ỦY BAN NHÂN DÂN TỈNH ĐIỆN BIÊN	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc
Số: 19 /2022/QĐ-UBND	*Điện Biên, ngày 27 tháng 6 năm 2022*

QUYẾT ĐỊNH
Ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin, chuyển đổi số của cơ quan, đơn vị tỉnh Điện Biên

ỦY BAN NHÂN DÂN TỈNH ĐIỆN BIÊN

Căn cứ Luật Tổ chức chính quyền địa phương ngày 19 tháng 6 năm 2015; Luật Sửa đổi, bổ sung một số điều Luật Tổ chức chính phủ và Luật Tổ chức chính quyền địa phương ngày 22 tháng 11 năm 2019;

Căn cứ Luật Ban hành văn bản quy phạm pháp luật ngày 22 tháng 6 năm 2015; Luật Sửa đổi, bổ sung một số điều của Luật Ban hành văn bản quy phạm pháp luật ngày 18 tháng 6 năm 2020;

Căn cứ Luật Công nghệ thông tin ngày 29 tháng 6 năm 2006;

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

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

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ về Ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước;

Căn cứ Nghị định số 72/2013/NĐ-CP ngày 15 tháng 7 năm 2013 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng;

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

Căn cứ Quyết định số 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 trưởng Bộ Thông tin và Truyền thông về 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 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 27/2017/TT-BTTTT ngày 20 tháng 10 năm 2017 của Bộ Thông tin và Truyền thông quy định về việc quản lý vận hành, sử dụng và

bảo đảm an toàn thông tin trên Mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước;

Theo đề nghị của Giám đốc Sở Thông tin và Truyền thông.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này "Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin, chuyển đổi số của các cơ quan, đơn vị tỉnh Điện Biên".

Điều 2. Quyết định này có hiệu lực kể từ ngày 08 tháng 7 năm 2022.

Điều 3. Chánh Văn phòng Ủy ban nhân dân tỉnh; Giám đốc Sở Thông tin và Truyền thông, Thủ trưởng các sở, ban, ngành, đoàn thể tỉnh; Chủ tịch Ủy ban nhân dân các huyện, thị xã, thành phố và 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;
- Bộ Thông tin và Truyền thông;
- Vụ Pháp chế - Bộ Thông tin và Truyền thông;
- TT: Tỉnh ủy, HĐND tỉnh;
- Lãnh đạo UBND tỉnh;
- Uỷ ban MTTQ tỉnh;
- VP.Tỉnh ủy, các Ban đảng tỉnh;
- Cơ quan Báo, Đài tỉnh;
- Cổng thông tin điện tử tỉnh;
- Trung tâm Tin học - Công báo tỉnh;
- Lưu: VT, KTN(LVC).

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

ỦY BAN NHÂN DÂN TỈNH ĐIỆN BIÊN

Lê Thành Đô

ỦY BAN NHÂN DÂN TỈNH ĐIỆN BIÊN	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc

QUY CHẾ

Bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin, chuyển đổi số của cơ quan, đơn vị tỉnh Điện Biên

(Ban hành kèm theo Quyết định số 19 /2022/QĐ-UBND ngày 27 tháng 6 năm 2022 của Uỷ ban nhân dân tỉnh Điện Biên)

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 việc bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin, chuyển đổi số của các cơ quan, đơn vị, địa phương trên địa bàn tỉnh Điện Biên.

2. Đối tượng áp dụng:

a) Các cơ quan Đảng, đoàn thể, các tổ chức chính trị - xã hội; các sở, ban, ngành tỉnh; các đơn vị sự nghiệp công lập trực thuộc Ủy ban nhân dân tỉnh; Ủy ban nhân dân các huyện, thị xã, thành phố; Ủy ban nhân dân các xã, phường, thị trấn; các cơ quan được ngân sách Nhà nước bảo đảm kinh phí hoạt động có sử dụng các hệ thống thông tin trên địa bàn tỉnh (sau đây gọi tắt là các cơ quan, đơn vị).

b) Cán bộ, công chức, viên chức, người lao động (gọi tắt là cán bộ, công chức) và các tổ chức, cá nhân có liên quan tham gia vận hành, khai thác các hệ thống thông tin tại các cơ quan, đơn vị.

c) Khuyến khích các cơ quan, đơn vị khác trên địa bàn tỉnh áp dụng quy chế này trong hoạt động ứng dụng công nghệ thông tin, chuyển đổi số tại cơ quan, đơn vị.

