UBND TỈNH CAO BẰNG **VĂN PHÒNG**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**
Số: 69 /QĐ-VP	*Cao Bằng, ngày 22 tháng 7 năm 2025*

QUYẾT ĐỊNH

Ban hành Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của Văn phòng UBND tỉnh Cao Bằng

CHÁNH VĂN PHÒNG ỦY BAN NHÂN DÂN TỈNH CAO BẰNG

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

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 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 03/2017/TT-BTTTT ngày 24 tháng 4 năm 2017 của 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 Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 của 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 31/2017/TT-BTTTT ngày 15 tháng 11 năm 2017 của 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 số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Kế hoạch số 3116/KH-UBND ngày 15 tháng 11 năm 2024 của UBND tỉnh Cao Bằng ban hành Kế hoạch ứng phó sự cố an toàn thông tin mạng trên địa bàn tỉnh Cao Bằng năm 2025;

Căn cứ Quyết định số 35/2022/QĐ-UBND ngày 12 tháng 12 năm 2022 của Ủy ban nhân dân tỉnh Cao Bằng ban hành Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Văn phòng Ủy ban nhân dân tỉnh Cao Bằng;

Theo đề nghị của Giám đốc Trung tâm Thông tin.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của Văn phòng Ủy ban nhân dân tỉnh Cao Bằng.

Điều 2. Quyết định này có hiệu lực từ ngày ký.

Điều 3. Giám đốc Trung tâm Thông tin, Trưởng các phòng, đơn vị trực thuộc và công chức, viên chức, người lao động thuộc Văn phòng Ủy ban nhân dân tỉnh chịu trách nhiệm thi hành quyết định này./.

Nơi nhận:
- Như Điều 3;
- UBND tỉnh;
- LĐ VP UBND tỉnh;
- Sở Khoa học và Công nghệ (b/c);
- Công an tỉnh (PA05);
- Trang TTĐT VP;
- Lưu: VT, TTTT (Tg).

CHÁNH VĂN PHÒNG

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

Dương Hùng Dũng

UBND TỈNH CAO BẰNG
VĂN PHÒNG

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

QUY CHẾ
Đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của Văn phòng Ủy ban nhân dân tỉnh Cao Bằng

(Ban hành kèm theo Quyết định số 69 /QĐ-VP ngày 22 tháng 7 năm 2025 của Văn phòng Ủy ban nhân dân tỉnh Cao Bằng)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định về việc bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của Văn phòng Ủy ban nhân dân tỉnh và các đơn vị trực thuộc Văn phòng.

Điều 2. Đối tượng áp dụng

1. Quy chế này áp dụng đối với tất cả các phòng, ban, đơn vị trực thuộc Văn phòng (gọi chung là các đơn vị trực thuộc).

2. Công chức, viên chức và người lao động đang làm việc trong Văn phòng Ủy ban nhân dân tỉnh và những tổ chức, cá nhân có liên quan áp dụng Quy chế này trong việc đảm bảo an toàn thông tin tại cơ quan.

Điều 3. Giải thích từ ngữ

Trong Quy chế này, các từ ngữ dưới đây được hiểu như sau:

1. Các khái niệm *"an toàn thông tin mạng", "mạng", "hệ thống thông tin", "xâm phạm an toàn thông tin mạng", "sự cố an toàn thông tin mạng", "phần mềm độc hại", "xung đột thông tin", "thông tin cá nhân"* được định nghĩa theo quy định tại các khoản 1, 2, 3, 6, 11, 14, 15 Điều 3 Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015.

2. An toàn thông tin: Là sự bảo vệ thông tin và hệ thống thông tin 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. Người sử dụng: Công chức, viên chức và người lao động.

4. Chuyên viên quản trị mạng (Viên chức thuộc Trung tâm Thông tin) là chuyên viên được giao phụ trách công tác đảm bảo hạ tầng, ứng dụng, cơ sở dữ liệu và an toàn, an ninh thông tin cho việc triển khai, vận hành, khai thác hệ thống công nghệ thông tin tại Văn phòng Ủy ban nhân dân tỉnh.

5. 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.

6. Tin tặc hay còn gọi là hacker. Họ là những người hiểu rõ hoạt động của hệ thống máy tính, mạng máy tính. Nhờ khả năng sử dụng công nghệ thông tin cực kỳ thông thạo của mình, tin tặc có thể viết hay chỉnh sửa phần mềm, phần cứng máy tính để làm thay đổi, chỉnh sửa nó với nhiều mục đích tốt xấu khác nhau.

