UBND TỈNH BẮC KẠN **VĂN PHÒNG**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 141 /QĐ-VP	*Bắc Kạn, ngày 29 tháng 9 năm 2023*

QUYẾT ĐỊNH

Ban hành Quy chế bảo đảm an toàn, an ninh thông tin mạng Văn phòng Ủy ban nhân dân tỉnh Bắc Kạn

CHÁNH VĂN PHÒNG ỦY BAN NHÂN DÂN TỈNH BẮC KẠN

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 Nghị định số 142/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về ngăn chặn xung đột thông tin trên mạng;

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 Quyết định số 1622/QĐ-TTg ngày 25 tháng 10 năm 2017 của Thủ tướng Chính phủ về việc phê duyệt Đề án đẩy mạnh hoạt động của mạng lưới ứng cứu sự cố, tăng cường năng lực cho cán bộ, bộ phận chuyên trách ứng cứu sự cố an toàn thông tin mạng trên toàn quốc đến 2020, định hướng đến 2025;

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 Quyết định số 22/2021/QĐ-UBND ngày 03/12/2021 của UBND tỉnh Bắc Kạn về việc 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 ban tỉnh Bắc Kạn;

Căn cứ Quyết định số 42/2022/QĐ-UBND ngày 16/11/2022 của UBND tỉnh ban hành Quy định chức năng, nhiệm vụ, quyền hạn của Văn phòng UBND tỉnh Bắc Kạn;

Xét đề nghị của Giám đốc Trung tâm Công báo - Tin học, Văn phòng UBND tỉnh.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn, an ninh thông tin mạng Văn phòng Ủy ban nhân dân tỉnh.

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

Điều 3. Giám đốc Trung tâm Công báo - Tin học, Trưởng các phòng, ban, các đơn vị và cán bộ, 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 (b/c);
- Sở Thông tin và Truyền thông tỉnh (b/c);
- LĐVP;
- Lưu: VT, TTCBTH (Hiếu).

CHÁNH VĂN PHÒNG

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

Vũ Đức Chính

UBND TỈNH BẮC KẠN
VĂN PHÒNG

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

QUY CHẾ
BẢO ĐẢM AN TOÀN, AN NINH THÔNG TIN MẠNG VĂN PHÒNG ỦY BAN NHÂN DÂN TỈNH

(Ban hành kèm theo Quyết định số /QĐ-VP ngày 29 tháng 9 năm 2023 của Chánh Văn phòng Ủy ban nhân dân tỉnh)

Chương I
QUY ĐỊNH CHUNG

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

1. Phạm vi điều chỉnh: Quy chế này quy định về bảo đảm an toàn, an ninh thông tin mạng trong các hoạt động của Văn phòng Ủy ban nhân dân tỉnh.

2. Đối tượng áp dụng:

a) Các phòng, ban, đơn vị trực thuộc Văn phòng Ủy ban nhân dân tỉnh và công chức, viên chức và người lao động thuộc thuộc Văn phòng.

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 thông tin 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. Bảo đảm an toàn thông tin mức vật lý là việc bảo vệ hệ thống hạ tầng kỹ thuật, phần mềm, ứng dụng và cơ sở dữ liệu khỏi các mối nguy hiểm vật lý (như: cháy, nổ; nhiệt độ, độ ẩm ngoài mức cho phép; thiên tai; mất điện; tác động cơ học) có thể gây ảnh hưởng đến hoạt động của hệ thống.

4. Không gian mạng là mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, bao gồm mạng viễn thông, mạng internet, hệ thống máy tính, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, là nơi con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian.

5. Hạ tầng kỹ thuật là tập hợp các thiết bị tính toán, lưu trữ, thiết bị ngoại vi, thiết bị kết nối mạng, thiết bị phụ trợ, đường truyền, mạng nội bộ, mạng diện rộng.

6. Cổng thông tin điện tử là điểm truy nhập duy nhất của cơ quan, đơn vị trên môi trường mạng, liên kết, tích hợp các kênh thông tin, các dịch vụ và các ứng dụng mà qua đó người dùng có thể khai thác, sử dụng và cá nhân hóa việc hiển thị thông tin.

7. Trang thông tin điện tử là trang thông tin hoặc tập hợp trang thông tin trên môi trường mạng phục vụ cho việc cung cấp, trao đổi thông tin.