Điều 2. Mục đích, nguyên tắc bảo đảm an toàn thông tin mạng

1. 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, chuyển đổi số trong hoạt động của các cơ quan, đơn vị.

2. Hoạt động ứng dụng công nghệ thông tin, chuyển đổi số của các cơ quan, đơn vị phải tuân thủ theo nguyên tắc bảo đảm an toàn thông tin mạng được quy định tại Điều 4, Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015 và Điều 41 Nghị định 64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước.

Chương II
ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG

Điều 3. Quản lý an toàn thông tin của các cơ quan, đơn vị đối với người sử dụng

1. Cơ quan, đơn vị, địa phương khi tiếp nhận, tuyển dụng nhân sự mới phải có trách nhiệm phổ biến cho nhân sự mới các quy định về bảo đảm an toàn thông tin mạng tại cơ quan, đơn vị, địa phương.

2. Cơ quan, đơn vị, địa phương phải thường xuyên tổ chức quán triệt các quy định về an toàn thông tin mạng, nhằm nâng cao nhận thức về trách nhiệm bảo đảm an toàn thông tin mạng của từng cá nhân trong cơ quan, đơn vị, địa phương.

3. Quản lý và phân quyền truy cập trong các phần mềm, nền tảng ứng dụng, hệ thống thông tin, cơ sở dữ liệu phù hợp với chức năng, nhiệm vụ, quyền hạn của người tham gia quản lý, vận hành, khai thác, sử dụng.

4. Khi cán bộ, công chức đã nghỉ việc hoặc chuyển công tác, cơ quan, đơn vị, địa phương phải thực hiện việc thu hồi các thiết bị công nghệ thông tin thuộc quyền quản lý; đồng thời phải thông báo ngay bằng văn bản đến cơ quan quản lý, quản trị phần mềm, nền tảng ứng dụng dùng chung, hệ thống thông tin, cơ sở dữ liệu để thực hiện các biện pháp kỹ thuật cập nhật lại, khóa hoặc hủy tài khoản người dùng.

Điều 4. Quản lý truy cập

1. Đối với cơ quan, đơn vị, người sử dụng có trách nhiệm

a) Bảo vệ bí mật thông tin tài khoản cá nhân, hoặc tài khoản của cơ quan, đơn vị, địa phương khi được phân công sử dụng; 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) Khi khai thác, sử dụng các phần mềm, nền tảng dùng chung của tỉnh tại các điểm truy cập Internet công cộng, không đặt chế độ lưu trữ mật khẩu trong quá trình 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 các cơ quan, 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 (độ dài tối thiểu 8 ký tự, có ký tự chữ cái thường, ký tự chữ cái hoa, ký tự số hoặc ký tự đặc biệt như !, @, #, $, %) và phải được thay đổi ít nhất 03 tháng/lần

cho tất cả các tài khoản truy cập vào hệ thống máy chủ, thiết bị mạng, máy tính, các ứng dụng;

e) Cơ quan, đơn vị rà soát tối thiểu 03 tháng/lần các tài khoản đăng nhập, bảo đảm các tài khoản và quyền truy cập hệ thống được cấp phát đúng, đủ;

g) Cơ quan, đơn vị, địa phương, cá nhân tham gia sử dụng mạng chuyên dùng thực hiện nghiêm túc các nội dung về đảm bảo an toàn thông tin mạng trên mạng truyền số liệu chuyên dùng được quy định tại các Điều 11, 12, 13 của Thông tư số 27/2017/TT-BTTTT ngày 20 tháng 10 năm 2017 của Bộ Thông tin và Truyền thông quy định về việc quản lý vận hành, sử dụng và bảo đảm an toàn thông tin trên Mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước; Quyết định số 10/2021/QĐ-UBND ngày 05 tháng 5 năm 2021 của Ủy ban nhân dân tỉnh Điện Biên về Ban hành Quy chế quản lý, vận hành và sử dụng mạng truyền số liệu chuyên dùng cấp II trên địa bàn tỉnh Điện Biên.

