sung, thay thế, bãi bỏ bằng các văn bản khác thì nội dung viện dẫn được áp dụng theo các văn bản sửa đổi, bổ sung, thay thế, bãi bỏ đó.

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 số và các 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. *An ninh mạng:* Là việc bảo đảm thông tin trên mạng không gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội, bí mật nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân.

3. *Hệ thống thông tin:* Là tập hợp phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên mạng.

4. *Chủ quản hệ thống thông tin:* Là cơ quan, tổ chức, cá nhân có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin.

5. *Đơn vị vận hành hệ thống thông tin:* Là cơ quan, tổ chức được chủ quản hệ thống thông tin giao nhiệm vụ vận hành hệ thống thông tin.

6. *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.

7. *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.

8. *Phần mềm độc hại (mã độc):* Là phần mềm có khả năng gây ra hoạt động bất thường hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong hệ thống thông tin.

9. *Mật khẩu mạnh:* Là một chuỗi có tối thiểu 08 ký tự, bao gồm chữ thường, chữ in hoa, ký tự đặc biệt, chữ số và được yêu cầu thay đổi định kỳ ít nhất 90 ngày một lần.

10. *Trung tâm dữ liệu:* Là cơ sở hạ tầng tích hợp được thiết kế để lưu trữ, quản lý và xử lý dữ liệu, bao gồm các thành phần chính như máy chủ, thiết bị lưu trữ, thiết bị mạng, hệ thống làm mát, nguồn điện dự phòng và các biện pháp bảo mật vật lý, bảo đảm hoạt động ổn định, an toàn và liên tục.

11. *Tường lửa (Firewall):* là một hệ thống an ninh mạng (phần cứng hoặc phần mềm) giám sát và kiểm soát lưu lượng mạng đến và đi dựa trên các quy tắc bảo mật đã được xác định trước.

12. *Nhật ký (log):* là một tập hợp các bản ghi được tạo ra liên tục bởi một hệ thống, ứng dụng hoặc thiết bị, ghi lại các sự kiện, trạng thái, cảnh báo hoặc lỗi xảy ra trong quá trình hoạt động.

13. *Mạng riêng ảo (VPN):* là công nghệ cho phép tạo một kết nối an toàn, được mã hóa qua một mạng công cộng (như Internet) tới một mạng riêng.

14. *Dữ liệu nhạy cảm:* Là dữ liệu có thông tin mật, thông tin lưu hành nội bộ của đơn vị hoặc do đơn vị quản lý, mà việc tiết lộ trái phép có thể gây ảnh hưởng tiêu cực đến danh tiếng, tài chính và hoạt động của đơn vị.

15. *Dữ liệu cá nhân:* là thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự trên môi trường điện tử gắn liền với một con người cụ thể hoặc giúp xác định một con người cụ thể.

Điều 3. Nguyên tắc chung

1. Bảo đảm an toàn thông tin, an ninh mạng là yêu cầu bắt buộc, thường xuyên, liên tục, xuyên suốt quá trình thiết kế, xây dựng, quản lý vận hành, bảo trì, bảo dưỡng, nâng cấp, hủy bỏ hệ thống thông tin.

2. Việc bảo đảm an toàn thông tin phải được thực hiện trên cơ sở tuân thủ các quy định của pháp luật về an toàn thông tin, an ninh mạng, bảo vệ bí mật nhà nước, bảo vệ dữ liệu cá nhân và các quy định khác có liên quan.

3. Thủ trưởng các cơ quan, đơn vị là người chịu trách nhiệm trực tiếp chỉ đạo công tác bảo đảm an toàn thông tin, an ninh mạng và xác định rõ quyền hạn, trách nhiệm của Thủ trưởng, các phòng, cá nhân trong cơ quan, đơn vị.

4. Bố trí nguồn lực phù hợp với quy mô và điều kiện của cơ quan, đơn vị nhằm tối ưu hóa công tác bảo đảm an toàn thông tin, an ninh mạng trên cơ sở hài hòa giữa lợi ích, chi phí và mức độ chấp nhận rủi ro.