8. Phần mềm độc hại là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay toàn bộ hệ thống thông tin hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong hệ thống thông tin.

Điều 3. Nguyên tắc bảo đảm an toàn, an ninh thông tin mạng

1. Bảo đảm an toàn, an ninh thông tin thường xuyên, liên tục, có tính xuyên suốt quá trình liên quan đến thông tin và thiết kế, xây dựng, vận hành, nâng cấp, hủy bỏ hệ thống thông tin. Bảo đảm an toàn, an ninh thông tin tuân thủ các nguyên tắc chung quy định tại Điều 4 Luật An toàn thông tin mạng và Điều 4 Nghị định số 85/2016/NĐ-CP.

2. Các đơn vị trực thuộc Văn phòng có trách nhiệm bảo đảm an toàn, an ninh thông tin mạng, chịu trách nhiệm bảo đảm an toàn, an ninh thông tin mạng; xác định rõ nhiệm của lãnh đạo phòng, ban, đơn vị, cá nhân đối với công tác bảo đảm an toàn, an ninh thông tin mạng.

3. Cán bộ, công chức, viên chức, người lao động thuộc Văn phòng có trách nhiệm bảo đảm an toàn, an ninh thông tin trong phạm vi xử lý công việc của mình theo quy định của Nhà nước và của Văn phòng UBND tỉnh.

4. Thông tin mật, thông tin thuộc Danh mục bí mật nhà nước phải được bảo vệ theo quy định của Nhà nước, quy định của Văn phòng UBND tỉnh về công tác bảo vệ bí mật nhà nước và các nội dung tương ứng trong Quy chế này.

5. Xử lý sự cố an toàn thông tin 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.

Điều 4. Các hành vi bị nghiêm cấm

1. Các hành vi bị nghiêm cấm quy định tại Điều 7 Luật An toàn thông tin mạng.

2. Tự ý đấu nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập mạng không dây của cá nhân vào mạng nội bộ; trên cùng một thiết bị thực hiện đồng thời truy cập vào mạng nội bộ và truy cập Internet bằng thiết bị kết nối Internet của cá nhân (modem quay số, USB 3G/4G, điện thoại di động, máy tính bảng, máy tính xách tay).

3. Tự ý thay đổi, gỡ bỏ biện pháp an toàn thông tin cài đặt trên thiết bị công nghệ thông tin phục vụ công việc; tự ý thay thế, lắp mới, tráo đổi thành phần của máy tính phục vụ công việc.

4. Tạo ra, cài đặt, phát tán phần mềm độc hại.

5. Cản trở hoạt động cung cấp dịch vụ của hệ thống thông tin; ngăn chặn việc truy nhập đến thông tin của cơ quan, cá nhân khác trên môi trường mạng, trừ trường hợp pháp luật cho phép.

6. Bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã và thông tin của cơ quan, cá nhân khác trên môi trường mạng.

7. Các hành vi làm mất an toàn, bí mật thông tin của cơ quan, cá nhân khác được trao đổi, truyền đưa, lưu trữ trên môi trường mạng.

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

Điều 5. Quản lý trang thiết bị công nghệ thông tin

1. Các phòng, ban, đơn vị trực thuộc Văn phòng UBND tỉnh có trách nhiệm quản lý các trang thiết bị, dữ liệu trên máy tính của đơn vị mình; khai thác và sử dụng thông tin phục vụ yêu cầu công tác theo hướng dẫn kỹ thuật của cán bộ kỹ thuật và đơn vị trực tiếp quản lý kỹ thuật.

2. Trung tâm Công báo - Tin học thuộc Văn phòng UBND tỉnh làm công tác quản trị mạng, trực tiếp quản lý kỹ thuật và duy trì hoạt động của hệ thống tin học của Văn phòng UBND tỉnh. Trung tâm Công báo - Tin học là đầu mối kết nối mạng LAN, Internet và các phần mềm ứng dụng cho các phòng, ban, đơn vị thuộc Văn phòng. Cán bộ, công chức, viên chức, người lao động khi có nhu cầu kết nối máy tính vào mạng LAN, mạng Internet, các phần mềm ứng dụng thì thông báo tới Trung tâm Công báo - Tin học để thực hiện việc kết nối.