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 dùng chung là duy nhất;

b) Phân công cán bộ, công chức chuyên trách hoặc phụ trách công nghệ thông tin, chuyển đổi số để quản lý kỹ thuật nghiệp vụ về an toàn thông tin tại cơ quan, đơn vị;

c) Thủ trưởng cơ quan, đơn vị tạo điều kiện để cán bộ, công chức chuyên trách hoặc phụ trách công nghệ thông tin, chuyển đổi số học tập, tiếp thu công nghệ, kiến thức an toàn thông tin;

d) Hàng năm, xác định các nhiệm vụ bảo đảm an toàn cho hệ thống thông tin (mở rộng, nâng cấp trang thiết bị; đào tạo, bồi dưỡng kiến thức công nghệ thông tin, ...), để đề xuất kinh phí đến cơ quan có thẩm quyền hoặc phân bổ kinh phí duy trì hoạt động hệ thống thông tin hiệu quả;

đ) Quản lý các tài khoản của hệ thống thông tin, tài khoản người dùng bao gồm: Tạo mới, sửa đổi, hủy các tài khoản. Thường xuyên kiểm tra các tài khoản của hệ thống thông tin; triển khai các công cụ để hỗ trợ việc quản lý các tài khoản của hệ thống thông tin;

e) 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;

g) Kiểm soát và theo dõi tất cả các phương pháp truy cập từ xa tới hệ thống thông tin, triển khai nhiều cơ chế giám sát, cam kết từ các truy cập từ xa; phát hiện sớm việc truy cập trái phép vào mạng máy tính hay thiết bị lưu trữ dữ liệu;

h) Thiết lập hệ thống thông tin ghi nhận và lưu vết các sự kiện: Quá trình đăng nhập hệ thống, các thao tác cấu hình hệ thống, quá trình truy xuất hệ thống,...ghi nhận đầy đủ các thông tin trong các bản ghi nhật ký, thời gian lưu trữ các bản ghi nhật ký hệ thống tối thiểu 01 năm;

i) Cập nhật và lưu trữ cấu hình chuẩn các thành phần của hệ thống, trước khi tiến hành cài đặt, thiết lập cấu hình lại hệ thống thông tin, đảm bảo duy trì hoạt động của hệ thống thông tin; kiểm soát quá trình cài đặt trên máy chủ;

k) Cấu hình hệ thống thông tin cung cấp những chức năng cơ bản cho người dùng; thiết lập các chế độ phân quyền truy cập theo chỉ đạo của Thủ trưởng đơn vị;

l) Định kỳ hàng tuần sao lưu thông tin (không lưu đè thông tin, sao lưu dự phòng các thông tin thay đổi), dữ liệu của cơ quan, đơn vị và lưu trữ thông tin sao lưu ở nơi an toàn theo quy định; thường xuyên kiểm tra thông tin, dữ liệu sao lưu để đảm bảo tính sẵn sàng và toàn vẹn;

m) Cơ quan, đơn vị, địa phương và người dùng chịu trách nhiệm về những thiệt hại do người dùng tại cơ quan, đơn vị 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 5. Quản lý nhật ký trong quá trình vận hành các hệ thống thông tin

1. Cơ quan, đơn vị, địa phương phải thực hiện việc ghi nhật ký trên các thiết bị mạng máy tính, phần mềm ứng dụng, hệ điều hành, cơ sở dữ liệu nhằm bảo đảm các sự kiện quan trọng xảy ra trên hệ thống được ghi nhận và lưu giữ. Các bản ghi nhật ký này phải được bảo vệ an toàn nhằm sử dụng để phục vụ công tác kiểm tra, phân tích khi cần thiết.

2. Các sự kiện tối thiểu cần phải được ghi nhật ký gồm: Quá trình đăng nhập hệ thống; tạo, cập nhật hoặc xóa dữ liệu; các hành vi xem, thiết lập cấu hình hệ thống; việc thiết lập các kết nối bất thường vào, ra hệ thống; thay đổi quyền truy cập hệ thống.