5. Việc xử lý sự cố an toàn thông tin, an ninh mạng phải phù hợp với trách nhiệm, quyền hạn và bảo đảm lợi ích hợp pháp của cơ quan, đơn vị, cá nhân liên quan và theo quy định của pháp luật.

6. Thông tin thuộc Danh mục bí mật nhà nước được bảo vệ theo quy định của pháp luật về bảo vệ bí mật nhà nước.

7. Mỗi cán bộ, công chức, viên chức, người lao động tại các đơn vị phải có trách nhiệm chủ động, tự giác áp dụng các biện pháp an toàn thông tin, an ninh mạng.

Điều 4. Các hành vi bị nghiêm cấm

Tuân thủ nghiêm các quy định về hành vi bị nghiêm cấm tại Điều 8 Luật An ninh mạng năm 2018, Điều 7 Luật An toàn thông tin mạng năm 2015, Điều 5 Luật Bảo vệ bí mật nhà nước năm 2018 và các quy định khác của pháp luật có liên quan.

Chương II
BẢO ĐẢM AN TOÀN THÔNG TIN, AN NINH MẠNG

Điều 5. Đào tạo, bồi dưỡng nghiệp vụ, tuyên truyền, phổ biến nâng cao nhận thức về an toàn thông tin, an ninh mạng

1. Các cơ quan, đơn vị có trách nhiệm tổ chức đào tạo, bồi dưỡng kiến thức, kỹ năng về an toàn thông tin, an ninh mạng cho cán bộ quản lý, cán bộ kỹ thuật và người sử dụng máy tính thuộc đơn vị.

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

3. Cán bộ, công chức, viên chức, người lao động phải tuân thủ nghiêm các quy định về an toàn, an ninh thông tin của cơ quan, đơn vị mình.

Điều 6. Quản lý nhân sự và quyền truy cập

1. Các cơ quan, đơn vị cần xây dựng quy trình cấp mới, quản lý và thu hồi tài khoản, phân quyền truy cập các hệ thống thông tin đối với các cá nhân do cơ quan, đơn vị quản lý.

2. Khi cá nhân chấm dứt hoặc thay đổi công việc, cơ quan, đơn vị phải xác định rõ trách nhiệm của cá nhân và các bên liên quan; lập biên bản bàn giao tài sản CNTT; thay đổi hoặc thu hồi quyền truy cập các hệ thống thông tin.

3. Cán bộ quản trị phải vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc.

Điều 7. Quản lý và sử dụng máy tính, thiết bị đầu cuối

1. Quy định chung đối với máy tính kết nối mạng:

a) Máy tính phải được cài đặt phần mềm hợp lệ (có bản quyền hoặc mã nguồn mở có nguồn gốc rõ ràng); việc cài đặt hoặc gỡ bỏ các phần mềm phải được sự chấp thuận của bộ phận chuyên trách về công nghệ thông tin.

b) Phải cài đặt phần mềm phòng chống mã độc tập trung và thiết lập chế độ tự động cập nhật cơ sở dữ liệu.

c) Phải được cấu hình vô hiệu hóa tính năng tự động thực thi (autoplay) các tệp tin trên các thiết bị lưu trữ di động.

d) Thực hiện thao tác khóa máy tính (sử dụng tính năng có sẵn trên máy tính) khi rời khỏi nơi đặt máy tính; tắt máy tính khi rời khỏi đơn vị.

đ) Khi phát hiện dấu hiệu nhiễm mã độc, người dùng phải ngắt kết nối và thông báo cho bộ phận chuyên trách về công nghệ thông tin để xử lý kịp thời.

2. Quản lý thiết bị lưu trữ di động:

a) Chỉ sử dụng thiết bị lưu trữ di động cho các hoạt động nghiệp vụ, quản lý khi được phép và phải thực hiện các biện pháp bảo đảm an toàn như mã hóa dữ liệu, quét mã độc định kỳ.

b) Phải quét mã độc thiết bị lưu trữ ngoài (thẻ nhớ, ổ đĩa ngoài...) trước khi sử dụng.