3. Thực hiện giữ gìn bảo vệ trang thiết bị công nghệ thông tin như: Không mang ra khỏi cơ quan, trang thiết bị công nghệ thông tin liên quan đến dữ liệu mang bí mật nhà nước; không tự ý cài đặt, cấu hình các thiết bị công nghệ thông tin.

4. Trang thiết bị công nghệ thông tin có lưu trữ dữ liệu trong thực hiện nhiệm vụ của cơ quan, nhà nước khi thay đổi mục đích sử dụng hoặc thanh lý, đơn vị phải thực hiện các biện pháp xóa, tiêu hủy dữ liệu đó đảm bảo không có khả năng phục hồi. Trường hợp không thể tiêu hủy được dữ liệu, đơn vị phải thực hiện tiêu hủy cấu phần lưu trữ dữ liệu trên trang thiết bị công nghệ thông tin đó.

5. Thiết bị tính toán có chứa dữ liệu hoặc thiết bị lưu trữ khi mang đi bảo hành, sửa chữa phải sao chép ra thiết bị khác, sau đó xoá trên thiết bị tránh thất thoát dữ liệu.

Điều 6. Trách nhiệm của cán bộ, công chức, viên chức và người lao động

1. Trưởng các phòng, ban, đơn vị có trách nhiệm phổ biến các quy định về bảo đảm an toàn, an ninh thông tin tại đơn vị; đối với các vị trí tiếp xúc, quản lý

các thông tin, dữ liệu quan trọng hoặc quản trị các hệ thống thông tin quan trọng, đơn vị phải yêu cầu cam kết bảo mật thông tin bằng văn bản hoặc cam kết trong hợp đồng làm việc, hợp đồng lao động.

2. Thường xuyên tổ chức quán triệt các quy định về an toàn, an ninh thông tin, nhằm nâng cao nhận thức về trách nhiệm bảo đảm an toàn thông tin của từng cá nhân trong đơn vị.

3. Cán bộ, công chức, viên chức, người lao động thuộc Văn phòng được phép truy cập mạng máy tính của Văn phòng sẽ được cấp tài khoản người dùng (Account) để truy cập và phải chịu trách nhiệm bảo đảm bí mật của tài khoản được cấp; được bộ phận quản trị mạng phân quyền khai thác cơ sở dữ liệu, dịch vụ trên mạng theo chức năng, nhiệm vụ được phân công và chỉ có quyền sử dụng những thông tin đã phân quyền. Ngoài ra mỗi cá nhân khi được cấp tài khoản để truy cập và sử dụng hệ thống thông tin cần phải thực hiện tốt việc quản lý tài khoản và mật khẩu theo quy định.

4. Khi cán bộ, công chức, viên chức và người lao động chấm dứt hoặc thay đổi công việc, cơ quan, đơn vị phải lập biên bản bàn giao tài sản công nghệ thông tin; thay đổi hoặc thu hồi quyền truy cập các hệ thống thông tin.

Điều 7. Bảo đảm an toàn hệ thống công nghệ thông tin

1. Bảo đảm an toàn thông tin đối với phòng máy chủ

a) Các thiết bị kết nối mạng, thiết bị bảo mật quan trọng như tường lửa (firewall), thiết bị định tuyến (router), hệ thống máy chủ, hệ thống lưu trữ SAN, NAS, ... được đặt trong phòng máy chủ và được thiết lập cơ chế bảo vệ, theo dõi phát hiện xâm nhập và biện pháp kiểm soát truy nhập, kết nối vật lý phù hợp với từng khu vực như: Máy chủ và hệ thống lưu trữ; tủ mạng và đầu nối; thiết bị nguồn điện và dự phòng điện khẩn cấp; vận hành, kiểm soát, quản trị hệ thống.

b) Chỉ có bộ phận quản trị mạng có quyền làm việc trên máy chủ và các thiết bị mạng, chỉ những cá nhân có quyền, nhiệm vụ mới được phép vào phòng máy chủ.

d) Phòng máy chủ được trang bị hệ thống lưu điện đủ công suất và duy trì thời gian hoạt động của các máy chủ ít nhất 15 phút khi có sự cố mất điện.