3. Thường xuyên thực hiện việc theo dõi bản ghi nhật ký của hệ thống và các sự kiện khác có liên quan để đánh giá, báo cáo các rủi ro và mức độ nghiêm trọng các rủi ro đó.

Điều 6. Phòng chống phần mềm độc hại

1. Các máy chủ, máy trạm, các thiết bị công nghệ thông tin trong mạng và hệ thống thông tin phải được cài đặt phần mềm phòng chống mã độc tập trung. 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. Hệ điều hành, phần mềm cài đặt trên máy chủ, máy trạm phải được cập nhật vá lỗ hổng bảo mật thường xuyên, kịp thời.

3. Cán bộ, công chức trong các cơ quan, đơn vị, địa phương phải được hướng dẫn về phòng chống phần mềm độc hại, các rủi ro do mã độc gây ra; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm trên máy trạm khi chưa có sự đồng ý của người có thẩm quyền theo quy định của đơn vị.

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

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

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

7. Máy chủ chỉ được dùng để cài đặt các phần mềm, dịch vụ dùng chung của cơ quan, đơn vị; không cài đặt phần mềm không rõ nguồn gốc, phần mềm phục vụ mục đích cá nhân và mục đích khác, không phục vụ công việc.

8. Khi phát hiện bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại trên máy trạm như: Máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống phần mềm độc hại, sự cố lặp đi lặp lại, có dấu hiệu mất dữ liệu..., người sử dụng phải tắt máy, ngắt kết nối từ máy tính đến mạng nội bộ (LAN), mạng WAN nội tỉnh, mạng Internet,... và báo trực tiếp cho bộ phận có trách nhiệm của cơ quan, đơn vị để xử lý.

Điều 7. Bảo đảm an toàn trong xây dựng hệ thống thông tin

1. Các hoạt động liên quan đến xây dựng, thiết lập, quản lý, vận hành, nâng cấp mở rộng hệ thống thông tin phải thực hiện xác định cấp độ và phương án bảo đảm an toàn thông tin mạng theo quy định tại 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 (sau đây viết tắt là Nghị định 85/2016/NĐ-CP) và hướng dẫn tại 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 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ (sau đây viết tắt là Thông tư số 03/2017/TT-BTTTT).

2. Nhiệm vụ quản lý về hướng dẫn xác định hệ thống thông tin và cấp độ an toàn hệ thống thông tin; thực hiện các yêu cầu bảo đảm an toàn hệ thống thông tin theo cấp độ; thực hiện kiểm tra, đánh giá an toàn thông tin mạng; tiếp nhận và thẩm định hồ sơ đề xuất cấp độ; báo cáo, chia sẻ thông tin thực hiện theo hướng dẫn của Bộ Thông tin và Truyền thông tại Thông tư số 03/2017/TT-BTTTT.

3. Cơ quan, đơn vị, địa phương chủ quản hệ thống thông tin phải tổ chức kiểm tra, đánh giá định kỳ về an toàn thông tin của các hệ thống thông tin đang quản lý.

4. Sở Thông tin và Truyền thông tổ chức kiểm tra, đánh giá an toàn thông tin đối với các hệ thống thông tin do Sở Thông tin và Truyền thông phê duyệt hồ sơ đề xuất cấp độ; kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin.

Điều 8. Sao lưu dữ liệu dự phòng

1. Đối với các cơ quan, đơn vị, địa phương và người sử dụng

a) Khi lưu trữ, khai thác, trao đổi thông tin, dữ liệu phải bảo đảm tính toàn vẹn, tính tin cậy, tính sẵn sàng. Khi lưu trữ, trao đổi thông tin, dữ liệu quan trọng phải áp dụng kỹ thuật mã hóa, thiết lập mật mã, ứng dụng chữ ký số và phải có cơ chế lưu trữ dự phòng;