Điều 8. Bảo vệ bí mật Nhà nước trong ứng dụng công nghệ thông tin

1. Máy tính soạn thảo văn bản chứa nội dung bí mật nhà nước:

a) Là máy tính độc lập, không được kết nối và không từng kết nối với mạng Internet, mạng nội bộ hoặc bất kỳ mạng nào khác.

b) Được thiết lập cơ chế đăng nhập, đặt mật khẩu mạnh.

c) Nghiêm cấm sử dụng máy tính nối mạng để soạn thảo, chuyển giao, lưu trữ thông tin có nội dung bí mật nhà nước hoặc đưa thông tin bí mật nhà nước lên không gian mạng.

2. Quản lý thiết bị:

a) Máy vi tính, các thiết bị có chức năng lưu giữ trang bị cho công tác bảo vệ bí mật nhà nước, trước khi đưa vào sử dụng phải qua kiểm định của cơ quan

chức năng.

b) Khi máy tính dùng để soạn thảo văn bản mật có sự cố, đơn vị phải thông báo cho bộ phận chuyên trách để xử lý theo quy định, không được tự ý sửa chữa.

c) Ổ cứng và các bộ phận lưu trữ của máy tính xử lý thông tin mật khi hỏng hoặc thanh lý phải được xử lý (niêm phong, lưu trữ hoặc tiêu hủy) theo quy định về vật mang bí mật nhà nước.

Điều 9. Bảo đảm an toàn hệ thống mạng

1. Hệ thống mạng nội bộ phải được thiết kế phân vùng theo chức năng và mức độ an toàn, bao gồm tối thiểu: vùng mạng người dùng, vùng mạng máy chủ công cộng, vùng mạng máy chủ nội bộ và vùng mạng quản trị.

2. Dữ liệu trao đổi giữa các vùng mạng phải được kiểm soát chặt chẽ bởi hệ thống tường lửa và các thiết bị bảo mật. Nhật ký (log) về luồng dữ liệu phải được thu thập và chia sẻ về Trung tâm An ninh mạng tỉnh để giám sát tập trung.

3. Mạng không dây phải sử dụng chế độ xác thực mạnh (như WPA2-Enterprise) hoặc mật khẩu mạnh và được thay đổi định kỳ đối với mạng nội bộ. Mạng không dây dành cho khách phải được cách ly hoàn toàn với mạng nội bộ.

4. Hệ thống mạng kết nối Internet phải có hệ thống tường lửa, hệ thống bảo vệ truy cập Internet, và có khả năng bảo vệ trước các loại tấn công từ chối dịch vụ (DDoS); thực hiện lọc bỏ, ngăn chặn truy cập các trang tin được xác định là chứa mã độc hoặc nội dung không phù hợp.

5. Truy cập từ xa vào mạng nội bộ phải thông qua kết nối mạng riêng ảo (VPN) được mã hóa, có kiểm soát và áp dụng hình thức xác thực đa yếu tố (MFA).

Điều 10. Mạng truyền số liệu chuyên dùng

Quản lý, vận hành và bảo đảm an toàn thông tin đối với Mạng truyền số liệu chuyên dùng phục vụ các cơ quan Đảng, Nhà nước phải tuân thủ các quy định của Thủ tướng Chính phủ và hướng dẫn của Bộ Khoa học và Công nghệ. Chỉ được sử dụng cho mục đích công vụ, không được kết nối trực tiếp ra Internet.

Điều 11. Quản lý Trung tâm dữ liệu/Phòng máy chủ

1. Các thiết bị tường lửa, máy chủ, hệ thống lưu trữ... phải được đặt trong Trung tâm dữ liệu/Phòng máy chủ và thiết lập cơ chế bảo vệ, theo dõi phát hiện xâm nhập và biện pháp kiểm soát truy cập vật lý phù hợp.

2. Máy chủ phải được cài đặt phần mềm phòng chống mã độc và quản lý thống nhất, tập trung. Nhật ký hoạt động của thiết bị, phần mềm bảo đảm thời gian lưu giữ theo đúng cấp độ an toàn của hệ thống thông tin.