7. Mạng nội bộ (LAN) tên tiếng anh là Local Area Network tạm dịch là mạng máy tính nội bộ, giao tiếp này cho phép các máy tính kết nối với nhau để cùng làm việc và chia sẻ dữ liệu. Kết nối này được thực hiện thông qua sợi cáp LAN hoặc Wifi (không dây) trong không gian hẹp.

8. Mạng diện rộng (WAN) tên tiếng anh là Wide Area Network, được kết hợp giữa các mạng đô thị thông qua thiết bị vệ tinh, cáp quang, cáp dây điện.

Điều 4. Mục đích, nguyên tắc đảm bảo an toàn thông tin mạng

1. Đảm bảo an toàn thông tin mạng là yêu cầu bắt buộc, thường xuyên, liên tục, có tính xuyên suốt quá trình, đồng bộ từ khi thiết kế, xây dựng, vận hành, nâng cấp và hủy bỏ (dừng hoạt động) hệ thống thông tin. Đảm bảo an toàn thông tin mạng phải tuân thủ các nguyên tắc chung, được quy định tại Điều 4 Luật An toàn thông tin mạng và Điều 4 Nghị định số 85/2016/NĐ-CP ngày 01 tháng 6 năm 2016 của Chính phủ.

2. Đơn vị vận hành hệ thống thông tin có trách nhiệm đảm bảo an toàn thông tin mạng đối với hệ thống thông tin của đơn vị mình quản lý và sử dụng; bố trí nhân sự để sẵn sàng xử lý sự cố an toàn thông tin mạng đối với các hệ thống thông tin do đơn vị mình quản lý.

3. Người sử dụng có trách nhiệm đảm bảo an toàn thông tin mạng trong phạm vi xử lý công việc của mình theo quy định của Nhà nước và của Bộ.

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

5. Việc áp dụng Quy chế này nhằm phòng ngừa, ngăn chặn, xử lý và giảm các nguy cơ gây mất an toàn thông tin mạng và bảo đảm an ninh thông tin trong quá trình ứng dụng công nghệ thông tin cơ quan.

6. Giảm thiểu được các nguy cơ gây sự cố mất an toàn, an ninh thông tin và đảm bảo an toàn về dữ liệu, các thiết bị công nghệ thông tin trong hoạt động ứng dụng công nghệ thông tin cơ quan.

Điều 5. Các hành vi bị nghiêm cấm

1. Ngăn chặn việc truyền tải thông tin trên mạng, can thiệp, truy nhập, gây nguy hại, xóa, thay đổi, sao chép và làm sai lệch thông tin trên mạng trái pháp luật.

2. Gây ảnh hưởng, cản trở trái pháp luật tới hoạt động bình thường của hệ thống thông tin hoặc tới khả năng truy nhập hệ thống thông tin của người sử dụng.

3. Tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng của biện pháp bảo vệ an toàn thông tin mạng của hệ thống thông tin; tấn công, chiếm quyền điều khiển, phá hoại hệ thống thông tin.

4. Phát tán thư rác, phần mềm độc hại, thiết lập hệ thống thông tin giả mạo, lừa đảo.

5. Đăng lên, 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.

6. Thu thập, sử dụng, phát tán, kinh doanh trái pháp luật thông tin cá nhân; phát tán thông tin, hồ sơ, lợi dụng sơ hở, điểm yếu của hệ thống thông tin để thu thập, khai thác thông tin cá nhân.

7. 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, lợi ích quốc gia trên mạng; phá hại khối đại đoản 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.

8. Lợi dụng mạng đê truyền bá trái phép tài liệu, hình anh, âm thanh hoặc dạng thông tin khác nhàm 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.

Chương II
NỘI DUNG BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 6. Yêu cầu chung về quản lý an toàn thông tin mạng

1. Đối với các đơn vị trực thuộc:

a) Phân loại thông tin có nội dung quan trọng, thuộc tính bí mật để có biện pháp bảo vệ phù hợp theo quy định của pháp luật về bảo vệ bí mật nhà nước. Khi sử dụng thông tin đã phân loại và chưa phân loại trong hoạt động thuộc lĩnh vực của đơn vị phải xây dựng quy định, thủ tục để xử lý thông tin; xác định nội dung và phương pháp ghi truy nhập được phép vào thông tin đã được phân loại;

b) Áp dụng các biện pháp quản lý và kỹ thuật phù hợp để ngăn chặn mất an toàn thông tin mạng; phối hợp, cung cấp thông tin liên quan đến an toàn tài nguyên viễn thông theo yêu cầu của cơ quan nhà nước có thẩm quyền;

c) Tổ chức các biện pháp bảo vệ hệ thống thông tin, ngăn chặn xung đột thông tin trên mạng thuộc quyền quản lý và phối hợp chặt chẽ với cơ quan chức

năng theo quy định của pháp luật để triển khai các biện pháp ngăn chặn xung đột thông tin trên mạng khi vượt quá thẩm quyền, khả năng;

d) Áp dụng các biện pháp quản lý và kỹ thuật phù hợp để ngăn chặn thông tin phá hoại xuất phát từ hệ thống thông tin của đơn vị. Phối hợp với các cơ quan chức năng xác định nguồn, đẩy lùi, khắc phục hậu quả;