b) Phải lập kế hoạch và thực hiện sao lưu dữ liệu dự phòng định kỳ ít nhất một lần trong tuần các dữ liệu quan trọng, bao gồm: Cơ sở dữ liệu và các dữ liệu quan trọng được triển khai, lưu trữ (bao gồm dữ liệu phát sinh trong quá trình vận hành các phần mềm ứng dụng như: Các tập tin văn bản, hình ảnh, các tập tin dữ liệu khác). Sau khi sao lưu, lưu trữ bản sao lưu bằng thiết bị lưu trữ ngoài (như: Đĩa quang, ổ cứng ngoài, các thiết bị lưu trữ khác) theo quy định lưu trữ hiện hành, bảo đảm tính sẵn sàng, bảo mật và toàn vẹn nhằm đáp ứng yêu cầu phục hồi dữ liệu, khắc phục hệ thống thông tin cho hoạt động bình thường kịp thời khi có sự cố xảy ra.

2. Đối với cơ quan, đơn vị, địa phương chủ quản các hệ thống thông tin

a) Có trách nhiệm ban hành và thực hiện quy trình sao lưu dự phòng và phục hồi cho các phần mềm, dữ liệu;

b) Xây dựng 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;

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

Điều 9. Quản lý sự cố

1. Phân loại mức độ nghiêm trọng của các sự cố, bao gồm:

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

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

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

d) Khẩn cấp: Sự cố ảnh hưởng đến sự liên tục của nhiều hoạt động chính của cơ quan, đơn vị, địa phương như: Toàn bộ hệ thống thiết bị công nghệ thông

tin, hệ thống cung cấp điện ngừng hoạt động, hệ thống trang thông tin điện tử bị tin tặc (hacker) tấn công, xâm nhập, thay đổi nội dung...

2. Khi có sự cố hoặc nguy cơ mất an toàn thông tin mạng xảy ra như: Hệ thống hoạt động chậm bất thường, không truy cập được hệ thống, nội dung thông tin bị thay đổi không chủ động hoặc các dấu hiệu bất thường khác thì tiến hành quy trình ứng cứu sự cố theo các bước sau:

a) Bước 1: Nếu hệ thống có nguy cơ mất an toàn thông tin mạng thuộc thẩm quyền cơ quan, đơn vị, địa phương trực tiếp quản lý thì thực hiện tiếp Bước 2. Nếu hệ thống có nguy cơ mất an toàn thông tin mạng thuộc Trung tâm Công nghệ thông tin và Truyền thông trực thuộc Sở Thông tin và Truyền thông quản lý (các hệ thống được triển khai tập trung tại Trung tâm Dữ liệu tỉnh) thì thực hiện tiếp Bước 3;

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

c) Bước 3: Báo sự cố đến Sở Thông tin và Truyền thông theo Mẫu số 03 của 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 và thực hiện tiếp Bước 4;

d) Bước 4: Phối hợp với Trung tâm Công nghệ thông tin và Truyền thông trực thuộc Sở Thông tin và Truyền thông và các cơ quan, tổ chức có liên quan để tiến hành khắc phục sự cố và thực hiện tiếp Bước 5;

đ) Bước 5: Lập biên bản ghi nhận và kết thúc quy trình phối hợp xử lý sự cố theo Mẫu số 04 của Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông Quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc, lãnh đạo cơ quan, đơn vị phải chỉ đạo kịp thời để khắc phục và hạn chế thiệt hại, báo cáo bằng văn bản cho cơ quan cấp trên trực tiếp quản lý và Sở Thông tin và Truyền thông.

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

Chương III
ĐIỀU KHOẢN THI HÀNH

Điều 10. Trách nhiệm của Ban chỉ đạo Chuyển đổi số

Ban chỉ đạo Chuyển đổi số tỉnh đảm nhiệm chức năng Ban chỉ đạo ứng cứu khẩn cấp sự cố an toàn thông tin mạng tại tỉnh Điện Biên và có trách nhiệm, quyền hạn thực hiện theo quy định tại Điều 5, Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 2017 của Thủ tướng Chính phủ về ban hành quy định

về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia (sau đây gọi tắt là Quyết định số 05/2017/QĐ-TTg).