3. Mang thiết bị vào, ra Trung tâm dữ liệu/Phòng máy chủ để lắp đặt hoặc sửa chữa phải có sự chấp thuận của Lãnh đạo đơn vị quản lý, vận hành.

Điều 12. Xác định cấp độ an toàn hệ thống thông tin

1. Hệ thống thông tin phải được xác định cấp độ an toàn, thẩm định, phê duyệt Hồ sơ đề xuất cấp độ và xây dựng, triển khai phương án bảo đảm an toàn

tương ứng theo đúng quy định tại Nghị định số 85/2016/NĐ-CP và Thông tư số 12/2022/TT-BTTTT.

2. Khi thực hiện nâng cấp, mở rộng hệ thống thông tin, đơn vị chủ quản phải rà soát, đánh giá lại cấp độ an toàn và thực hiện điều chỉnh, bổ sung phương án bảo đảm an toàn cho phù hợp.

3. Tất cả các hệ thống thông tin phải được bảo vệ theo mô hình bảo đảm an toàn thông tin 4 lớp theo chỉ đạo của Thủ tướng Chính phủ và hướng dẫn của các cơ quan chuyên trách.

Điều 13. Bảo đảm an toàn ứng dụng

1. Yêu cầu về bảo đảm an toàn thông tin, an ninh mạng phải được lồng ghép vào các công đoạn thiết kế, xây dựng, triển khai và vận hành, sử dụng phần mềm ứng dụng.

2. Phần mềm ứng dụng phải đáp ứng các yêu cầu sau: áp dụng xác thực đa yếu tố khi đăng nhập; cấu hình để xác thực người sử dụng; giới hạn số lần đăng nhập sai liên tiếp; giới hạn thời gian để chờ đóng phiên kết nối; mã hóa thông tin xác thực trên hệ thống; không khuyến khích việc đăng nhập tự động.

3. Chỉ cho phép sử dụng các giao thức mạng có hỗ trợ chức năng mã hóa thông tin (SSH, TLS, VPN hoặc tương đương) khi truy cập, quản trị phần mềm, ứng dụng từ xa.

Điều 14. Quản lý tài khoản truy cập và mật khẩu

1. Mỗi cá nhân, đơn vị thuộc tỉnh được cấp một tài khoản định danh duy nhất từ Hệ thống định danh và xác thực tập trung của tỉnh để truy cập các hệ thống thông tin. Việc sử dụng chung tài khoản bị nghiêm cấm.

2. Mật khẩu của người dùng phải tuân thủ định nghĩa về mật khẩu mạnh và phải được thay đổi định kỳ tối thiểu 90 ngày/lần. Hệ thống có cơ chế bắt buộc người dùng thay đổi mật khẩu ngay trong lần đăng nhập đầu tiên và có chức năng tự động khóa tài khoản tạm thời sau 05 lần đăng nhập sai liên tiếp.

3. Tài khoản quản trị hệ thống phải tách biệt với tài khoản truy cập của người sử dụng thông thường, được giao đích danh cá nhân làm công tác quản trị và phải đặt mật khẩu mạnh tối thiểu 14 ký tự.

4. Đơn vị quản lý, vận hành hệ thống thông tin có quyền khóa tài khoản truy cập trong trường hợp phát hiện tài khoản đó có hành vi tấn công hoặc gây mất an toàn thông tin, an ninh mạng.

Điều 15. Quản lý và sử dụng chữ ký số, chứng thư số

1. Chữ ký số và chứng thư số chuyên dùng trong các cơ quan nhà nước được cấp bởi tổ chức cung cấp dịch vụ chứng thực chữ ký số chuyên dùng Chính phủ (Ban Cơ yếu Chính phủ) hoặc các tổ chức được cấp phép.

2. Cá nhân được cấp chữ ký số, chứng thư số chịu trách nhiệm quản lý, bảo vệ an toàn, bí mật khóa bí mật và thiết bị lưu khóa bí mật.

3. Nghiêm cấm việc cho người khác mượn thiết bị lưu khóa bí mật hoặc sử dụng chữ ký số được cấp vào các mục đích cá nhân, không phục vụ công vụ.