đ) Xây dựng và công bố công khai biện pháp xử lý, bảo vệ thông tin cá nhân, thông tin nội bộ của đơn vị. Khi xử lý thông tin phải có trách nhiệm bảo đảm an toàn thông tin mạng đối với thông tin được xử lý;

e) Thường xuyên tuyên truyền, phổ biến, nâng cao nhận thức của công chức, viên chức, người lao động về trách nhiệm bảo đảm an toàn thông tin mạng. Khi tiếp nhận, tuyển dụng nhân sự mới phải quán triệt các quy định, quy chế, quy trình, thủ tục an toàn thông tin mạng. Khi nhân sự chuyển công tác, nghỉ việc, nghỉ theo chế độ phải tổ chức bàn giao, thu hồi tài khoản, quyền truy nhập và tất cả tài sản liên quan tới các hệ thống thông tin của đơn vị.

2. Đối với người sử dụng:

a) Thường xuyên cập nhật và nghiêm túc chấp hành quy định, quy chế, quy trình, thủ tục an toàn thông tin mạng của đơn vị và thực hiện các hướng dẫn, khuyến cáo của Chuyên viên quản trị mạng;

b) Tự bảo vệ thông tin cá nhân của mình và tuân thủ quy định của pháp luật về cung cấp thông tin cá nhân khi sử dụng dịch vụ trên mạng, đồng thời có trách nhiệm bảo đảm an toàn thông tin mạng đối với thông tin được xử lý;

c) Khi tham gia quản lý, vận hành mạng máy tính của cơ quan phải nghiêm chỉnh chấp hành chế độ bảo mật, an toàn, an ninh thông tin mạng đồng thời chịu trách nhiệm đối với các thông tin đã cung cấp;

d) Tự quản lý, bảo quản thiết bị được giao sử dụng; không tự ý thay đổi, tháo lắp các thiết bị trên máy tính làm ảnh hưởng đến an toàn thông tin mạng; không truy cập các trang mạng xã hội, giải trí... không phục vụ mục đích công việc, các trang web có nội dung đồi trụy, bạo lực, cờ bạc hoặc các trang nằm trong danh sách cảnh báo của cơ quan chức năng; không tải và cài đặt các phần mềm không rõ nguồn gốc, không liên quan đến công việc chuyên môn; không truy cập vào các liên kết lạ không rõ về nội dung; không cung cấp thông tin không trung thực để công bố trên mạng; sử dụng mạng để truy cập vào các mạng máy tính khi chưa được phép; không đưa các thông tin, tài liệu chứa bí mật nhà nước lên hệ thống máy tính có kết nối mạng Internet;

đ) Phải sử dụng thư điện tử công vụ và các công cụ trao đổi thông tin, dữ liệu do các cơ quan nhà nước hoặc tổ chức có thẩm quyền cung cấp, cho phép sử dụng trong trao đổi thông tin, dữ liệu phục vụ công việc; không sử dụng các trang mạng xã hội, dịch vụ thư điện tử, công cụ tiện ích điện tử công cộng để trao đổi thông tin quan trọng liên quan đến công việc chuyên môn của đơn vị;

e) Khi phát hiện nguy cơ mất an toàn thông tin mạng hoặc dấu hiệu sự cố an toàn thông tin mạng phải báo cáo kịp thời với Lãnh đạo Văn phòng, Chuyên

viên quản trị mạng hoặc lãnh đạo Trung tâm Thông tin để xem xét, tham mưu, tổ chức ngăn chặn, xử lý, khắc phục.

Điều 7. Quản lý đăng nhập, truy nhập hệ thống thông tin khi quản trị, sử dụng hệ thống thông tin

1. Thiết lập mật mã truy nhập và chế độ tự động bảo vệ màn hình sau 10 phút không sử dụng cho tất cả máy tính.

2. Bảo vệ bí mật thông tin tài khoản của cá nhân hoặc tài khoản của đơn vị khi được phân công quản lý, đồng thời phải thay đổi ngay mật khẩu tài khoản khi mới được cấp và tự chịu trách nhiệm trong việc quản lý, sử dụng và bảo vệ mật khẩu của tài khoản. Không được cho người khác sử dụng tài khoản của cá nhân hoặc của đơn vị.