Điều 11. Trách nhiệm của Sở Thông tin và Truyền thông

1. Tham mưu giúp Ủy ban nhân dân tỉnh về công tác bảo đảm an toàn thông tin mạng trên địa bàn tỉnh và chịu trách nhiệm trước Ủy ban nhân dân tỉnh trong việc bảo đảm an toàn thông tin mạng cho các hệ thống thông tin của tỉnh.

2. Thực hiện thủ tục xác định cấp độ an toàn thông tin mạng và bảo đảm an toàn cho các hệ thống thông tin theo quy định của Luật An toàn thông tin mạng, Nghị định số 85/2016/NĐ-CP và hướng dẫn tại Thông tư số 03/2017/TT-BTTTT.

3. Xây dựng và triển khai các Kế hoạch, chương trình, dự án đầu tư, đào tạo về an toàn thông tin trong ứng dụng công nghệ thông tin, chuyển đổi số trên địa bàn tỉnh.

4. Tùy theo mức độ sự cố, phối hợp Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) và các đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố an toàn thông tin trên địa bàn tỉnh; Cảnh báo các vấn đề về an toàn thông tin trong các cơ quan nhà nước trên địa bàn tỉnh.

5. Định kỳ tổng hợp báo cáo Ủy ban nhân dân tỉnh và Bộ Thông tin và Truyền thông về công tác an toàn thông tin số trên địa bàn tỉnh.

5. Chủ trì, phối hợp với các cơ quan, đơn vị liên quan thanh tra, kiểm tra định kỳ hoặc đột xuất; kịp thời phát hiện và xử lý theo thẩm quyền đối với các hành vi vi phạm an toàn thông tin mạng trên địa bàn tỉnh.

6. Tuyên truyền và định hướng tuyên truyền, phối hợp tuyên truyền đến các phương tiện truyền thông đại chúng trên địa bàn tỉnh về công tác bảo đảm an toàn thông tin.

7. Chỉ đạo, hướng dẫn về nghiệp vụ quản lý vận hành, kỹ thuật bảo đảm an toàn thông tin mạng; hỗ trợ giải quyết sự cố khi có yêu cầu.

8. Tham gia mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia và thực hiện trách nhiệm, quyền hạn của thành viên mạng lưới ứng cứu an toàn thông tin mạng quốc gia theo quy định tại Quyết định số 05/2017/QĐ-TTg.

9. Hàng năm, tổ chức đào tạo chuyên sâu về an toàn thông tin mạng cho cán bộ, công chức chuyên trách công nghệ thông tin đảm bảo an toàn thông tin mạng của các cơ quan, đơn vị.

10. Khảo sát, triển khai, xây dựng mô hình kết nối mạng nội bộ (LAN) đảm bảo an toàn thông tin chung cho các cơ quan, đơn vị triển khai thực hiện.

Điều 12. Trách nhiệm của Công an tỉnh

1. Chủ trì, phối hợp với Sở Thông tin và Truyền thông và các cơ quan, đơn vị có liên quan xây dựng kế hoạch, kiểm soát, phòng ngừa, phát hiện, đấu tranh, ngăn chặn các loại tội phạm lợi dụng hệ thống thông tin gây phương hại đến an ninh quốc gia và trật tự an toàn xã hội trên địa bàn tỉnh.

2. Phối hợp với Sở Thông tin và Truyền thông trong công tác thanh tra, kiểm tra về an toàn thông tin mạng.

3. Tiếp nhận điều tra và xử lý các tổ chức, cá nhân vi phạm pháp luật về an toàn thông tin mạng theo thẩm quyền.

Điều 13. Trách nhiệm của Sở Kế hoạch và Đầu tư

Căn cứ khả năng cân đối vốn trong kế hoạch đầu tư công trung hạn và các quy định của pháp luật tham mưu cho Ủy ban nhân dân tỉnh xem xét, bố trí nguồn vốn ngân sách nhà nước để thực hiện các dự án, nhiệm vụ về bảo đảm an toàn thông tin mạng phù hợp với quy định và nhu cầu thực tế của địa phương.