đ) Bộ phận quản trị mạng có trách nhiệm thường xuyên theo dõi, kiểm tra phát hiện kịp thời các hoạt động xâm nhập và có biện pháp xử lý kịp thời.

2. Bảo đảm an toàn thông tin khi sử dụng máy tính

a) Cá nhân chỉ cài đặt phần mềm hợp lệ và thuộc danh mục phần mềm được phép sử dụng do cơ quan có thẩm quyền phát hành được đơn vị cấp; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm khi chưa có sự đồng ý của bộ phận chuyên trách về công nghệ thông tin; thường xuyên cập nhật phần mềm và hệ điều hành.

b) Cài đặt phần mềm xử lý phần mềm độc hại và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm; khi phát hiện bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại trên máy tính phải ngắt kết nối mạng, tắt máy và báo trực tiếp cho bộ phận chuyên trách về công nghệ thông tin để được xử lý kịp thời.

c) Chỉ truy nhập vào các trang/cổng thông tin điện tử, ứng dụng trực tuyến tin cậy và các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình; có trách nhiệm bảo mật tài khoản truy nhập thông tin, không chia sẻ mật khẩu, thông tin cá nhân với người khác.

3. Bảo đảm an toàn thông tin đối với hệ thống mạng máy tính

a) Hệ thống mạng nội bộ (LAN) được thiết kế phân vùng theo chức năng cơ bản (theo các chính sách an toàn thông tin riêng), bao gồm: Vùng mạng người dùng; vùng mạng kết nối hệ thống ra bên ngoài Internet và các mạng khác; vùng mạng máy chủ công cộng; vùng mạng máy chủ nội bộ; vùng mạng máy chủ quản trị. Dữ liệu trao đổi giữa các vùng mạng được quản lý, giám sát bởi hệ thống các thiết bị mạng, thiết bị bảo mật.

b) Tham gia kết nối, sử dụng hệ thống mạng diện rộng (WAN) của Văn phòng UBND tỉnh có trách nhiệm bảo đảm an toàn thông tin đối với hệ thống mạng nội bộ và các thiết bị của mình khi thực hiện kết nối vào mạng diện rộng; thông báo sự cố hoặc các hành vi phá hoại, xâm nhập về Trung tâm Công báo - Tin học; không được tiết lộ phương thức (tên đăng ký, mật khẩu, tiện ích, tệp hỗ trợ và các cách thức khác) để truy nhập vào hệ thống mạng diện rộng cho tổ chức, cá nhân khác; không được tìm cách truy nhập dưới bất cứ hình thức nào vào các khu vực không được phép truy nhập.

c) Có hệ thống tường lửa và hệ thống bảo vệ truy nhập Internet, đáp ứng nhu cầu kết nối đồng thời hỗ trợ các công nghệ mạng riêng ảo thông dụng và có phần cứng mã hóa tích hợp để tăng tốc độ mã hóa dữ liệu và có khả năng bảo vệ hệ thống trước các loại tấn công từ chối dịch vụ (DDoS); lọc bỏ, không cho phép truy nhập các trang tin có nghi ngờ chứa mã độc hoặc các nội dung không phù hợp.

d) Các đường truyền dữ liệu, đường truyền Internet và các hệ thống dây dẫn các mạng LAN, WAN được lắp đặt trong ống, máng che đậy kín, hạn chế khả năng tiếp cận trái phép. Ngắt kết nối cổng Ethernet không sử dụng, đặc biệt là ở khu vực làm việc chung của các cơ quan, đơn vị.

4. Quản lý tài khoản truy cập

a) Cá nhân sử dụng hệ thống thông tin được cấp và sử dụng tài khoản truy cập với định danh duy nhất gắn với cá nhân đó. Các hệ thống thông tin dùng chung của bộ sử dụng cơ chế đăng nhập một lần, chung một tài khoản truy nhập và mật khẩu.

b) Trường hợp cá nhân thay đổi vị trí công tác, chuyển công tác, thôi việc hoặc nghỉ hưu, trong vòng không quá 05 ngày làm việc cá nhân, Trưởng các phòng, ban, đơn vị thuộc Văn phòng có trách nhiệm thông báo đến Trung tâm Công báo - Tin học để điều chỉnh, thu hồi, hủy bỏ các quyền sử dụng đối với hệ thống thông tin; đồng thời cán bộ, công chức, viên chức, người lao động phát hiện có tài khoản thực hiện các hành vi tấn công hoặc để xảy ra vấn đề mất an toàn, an ninh thông tin có trách nhiệm thông tin đến Trung tâm Công báo - Tin học, đơn vị vận hành hệ thống thông tin thực hiện việc khóa quyền truy cập.