3. Thiết lập mật khẩu đăng nhập, truy nhập khai thác, sử dụng 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 thay đổi ít nhất 03 tháng/lần. Không đặt chế độ tự động ghi nhớ mật khẩu đăng nhập, truy nhập khai thác, sử dụng hệ thống thông tin trên các trình duyệt của máy tính trong mọi trường hợp.

Điều 8. Phòng, chống phần mềm độc hại

1. Tất cả máy tính phải được trang bị, cài đặt phần mềm phòng, chống phần mềm độc hại có bản quyền và đã được cơ quan chức năng khuyến cáo sử dụng. Phần mềm phòng, chống phần mềm độc hại phải được thiết lập chế độ tự động cập nhật và chế độ tự động quét phần mềm độc hại khi sao chép, mở các tệp tin.

2. Hệ điều hành, phần mềm cài đặt trên máy tính phải được cập nhật bản vá lỗ hổng bảo mật thường xuyên, kịp thời.

3. Cá nhân không được tự ý gỡ bỏ các phần mềm phòng, chống phần mềm độc hại trên máy tính khi chưa có sự đồng ý của người có thẩm quyền.

4. Tất cả các máy tính 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 kết nối vào.

5. Máy tính xách tay, thiết bị di động (máy tính bảng, điện thoại thông minh, thiết bị có phần mềm hệ điều hành) trước khi kết nối vào mạng nội bộ (LAN) của cơ quan phải bảo đảm đã được cài đặt phần mềm phòng, chống phần mềm độc hại và đã được kiểm duyệt về các phần mềm độc hại.

6. Máy tính chỉ được dùng để cài đặt các phần mềm, dịch vụ dùng chung của cơ quan; không cài đặt phần mềm không được cung cấp bởi Trung tâm Thông tin hoặc không có bản quyền hợp lệ, phần mềm phục vụ mục đích cá nhân và không phục vụ công việc.

7. Tất cả các tệp tin, thư mục phải được quét phần mềm độc hại trước khi sao chép, sử dụng.

8. Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại trên máy tính như: hoạt động chậm bất thường, có cảnh báo từ phần mềm phòng chống phần mềm độc hại, tình trạng này lặp đi lặp lại nhiều lần, ở các vị trí khác nhau, nhất là có dấu hiệu bị thay đổi, mất dữ liệu, người sử dụng phải tắt máy, ngắt kết nối từ máy tính đến mạng nội bộ (LAN), mạng diện rộng (WAN), mạng Internet và báo cáo, thông báo trực tiếp cho Chuyên viên quản trị mạng hoặc lãnh đạo Trung tâm Thông tin để xử lý.

Điều 9. Sao lưu dữ liệu dự phòng

1. Xác định 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 phục hồi dữ liệu.

2. Tổ chức lưu trữ dữ liệu sao lưu ở nơi an toàn, không cùng phân vùng lưu trữ các ứng dụng và thường xuyên kiểm tra, bảo đảm sẵn sàng cho việc sử dụng khi cần thiết.

3. Lập kế hoạch và thực hiện sao lưu dữ liệu dự phòng định kỳ đối với các dữ liệu quan trọng, tối thiểu mỗi tháng một lần; trường hợp cần thiết phải áp dụng kỹ thuật mã hóa, thiết lập mật mã, ứng dụng ký số chứng thực;

4. Việc sao lưu dữ liệu dự phòng phải bảo đảm tính đầy đủ, toàn vẹn và tin cậy. Sau khi sao lưu phải lưu trữ bản sao lưu bằng thiết bị lưu trữ ngoài phù hợp, bảo đảm tính bảo mật và sẵn sàng cho việc phục hồi dữ liệu khi cần thiết.