Điều 16. Sao lưu và phục hồi dữ liệu

1. Công tác sao lưu và phục hồi dữ liệu là yêu cầu bắt buộc đối với tất cả các hệ thống thông tin, nhằm bảo đảm tính sẵn sàng, toàn vẹn của dữ liệu.

2. Đơn vị chủ quản hệ thống thông tin có trách nhiệm xây dựng và tổ chức thực hiện kế hoạch sao lưu, phục hồi dữ liệu, xác định rõ danh mục dữ liệu cần sao lưu, tần suất, phương tiện lưu trữ và nơi lưu trữ (phải độc lập với hệ thống chính).

3. Dữ liệu sao lưu quan trọng phải được mã hóa để bảo vệ tính bí mật của dữ liệu.

4. Đơn vị vận hành hệ thống thông tin phải định kỳ tổ chức kiểm tra tính toàn vẹn và diễn tập phục hồi dữ liệu.

Điều 17. Đảm bảo hoạt động liên tục

1. Đơn vị phải xây dựng hoặc thuê hệ thống dự phòng cho các hệ thống thông tin quan trọng thuộc phạm vi quản lý của mình.

2. Hệ thống dự phòng phải bảo đảm khả năng thay thế hệ thống chính trong thời gian tối đa (04) bốn giờ đồng hồ tính từ thời điểm hệ thống chính phát sinh sự cố không thể khắc phục.

Điều 18. Quản lý rủi ro an toàn thông tin, an ninh mạng

1. Ban hành quy định, quy trình quản lý rủi ro an toàn thông tin, an ninh mạng nội bộ, xác định rõ phạm vi, vai trò, trách nhiệm của các bộ phận liên quan.

2. Chủ quản hệ thống thông tin tổ chức đánh giá rủi ro an toàn thông tin định kỳ tối thiểu 01 lần/năm hoặc khi có sự thay đổi lớn về kiến trúc hệ thống.

3. Căn cứ vào đánh giá rủi ro, cần rà soát, bổ sung các yêu cầu an toàn (biện pháp kiểm soát rủi ro) cho phù hợp với yêu cầu thực tế, tuân thủ các quy định pháp luật.

Điều 19. Giám sát an toàn thông tin, an ninh mạng

1. Các hệ thống thông tin phải được thực hiện giám sát an toàn thông tin, an ninh mạng, kết nối vào Trung tâm An ninh mạng của tỉnh và chia sẻ kết quả giám sát về Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT), Trung tâm An ninh mạng quốc gia thuộc Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an.

2. Đơn vị vận hành hệ thống thông tin có trách nhiệm phối hợp với Công an tỉnh tổ chức thực hiện giám sát hệ thống thông tin theo Nghị định số 53/2022/NĐ-CP và Thông tư số 31/2017/TT-BTTTT.

Điều 20. Ứng cứu sự cố an toàn thông tin mạng

1. Kế hoạch ứng phó sự cố an toàn thông tin, an ninh mạng được xây dựng, phê duyệt hằng năm đối với các hệ thống thông tin do đơn vị trực tiếp quản lý.

2. Quy trình ứng cứu sự cố an toàn thông tin mạng tuân thủ quy định tại Quyết định số 05/2017/QĐ-TTg và Thông tư số 20/2017/TT-BTTTT, bao gồm: Phát hiện, tiếp nhận, phân loại, xử lý ban đầu, phân tích, khắc phục và công bố thông tin.

Điều 21. Bảo đảm an toàn thông tin, an ninh mạng cho hệ thống thông tin quan trọng quốc gia

1. Các cơ quan, đơn vị có trách nhiệm rà soát, xác định các hệ thống thông tin thuộc phạm vi quản lý có khả năng thuộc Danh mục lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng và lập hồ sơ đề nghị đưa vào danh mục hệ thống thông tin quan trọng quốc gia theo quy định.

2. Việc bảo đảm an toàn thông tin, an ninh mạng cho Hệ thống thông tin quan trọng quốc gia phải được ưu tiên hàng đầu, được đầu tư nguồn lực tương xứng và áp dụng các biện pháp quản lý, kỹ thuật tăng cường.