Điều 14. Trách nhiệm của Sở Tài chính

Hàng năm, căn cứ khả năng cân đối ngân sách địa phương và chế độ, tiêu chuẩn, định mức do nhà nước ban hành, tham mưu Ủy ban nhân dân tỉnh bố trí kinh phí triển khai thực hiện các dự án, nhiệm vụ về bảo đảm an toàn thông tin mạng theo phân cấp ngân sách hiện hành.

Điều 15. Trách nhiệm của các cơ quan, đơn vị, địa phương

1. Thủ trưởng cơ quan, đơn vị có trách nhiệm tổ chức thực hiện các quy định tại Quy chế này và chịu trách nhiệm trước Ủy ban nhân dân tỉnh trong công tác bảo đảm an toàn thông tin mạng của cơ quan, đơn vị mình.

2. Phân công bộ phận hoặc cán bộ phụ trách hoặc chuyên trách bảo đảm an toàn thông tin của cơ quan, đơn vị; tạo điều kiện để cán bộ phụ trách hoặc chuyên trách an toàn thông tin được học tập, nâng cao trình độ về an toàn thông tin; thường xuyên tổ chức quán triệt các quy định về an toàn thông tin mạng trong cơ quan, đơn vị; xác định các yêu cầu, trách nhiệm bảo đảm an toàn thông tin mạng đối với các vị trí cần tuyển dụng hoặc phân công.

3. Ban hành quy định, quy trình nội bộ về bảo đảm an toàn thông tin mạng phù hợp với Quy chế này và các quy định của pháp luật.

4. Tuyên truyền, phổ biến Quy chế này và các quy định khác của pháp luật có liên quan về an toàn thông tin trong phạm vi trách nhiệm và quyền hạn của từng cơ quan.

5. Các cơ quan, đơn vị, địa phương có trách nhiệm thực hiện xác định cấp độ an toàn thông tin mạng và bảo đảm an toàn cho hệ thống thông tin của đơn vị quản lý theo quy định tại Luật An toàn thông tin mạng, Nghị định số 85/2016/NĐ-CP và hướng dẫn tại Thông tư số 03/2017/TT-BTTTT.

6. Phối hợp, cung cấp thông tin và tạo điều kiện cho các đơn vị có thẩm quyền triển khai công tác kiểm tra khắc phục sự cố an toàn thông tin mạng kịp thời, nhanh chóng và đạt hiệu quả.

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

8. Thường xuyên thông báo, báo cáo sự cố an toàn thông tin mạng (nếu có) về Sở Thông tin và Truyền thông để phối hợp xử lý theo quy định.

9. Báo cáo định kỳ vào ngày 15/10 hàng năm hoặc đột xuất theo yêu cầu về Sở Thông tin và Truyền thông để tổng hợp, báo cáo Ủy ban nhân dân tỉnh, Bộ Thông tin và Truyền thông.

10. Hằng năm bố trí kinh phí đảm an toàn thông tin mạng trong nội bộ cơ quan, đơn vị, địa phương mình; lập kế hoạch nâng cấp, bảo trì, sửa chữa, gia hạn bản quyền phần mềm… cho các hệ thống phần cứng, phần mềm nhằm thực hiện tốt công tác bảo mật, bảo đảm an toàn thông tin mạng.

Điều 16. Trách nhiệm của cán bộ, công chức trong các cơ quan, đơn vị, địa phương

1. Trách nhiệm của cán bộ, công chức phụ trách an toàn thông tin mạng:

a) Chịu trách nhiệm bảo đảm an toàn thông tin mạng của đơn vị;

b) Tham mưu lãnh đạo cơ quan, đơn vị ban hành các quy định, quy trình nội bộ, triển khai các giải pháp kỹ thuật bảo đảm an toàn thông tin mạng;

c) Thực hiện việc giám sát, đánh giá, báo cáo lãnh đạo cơ quan, đơn vị các rủi ro mất an toàn thông tin mạng và mức độ nghiêm trọng của các rủi ro đó;

d) Phối hợp với các tổ chức, cá nhân có liên quan trong việc kiểm soát, phát hiện và khắc phục các sự cố an toàn, an ninh thông tin mạng.