Điều 10. Ứng cứu sự cố an toàn thông tin mạng

1. Phân loại mức độ sự cố an toàn thông tin mạng:

a) Sự cố mức độ thấp (thông thường): Sự cố gây ảnh hưởng đến 01 (một) hoặc một vài cá nhân đơn lẻ và không làm gián đoạn hay đình trệ hoạt động chính của hệ thống thông tin như: Máy tính cá nhân bị nhiễm phần mềm độc hại hoặc hư hỏng phần cứng; phần mềm hệ điều hành, các phần mềm ứng dụng, tiện ích cài đặt trên máy tính cá nhân phát sinh lỗi;

b) Sự cố mức độ trung bình: Sự cố ảnh hưởng đến một nhóm lớn người khai thác, sử dụng nhưng vẫn chưa gây gián đoạn hoạt động chính của hệ thống thông tin như: Hệ thống mạng của 01 (một) đơn vị trực thuộc bị ngưng hoạt động; phần mềm độc hại lây nhiễm tất cả các máy tính trạm trong 01 (một) đơn vị;

c) Sự cố mức độ 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 hệ thống thông tin như: Ứng dụng quản lý văn bản và điều hành, một cửa điện tử, thư điện tử công vụ… của toàn cơ quan bị ngưng hoạt động; một số thiết bị công nghệ thông tin quan trọng bị hư hỏng;

d) Sự cố có tính chất nghiêm trọng: sự cố ảnh hưởng đến sự liên tục của nhiều hoạt động chính của hệ thống thông tin, như: Toàn bộ hệ thống thiết bị công nghệ thông tin ngừng hoạt động; hệ thống trang thông tin điện tử bị tin tặc (hacker) tấn công, xâm nhập, thay đổi nội dung hoặc sự cố có một hoặc nhiều

tính chất sau: Có khả năng xảy ra trên diện rộng, lan nhanh; có khả năng phá hoại hệ thống mạng máy tính, lấy cắp dữ liệu.

2. Khi có nguy cơ mất an toàn thông tin mạng hoặc sự cố an toàn thông tin mạng xảy ra ở mức độ thấp thì Trung tâm Thông tin chỉ đạo Chuyên viên quản trị mạng phối hợp với đơn vị, cá nhân bị ảnh hưởng tự xử lý, khắc phục hoặc liên hệ với đơn vị cung cấp sản phẩm, dịch vụ viễn thông, Internet, đơn vị triển khai ứng dụng phần mềm để được tư vấn, hỗ trợ ngăn chặn, xử lý, khắc phục.

3. Khi có nguy cơ hoặc sự cố an toàn thông tin mạng xảy ra ở mức độ trung bình trở lên, xét thấy không có khả năng tự xử lý được thì Trung tâm Thông tin thông báo cho Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh để tổ chức điều phối, hỗ trợ ứng cứu.

Chương III
QUY ĐỊNH BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 11. Bảo vệ bí mật nhà nước trong hoạt động ứng dụng công nghệ thông tin

1. Quy định về soạn thảo, in ấn, phát hành và sao chụp tài liệu mật

a) Không được sử dụng máy tính có kết nối mạng internet để soạn thảo văn bản, chuyển giao, lưu trữ thông tin có nội dung thuộc bí mật nhà nước; cung cấp tin, tài liệu và đưa thông tin bí mật nhà nước trên Cổng/Trang thông tin điện tử;

b) Không được in, sao chụp tài liệu bí mật nhà nước trên các thiết bị kết nối mạng internet;

2. Khi sửa chữa, khắc phục các sự cố của máy tính dùng soạn thảo văn bản mật, các phòng, đơn vị phải báo cáo cho người có thẩm quyền. Không được cho phép các công ty tư nhân hoặc người không có trách nhiệm trực tiếp sửa chữa, xử lý, khắc phục sự cố;

3. Trước khi thanh lý các máy tính trong các cơ quan nhà nước thì Chuyên viên quản trị mạng phải dùng các biện pháp kỹ thuật xoá bỏ vĩnh viễn dữ liệu trong ổ cứng máy tính hoặc thu hồi ổ cứng để phá hủy.

Điều 12. Quy định về cấp phát, thu hồi, cập nhật và quản lý các tài khoản truy cập vào hệ thống thông tin

Chuyên viên quản trị mạng quản trị, quản lý, cấp tài khoản cá nhân và phân quyền truy cập cho người sử dụng trên hệ thống thông tin của Văn phòng. Trong trường hợp cần thiết có thể hủy tài khoản truy cập cá nhân và ngắt kết nối đối với các hành vi cố ý tấn công hoặc gây trở ngại trên hệ thống thông tin; hủy hoặc ẩn quyền truy cập hệ thống thông tin đối với công chức, viên chức nghỉ chế độ, chuyển công tác...

Hướng dẫn người sử dụng thay đổi mật khẩu ngay sau khi đăng nhập lần đầu tiên; bảo vệ thông tin của tài khoản theo quy định.