3. Các hệ thống thông tin quan trọng quốc gia, đơn vị chủ quản phải tổ chức đánh giá rủi ro an toàn thông tin một cách toàn diện, chi tiết định kỳ hằng năm. Kết nối vào Trung tâm An ninh mạng tỉnh, chia sẻ dữ liệu, giám sát liên tục 24/7.

Chương III
BẢO VỆ DỮ LIỆU CÁ NHÂN

Điều 22. Nguyên tắc và yêu cầu chung trong xử lý dữ liệu cá nhân

1. Việc xử lý dữ liệu cá nhân tại các cơ quan, đơn vị phải tuân thủ đầy đủ các nguyên tắc quy định tại Điều 3 Nghị định số 13/2023/NĐ-CP.

2. Mọi hoạt động thu thập, xử lý dữ liệu cá nhân phải được sự đồng ý của chủ thể dữ liệu, trừ trường hợp pháp luật có quy định khác. Dữ liệu chỉ được xử lý đúng mục đích đã đăng ký hoặc thông báo.

3. Các cơ quan, đơn vị áp dụng các biện pháp quản lý và kỹ thuật phù hợp để bảo vệ dữ liệu cá nhân trong suốt quá trình xử lý, lưu trữ và hủy bỏ.

Điều 23. Quyền và nghĩa vụ của các bên liên quan

1. Chủ thể dữ liệu là cán bộ, công chức, viên chức, người lao động và công dân có các quyền và nghĩa vụ theo quy định tại Nghị định số 13/2023/NĐ-CP.

2. Thủ trưởng cơ quan, đơn vị chịu trách nhiệm trước pháp luật và cấp trên về việc bảo đảm an toàn dữ liệu cá nhân thuộc phạm vi quản lý của đơn vị mình.

3. Cán bộ, công chức, viên chức và người lao động được giao nhiệm vụ xử lý dữ liệu cá nhân có trách nhiệm bảo mật thông tin, không được tiết lộ, chia sẻ dữ liệu trái phép và phải chịu trách nhiệm nếu để xảy ra lộ, lọt dữ liệu.

Điều 24. Trách nhiệm bảo vệ dữ liệu cá nhân của cơ quan, đơn vị

1. Các cơ quan, đơn vị là Bên Kiểm soát dữ liệu hoặc Bên Kiểm soát và xử lý dữ liệu cá nhân có trách nhiệm:

a) Phân công bộ phận hoặc nhân sự phụ trách bảo vệ dữ liệu cá nhân.

b) Xây dựng và ban hành quy định nội bộ về bảo vệ dữ liệu cá nhân.

c) Thực hiện đánh giá tác động xử lý dữ liệu cá nhân và lập hồ sơ gửi Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (Bộ Công an) theo quy định.

2. Khi phát hiện vi phạm hoặc sự cố về dữ liệu cá nhân, cơ quan, đơn vị phải tiến hành các biện pháp khắc phục ngay lập tức và thông báo cho cơ quan chuyên trách bảo vệ dữ liệu cá nhân chậm nhất là 72 giờ kể từ khi xảy ra sự cố.

3. Áp dụng các biện pháp bảo vệ dữ liệu cá nhân trong hoạt động ứng dụng công nghệ thông tin, bao gồm: quản lý quyền truy cập, ghi nhật ký hệ thống, mã hóa dữ liệu quan trọng và các biện pháp kỹ thuật khác theo hướng dẫn của cơ quan chức năng.

Chương IV
KIỂM TRA, ĐÁNH GIÁ, QUẢN LÝ RỦI RO VÀ CHẾ ĐỘ BÁO CÁO

Điều 25. Kiểm tra, đánh giá an toàn thông tin và an ninh mạng

1. Mục đích kiểm tra, đánh giá: Đánh giá hiện trạng và mức độ tuân thủ các quy định của pháp luật và Quy chế này; phát hiện sớm các lỗ hổng, điểm yếu, rủi ro tiềm ẩn trong các hệ thống thông tin để đưa ra các biện pháp khắc phục, xử lý.