2. Trách nhiệm của cán bộ, công chức trong các cơ quan, đơn vị, địa phương:

a) Nghiêm túc chấp hành các quy định, quy trình nội bộ, Quy chế này và các quy định khác của pháp luật về an toàn thông tin mạng. Chịu trách nhiệm bảo đảm an toàn thông tin trong phạm vi trách nhiệm và quyền hạn được giao;

b) Khi tham gia vận hành mạng máy tính của cơ quan, đơn vị, địa phương phải nghiêm chỉnh chấp hành chế độ bảo mật, an toàn, an ninh thông tin đồng thời chịu trách nhiệm đối với các thông tin mà mình cung cấp. Mỗi cán bộ, công chức phải có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng; không tự ý thay đổi, tháo lắp các thiết bị trên máy tính; không được vào các trang thông tin điện tử không rõ về nội dung; không tải và cài đặt các phần mềm không rõ nguồn gốc, không liên quan đến công việc chuyên môn; không nhấp chuột vào các đường dẫn lạ không rõ về nội dung; không cho phép bất cứ hành vi nào gây tổn hại đến dịch vụ, gây hư hỏng thiết bị mạng; không cung cấp thông tin không trung thực để công bố trên mạng; sử dụng mạng để thâm nhập vào các mạng máy tính khi chưa được phép; không đưa các thông tin có nội dung "mật", "tối mật" và "tuyệt mật" lên hệ thống máy tính có kết nối mạng;

c) Trong trao đổi thông tin, dữ liệu phục vụ công việc, các cơ quan, đơn vị, cán bộ, công chức phải sử dụng hệ thống thông tin do cơ quan, đơn vị có thẩm quyền triển khai như: Hệ thống thư điện tử tỉnh (@dienbien.gov.vn) hoặc hệ thống thư điện tử của bộ, ngành, lĩnh vực; hệ thống quản lý văn bản và điều

hành. Mỗi cán bộ, công chức không sử dụng các trang mạng xã hội, các dịch vụ thư điện tử công cộng,... để trao đổi thông tin quan trọng liên quan đến công việc chuyên môn của cơ quan, đơn vị;

d) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo ngay với cấp trên và bộ phận phụ trách công nghệ thông tin của đơn vị để kịp thời ngăn chặn và xử lý;

đ) Tham gia các chương trình đào tạo, hội nghị về an toàn thông tin do các cơ quan, đơn vị chuyên trách an toàn thông tin mạng hoặc Sở Thông tin và Truyền thông tổ chức.

Điều 17. Trách nhiệm của các tổ chức, cá nhân khác

1. Các tổ chức, cá nhân khác có sử dụng các hệ thống thông tin do Ủy ban nhân dân tỉnh triển khai hoặc liên quan đến hoạt động ứng dụng công nghệ thông tin của các cơ quan Nhà nước tỉnh Điện Biên phải tuân thủ Quy chế này và các quy định hiện hành của pháp luật có liên quan.

2. Khi phát hiện sự cố ảnh hưởng đến an toàn hệ thống thông tin, phải thông báo ngay với cơ quan Nhà nước, nơi tổ chức, cá nhân đang thực hiện giao tiếp.

3. Các tổ chức, cá nhân tham gia vào quá trình ứng dụng công nghệ thông tin trên địa bàn tỉnh, chịu sự thanh tra, kiểm tra của các cơ quan Nhà nước có thẩm quyền về lĩnh vực an toàn thông tin mạng.

Điều 18. Tổ chức thực hiện

1. Sở Thông tin và Truyền thông chủ trì, phối hợp với các cơ quan, đơn vị và các tổ chức, cá nhân có liên quan triển khai thực hiện Quy chế này.

2. Thủ trưởng các các cơ quan, đơn vị, đia phương chịu trách nhiệm tổ chức triển khai thực hiện Quy chế tại cơ quan, đơn vị, địa phương mình.

3. Trong quá trình thực hiện nếu có phát sinh khó khăn, vướng mắc cần sửa đổi, bổ sung các cơ quan, đơn vị, địa phương kịp thời báo cáo về Sở Thông tin và Truyền thông tổng hợp trình Ủy ban nhân dân tỉnh xem xét, quyết định./.