Điều 13. Cơ chế thông tin, báo cáo và khắc phục sự cố an toàn, an ninh thông tin

1. Đối với người sử dụng

a) Thông tin, báo cáo kịp thời cho Chuyên viên quản trị mạng khi phát hiện các sự cố gây mất an toàn, an ninh thông tin mạng trong quá trình tham gia vào hệ thống thông tin;

b) Phối hợp tích cực trong suốt quá trình giải quyết và khắc phục sự cố.

2. Đối với Chuyên viên quản trị mạng

a) Phối hợp với Sở Khoa học và Công nghệ, Công an tỉnh, các đơn vị cung cấp hệ thống thông tin và các cơ quan chức năng khác xử lý, áp dụng mọi biện pháp để khắc phục và hạn chế thiệt hại do sự cố xảy ra, báo cáo lãnh đạo Trung tâm Thông tin và Văn phòng Ủy ban nhân dân tỉnh;

b) Cung cấp đầy đủ, chính xác, kịp thời những thông tin cần thiết; thực hiện theo đúng hướng dẫn và tạo điều kiện thuận lợi cho cơ quan chức năng tham gia khắc phục sự cố.

Điều 14. Xác định cấp độ và phương án đảm bảo an toàn hệ thống thông tin

1. Các hệ thống thông tin phải thực hiện đảm bảo an toàn thông tin cấp độ (quy định tại Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ).

2. Xác định cấp độ cho các hệ thống thông tin: Trung tâm Thông tin phối hợp với đơn vị cung cấp hệ thống thông tin để xây dựng, hỗ trợ, cung cấp đầu đủ tài liệu, thuyết minh cho đơn vị vận hành lập hồ sơ đề xuất cấp độ an toàn thông tin và gửi Công an tỉnh tổ chức thẩm định, phê duyệt hồ sơ đề xuất cấp độ theo quy định tại Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ.

3. Phương án đảm bảo an toàn hệ thống thông tin theo cấp độ

a) Trung tâm Thông tin phối hợp với đơn vị cung cấp hệ thống thông tin để xây dựng, đưa ra phương án đảm bảo an toàn hệ thống thông tin và gửi hồ sơ tới Công an tỉnh để được thẩm định, phê duyệt theo quy định; Trung tâm Thông tin chịu trách nhiệm trực tiếp giám sát, đánh giá việc triển khai các phương án đảm bảo an toàn thông tin đã được phê duyệt.

b) Phương án đảm bảo an toàn hệ thống thông tin phải phù hợp với cấp độ của hệ thống thông tin và đáp ứng yêu cầu quy định tại Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ Thông tin và Truyền thông, phù hợp với quy định về an toàn thông tin mạng.

c) Đơn vị vận hành hệ thống thông tin có trách nhiệm tổ chức triển khai phương án đảm bảo an toàn hệ thống thông tin sau khi được phê duyệt.

Điều 15. Giám sát an toàn hệ thống thông tin

1. Các hệ thông tin phải được thực hiện giám sát an toàn thông tin.

2. Đơn vị vận hành hệ thống có trách nhiệm phối hợp với Công an tỉnh tổ chức thực hiện việc giám sát hệ thống thông tin theo Thông tư số 31/2017/TT-BTTTT ngày 15 tháng 11 năm 2017 về quy định hoạt động giám sát an toàn hệ thống thông tin của Bộ Thông tin và Truyền thông.

Điều 16. Ứng cứu sự cố an toàn hệ thống thông tin

1. Trung tâm Thông tin là bộ phận phụ trách ứng cứu sự cố an toàn thông tin mạng của Văn phòng Ủy ban nhân dân tỉnh có trách nhiệm:

a) Nghiên cứu, sử dụng các sản phẩm dịch vụ an toàn thông tin nhằm đảm bảo an toàn thông tin có chất lượng.

b) Chủ động phối hợp với Sở Khoa học và Công nghệ, Công an tỉnh và các đơn vị liên quan trong việc tăng cường tập trung vào khả năng phát hiện, cảnh báo sớm các nguy cơ mất an toàn thông tin mạng, nhanh chóng khắc phục và phục hồi hệ thống khi xảy ra sự cố an toàn thông tin mạng.

c) Đề xuất, tham mưu cơ chế hỗ trợ, thu hút nguồn nhân lực số.

d) Triển khai và tham gia đầy đủ các khóa đào tạo, tập huấn, nâng cao nguồn nhân lực số đảm bảo an toàn thông tin mạng.

đ) Triển khai tuyên truyền, phổ biến nâng cao nhận thức và trách nhiệm của cán bộ công chức, viên chức về vai trò và tầm quan trọng của việc đảm bảo ATTT mạng

e) Tham gia hỗ trợ, hướng dẫn các hoạt động ứng cứu khẩn cấp bảo đảm ATTT mạng nội bộ khi có yêu cầu từ các đơn vị.