2. Nội dung kiểm tra, đánh giá:

a) Kiểm tra việc tuân thủ các quy định của pháp luật về bảo đảm an toàn thông tin theo cấp độ tại Nghị định số 85/2016/NĐ-CP, Thông tư số 12/2022/TT-BTTTT và các quy định tại Quy chế này.

b) Đánh giá hiệu quả các biện pháp quản lý và kỹ thuật bảo đảm an toàn hệ thống thông tin.

c) Kiểm tra, phát hiện mã độc, lỗ hổng, điểm yếu hệ thống thông tin.

3. Hình thức kiểm tra:

a) Kiểm tra định kỳ: thực hiện theo kế hoạch hằng năm được cấp có thẩm quyền phê duyệt.

b) Kiểm tra đột xuất: thực hiện khi có yêu cầu của cơ quan quản lý nhà nước có thẩm quyền hoặc khi xuất hiện các nguy cơ, sự cố an ninh mạng nghiêm trọng.

4. Công an tỉnh chủ trì, phối hợp với các đơn vị liên quan tổ chức kiểm tra, đánh giá việc thực hiện Quy chế này tại các cơ quan, đơn vị và báo cáo Ủy ban nhân dân tỉnh.

Điều 26. Chế độ báo cáo

Các cơ quan, đơn vị có trách nhiệm lập và gửi báo cáo về công tác an toàn

thông tin mạng theo định kỳ và đột xuất:

1. Báo cáo định kỳ hằng năm: Gửi báo cáo an toàn thông tin định kỳ hằng năm gồm các nội dung quy định tại Điều 13 và Điều 14 Thông tư số 12/2022/TT-BTTTT.

2. Báo cáo định kỳ 6 tháng: Gửi báo cáo hoạt động giám sát của chủ quản hệ thống thông tin theo mẫu tại Phụ lục 2 Thông tư số 31/2017/TT-BTTTT.

3. Báo cáo đột xuất: Báo cáo về công tác khắc phục mã độc, lỗ hổng, điểm yếu, triển khai cảnh báo an toàn thông tin và các báo cáo đột xuất khác theo yêu cầu của Công an tỉnh hoặc yêu cầu của Ủy ban nhân dân tỉnh.

4. Công an tỉnh chịu trách nhiệm tập hợp, tổng hợp báo cáo của các cơ quan, đơn vị, trình Ủy ban nhân dân tỉnh phê duyệt, gửi các cơ quan quản lý nhà nước về an toàn thông tin.

Chương V
TỔ CHỨC THỰC HIỆN

Điều 27. Trách nhiệm của Công an tỉnh

1. Thực hiện các trách nhiệm được giao tại Quy chế này và là cơ quan đầu mối, chủ trì tham mưu Ủy ban nhân dân tỉnh về công tác quản lý nhà nước về an toàn thông tin, an ninh mạng, bảo vệ bí mật nhà nước trên không gian mạng.

2. Chủ trì hướng dẫn, giám sát, đôn đốc, kiểm tra việc triển khai các nội dung tại Quy chế này.

3. Thực hiện thẩm định, phê duyệt hoặc cho ý kiến về mặt chuyên môn đối với hồ sơ đề xuất cấp độ theo thẩm quyền quy định của Luật An toàn thông tin mạng 2015 và các văn bản hướng dẫn thi hành.

4. Chủ trì công tác phòng ngừa, phát hiện, ngăn chặn và xử lý các hành vi vi phạm pháp luật trên môi trường mạng.

5. Phối hợp chặt chẽ với Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (Bộ Công an) trong giám sát, bảo đảm an toàn thông tin, an ninh mạng cho các hệ thống thông tin, cơ sở dữ liệu dùng chung của tỉnh và công tác phòng ngừa, phát hiện, xử lý sự cố về an ninh mạng.

Điều 28. Trách nhiệm của Sở Khoa học và Công nghệ

1. Phối hợp với Công an tỉnh trong việc hướng dẫn, hỗ trợ các cơ quan, đơn vị về công tác bảo đảm an toàn thông tin và an ninh mạng.