c) Tài khoản quản trị hệ thống (mạng, hệ điều hành, thiết bị kết nối mạng, phần mềm, ứng dụng, cơ sở dữ liệu) tách biệt với tài khoản truy nhập của người sử dụng thông thường. Tài khoản hệ thống được giao đích danh cá nhân làm công tác quản trị, hạn chế dùng chung tài khoản quản trị.

d) Việc quản lý tài khoản thư điện tử của Văn phòng UBND tỉnh theo quy định của Quy chế quản lý và khai thác tài nguyên mạng máy tính của Văn phòng UBND tỉnh.

5. Bảo đảm an toàn thông tin dữ liệu

a) Thực hiện bảo vệ thông tin, dữ liệu liên quan đến hoạt động công vụ, thông tin có nội dung quan trọng, nhạy cảm; thiết lập phương án bảo đảm tính bí mật, nguyên vẹn và khả dụng của thông tin, dữ liệu; mã hóa thông tin, dữ liệu khi lưu trữ trên hệ thống/thiết bị lưu trữ dữ liệu di động; sử dụng chữ ký số để xác thực và bảo mật thông tin, dữ liệu.

c) Bố trí máy tính riêng không kết nối mạng, đặt mật khẩu, mã hóa dữ liệu và các biện pháp bảo mật khác bảo đảm an toàn thông tin để soạn thảo, lưu trữ dữ liệu, thông tin và tài liệu quan trọng ở các mức độ mật, tuyệt mật, tối mật.

d) Thường xuyên kiểm tra, giám sát các hoạt động chia sẻ, gửi, nhận thông tin, dữ liệu trong hoạt động nội bộ; khuyến cáo việc chia sẻ, gửi, nhận thông tin trên môi trường mạng cần phải sử dụng mật khẩu để bảo vệ thông tin.

đ) Đối với hoạt động trao đổi thông tin, dữ liệu với bên ngoài, đơn vị và cá nhân thực hiện trao đổi thông tin, dữ liệu ra bên ngoài cam kết và có biện pháp bảo mật thông tin, dữ liệu được trao đổi. Giao dịch trực tuyến phải được truyền đầy đủ, đúng địa chỉ, tránh bị sửa đổi, tiết lộ hoặc nhân bản một cách trái phép; sử dụng các cơ chế xác thực mạnh, chữ ký số khi tham gia giao dịch, sử dụng các giao thức truyền thông an toàn.

Điều 8. Xử lý vi phạm

Các phòng, ban, đơn vị trực thuộc; công chức, viên chức, người lao động thuộc Văn phòng vi phạm Quy chế này và các quy định của pháp luật hiện hành về quản lý, khai thác và sử dụng hệ thống mạng, thiết bị tin học thì tuỳ theo tính chất, mức độ vi phạm sẽ bị xử lý theo quy định, nếu vi phạm gây thiệt hại hư hỏng đến tài sản, thiết bị, thông tin, dữ liệu trên mạng máy tính của Văn phòng thì phải chịu trách nhiệm bồi thường, khắc phục hậu quả theo quy định của pháp luật hiện hành.

Chương III
TỔ CHỨC THỰC HIỆN

1. Toàn thể công chức, viên chức, người lao động thuộc Văn phòng chịu trách nhiệm thi hành Quy chế này.

2. Lãnh đạo các phòng, ban, đơn vị trực thuộc Văn phòng có trách nhiệm quán triệt, chỉ đạo và giám sát công chức, viên chức, người lao động thuộc phòng, đơn vị mình thực hiện đúng nội dung Quy chế này.

3. Trong quá trình tổ chức thực hiện, nếu có những vấn đề khó khăn, vướng mắc các phòng, đơn vị cần phản ánh kịp thời với Trung tâm Công báo - Tin học để tổng hợp, trình Lãnh đạo Văn phòng xem xét, sửa đổi, bổ sung Quy chế cho phù hợp./.