2. Các đơn vị trực thuộc có trách nhiệm:

a) Chủ động nghiên cứu, học hỏi, nâng cao kiến thức về an toàn thông tin mạng, ứng cứu sự cố an toàn thông tin mạng.

b) Kiểm tra, rà soát hệ thống thông tin mạng khi có cảnh báo, thông báo về các nguy cơ làm mất an toàn thông tin từ các cơ quan chức năng.

c) Tuyên truyền, phổ biến nâng cao nhận thức và trách nhiệm của công chức, viên chức về vai trò và tầm quan trọng của việc đảm bảo an toàn thông tin mạng.

d) Tham gia đầy đủ các khóa đào tạo, tập huấn, nâng cao an toàn thông tin mạng.

đ) Cử công chức, viên chức tham gia hoạt động ứng cứu sự cố an toàn thông tin mạng khi có sự cố xảy ra.

3. Nghiêm túc thực hiện Kế hoạch số 3116/KH-UBND ngày 15 tháng 11 năm 2024 của UBND tỉnh Cao Bằng ban hành Kế hoạch ứng phó sự cố an toàn thông tin mạng trên địa bàn tỉnh Cao Bằng năm 2025;

4. Quy trình ứng cứu sự cố An toàn thông tin mạng được thực hiện theo Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 2017 của Thủ tướng Chính phủ và Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 của Bộ Thông tin và Truyền thông.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 17. Trách nhiệm của Người sử dụng

1. Nghiêm chỉnh chấp hành các quy định, quy trình về an toàn, an ninh thông tin của Văn phòng Ủy ban nhân dân tỉnh cũng như quy định khác của pháp luật, nâng cao ý thức cảnh giác và trách nhiệm bảo đảm an toàn, an ninh thông tin tại cơ quan, đơn vị.

2. Khi phát hiện sự cố phải báo ngay với Lãnh đạo đơn vị và chuyên viên quản trị mạng, Lãnh đạo Trung tâm Thông tin để kịp thời ngăn chặn, xử lý.

3. Hưởng ứng, tham gia các chương trình đào tạo, hội nghị, diễn tập ứng cứu về an toàn, an ninh thông tin do Công an tỉnh tổ chức (nếu có).

4. Có trách nhiệm quản lý, bảo quản thiết bị được giao sử dụng; không tự ý thay đổi cấu hình hoặc tháo lắp các thiết bị trên máy tính khi chưa có sự đồng ý của Lãnh đạo đơn vị.

5. Chịu trách nhiệm trước Lãnh đạo đơn vị và Lãnh đạo Văn phòng về các vi phạm làm mất an toàn thông tin mạng do không tuân thủ Quy chế này.

Điều 18. Trách nhiệm của Chuyên viên quản trị mạng

1. Chuyên viên quản trị mạng: Là viên chức thuộc Trung tâm Thông tin do Lãnh đạo Văn phòng phân công, chịu trách nhiệm quản lý, vận hành các hoạt động hệ thống thông tin. Tham mưu cho Lãnh đạo Văn phòng trong việc đầu tư thiết bị phần cứng, phần mềm, công tác bảo mật thông tin trên môi trường mạng; sử dụng phần mềm có bản quyền và phần mềm mã nguồn mở cho hệ thống máy tính; cập nhật cấu hình chuẩn cho các thành phần của hệ thống khi tiến hành cài đặt và thiết lập cấu hình chặt chẽ nhất cho các sản phẩm an toàn thông tin nhưng vẫn duy trì yêu cầu hoạt động của hệ thống thông tin.

2. Sao chép, lưu trữ thông tin tại nơi an toàn; kiểm tra thông tin sao lưu để đảm bảo tính sẵn sàng và toàn vẹn của thông tin. Xử lý các sự cố về an toàn, an ninh thông tin và bảo mật hệ thống thông tin.

3. Triển khai các biện pháp chống virus, thư rác cho hệ thống thông tin của Văn phòng. Sử dụng biện pháp chống virus, thư rác để phát hiện và loại trừ những đoạn mã độc (virus, trojan.,.) được truyền tải bởi: thư điện tử, tập tin đính kèm từ Internet, thiết bị lưu trữ tháo lắp để khai thác lỗ hổng của hệ thống thông tin; thường xuyên cập nhật các phần mềm chống virus, thư rác, bản vá lỗi hệ

thống và hướng dẫn người dùng (user) sử dụng chương trình để bảo vệ an toàn dữ liệu.