2. Thực hiện nghiêm túc công tác bảo đảm an toàn thông tin, an ninh mạng đối với các hệ thống thông tin được Ủy ban nhân dân tỉnh giao quản lý, vận hành.

3. Phối hợp với Ban Cơ yếu Chính phủ tổ chức triển khai ứng dụng chữ ký số cho các cơ quan, đơn vị trên địa bàn tỉnh nhằm bảo đảm an toàn thông tin mạng trong các giao dịch điện tử.

Điều 29. Trách nhiệm của đơn vị chủ quản hệ thống thông tin

1. Chịu trách nhiệm trực tiếp trước Ủy ban nhân dân tỉnh trong công tác bảo đảm an toàn thông tin, an ninh mạng đối với các hệ thống thông tin thuộc phạm vi quản lý.

2. Thực hiện xác định cấp độ an toàn thông tin và bảo đảm an toàn cho hệ thống thông tin theo quy định.

3. Phối hợp chặt chẽ với Công an tỉnh và các đơn vị liên quan trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn thông tin trên không gian mạng.

Điều 30. Kinh phí thực hiện

1. Kinh phí bảo đảm an toàn thông tin, an ninh mạng trong hoạt động ứng dụng công nghệ thông tin do ngân sách nhà nước bảo đảm theo phân cấp hiện hành, được bố trí trong dự toán ngân sách nhà nước hằng năm của cơ quan, đơn vị và các nguồn kinh phí hợp pháp khác (nếu có). Việc quản lý, sử dụng kinh phí từ ngân sách nhà nước thực hiện theo quy định của pháp luật về ngân sách nhà nước. Sở Tài chính chủ trì, phối hợp với Công an tỉnh và Sở Khoa học và Công nghệ tham mưu Ủy ban nhân dân tỉnh bảo đảm nguồn kinh phí triển khai, thực hiện các mặt công tác bảo đảm an toàn thông tin, an ninh mạng trên địa bàn tỉnh.

2. Các cơ quan, đơn vị hằng năm bố trí kinh phí cho việc ứng dụng công nghệ thông tin nói chung và công tác bảo đảm an toàn thông tin, an ninh mạng bảo vệ dữ liệu cá nhân nói riêng trong nội bộ cơ quan, đơn vị mình; lập kế hoạch nâng cấp, bảo trì, sửa chữa, gia hạn bản quyền phần mềm,... đối với các hệ thống phần cứng, phần mềm nhằm thực hiện tốt công tác bảo mật, bảo đảm an toàn thông tin, an ninh mạng để triển khai thực hiện; lập dự toán và thanh, quyết toán kinh phí từ ngân sách nhà nước theo quy định của pháp luật.

Điều 31. Khen thưởng, kỷ luật

1. Tổ chức, cá nhân có thành tích xuất sắc trong công tác bảo đảm an toàn thông tin, an ninh mạng sẽ được xem xét khen thưởng theo quy định hiện hành.

2. Tổ chức, cá nhân có hành vi vi phạm Quy chế này và các quy định khác của pháp luật về bảo đảm an toàn thông tin, an ninh mạng, bảo vệ dữ liệu cá nhân, tùy theo tính chất, mức độ vi phạm sẽ bị xử lý kỷ luật hoặc các hình thức xử lý khác.

Điều 32. Điều khoản thi hành

1. Công an tỉnh chủ trì, phối hợp với các sở, ban, ngành, các cơ quan, đơn vị và các cá nhân, tổ chức có liên quan triển khai thực hiện nội dung Quy chế này.

2. Các cơ quan, đơn vị chủ động xây dựng, ban hành quy chế, quy định nội bộ về bảo đảm an toàn thông tin, an ninh mạng trong hoạt động ứng dụng CNTT tại đơn vị mình phù hợp với Quy chế này.

3. Trong quá trình thực hiện, phát sinh khó khăn, vướng mắc các cơ quan, đơn vị phản ánh về Công an tỉnh để tổng hợp, báo cáo Ủy ban nhân dân tỉnh xem xét, sửa đổi, bổ sung cho phù hợp./.