4. Theo dõi và quản lý hoạt động hệ thống mạng, đề xuất lựa chọn công nghệ và triển khai các giải pháp nhằm đảm bảo cho hệ thống mạng LAN hoạt động thông suốt, đảm bảo an toàn và bảo mật các thông tin truyền dẫn cho hệ thống mạng máy tính và đảm bảo hệ thống mạng LAN luôn được kết nối, hoạt động thông suốt.

5. Xây dựng quy trình, thử nghiệm, trực tiếp cài đặt, quản lý các phần mềm hệ thống và phần mềm ứng dụng trong hệ thống mạng máy tính; nghiên cứu, đề xuất, nâng cấp công nghệ phần mềm theo định hướng quản lý nhà nước của cơ quan và tuân theo quy định của Chính phủ. Lắp đặt, hướng dẫn sử dụng, nâng cấp, cập nhật, bảo trì và quản trị mạng máy tính đảm bảo hoạt động ổn định và an toàn cho người sử dụng. Kiểm tra và xử lý các lỗi kỹ thuật đảm bảo việc truyền, nhận thông tin thông suốt giữa các đơn vị trực thuộc. Giữ bí mật tuyệt đối các thông tin trên mạng.

6. Thực hiện việc đánh giá, báo cáo và đề xuất với Lãnh đạo Văn phòng, Lãnh đạo Trung tâm Thông tin các biện pháp phòng chống các rủi ro và mức độ nghiêm trọng của rủi ro đối với hệ thống thông tin của Văn phòng (các rủi ro có thể xảy ra do sự truy cập, sử dụng thông tin trái phép; mất thông tin; thay đổi hoặc phá hủy thông tin của hệ thống).

Điều 19. Trách nhiệm của các đơn vị trực thuộc

1. Tổ chức phổ biến, chỉ đạo việc tuân thủ các quy định tại Quy chế này và các văn bản quy định có liên quan khác của Nhà nước đối với công chức, viên chức và người lao động thuộc đơn vị về an toàn thông tin mạng.

2. Thường xuyên kiểm tra, đôn đốc việc triển khai an toàn thông tin mạng trong công việc của cá nhân do mình quản lý.

3. Thực hiện các báo cáo theo yêu cầu gửi Trung tâm Thông tin để tổng hợp, báo cáo Lãnh đạo.

Điều 20. Kinh phí thực hiện

1. Kinh phí đảm bảo an toàn thông tin mạng thực hiện lồng ghép, tích hợp với các chương trình, đề án, nhiệm vụ công nghệ thông tin từ nguồn ngân sách nhà nước và các nguồn kinh phí hợp pháp khác.

2. Trung tâm Thông tin có trách nhiệm xây dựng kế hoạch, đề xuất dự toán kinh phí cho các hoạt động đảm bảo an toàn thông tin mạng, trình Lãnh đạo Văn phòng phê duyệt.

Điều 21. Trách nhiệm thi hành

1. Thủ trưởng đơn vị trực thuộc có trách nhiệm: Tổ chức quán triệt, thực hiện Quy chế này; thực hiện chế độ báo cáo định kỳ, đột xuất theo hướng dẫn của Công an tỉnh về tình hình, kết quả công tác bảo đảm an toàn thông tin mạng tại đơn vị.

2. Trung tâm Thông tin có trách nhiệm:

a) Phối hợp, cung cấp thông tin và tạo điều kiện cho Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh và các đơn vị liên quan kiểm tra, hỗ trợ ngăn chặn, xử lý, khắc phục nguy cơ, sự cố an toàn thông tin mạng kịp thời, nhanh chóng, hiệu quả.

b) Phối hợp chặt chẽ với các đơn vị chuyên môn thuộc Công an tỉnh, Sở Khoa học và Công nghệ và các cơ quan chức năng có liên quan trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn thông tin mạng.

c) Theo dõi, tổng hợp và báo cáo định kỳ theo quy định.

d) Phân công viên chức chuyên trách bảo đảm an toàn thông tin mạng của cơ quan, đơn vị; tạo điều kiện để các viên chức phụ trách an toàn thông tin mạng được học tập, nâng cao trình độ kiến thức, kỹ năng về an toàn thông tin mạng.

3. Trong quá trình triển khai thực hiện Quy chế, nếu có vấn đề phát sinh, vướng mắc hoặc cần sửa đổi, bổ sung, các đơn vị gửi kiến nghị về Trung tâm Thông tin để tổng hợp, báo cáo Lãnh đạo Văn phòng xem xét, sửa đổi, bổ sung cho phù hợp./.