ỦY BAN NHÂN DÂN TỈNH LÀO CAI	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 61 /2021/QĐ-UBND	*Lào Cai, ngày 31 tháng 12 năm 2021*

QUYẾT ĐỊNH

Ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin trong các cơ quan nhà nước trên địa bàn tỉnh Lào Cai

ỦY BAN NHÂN DÂN TỈNH LÀO CAI

Căn cứ Luật Tổ chức chính quyền địa phương ngày 19 tháng 6 năm 2015;

Căn cứ Luật sửa đổi, bổ sung một số điều của 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;

Căn cứ 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 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 34/2016/NĐ-CP ngày 14 tháng 5 năm 2016 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật ban hành văn bản quy phạm pháp luật;

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 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 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 27/2017/TT-BTTTT ngày 20 tháng 10 năm 2017 của Bộ Trưởng Bộ Thông tin và Truyền thông quy định về quản lý, vận hành, kết nối,

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

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;

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

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 trong các cơ quan nhà nước trên địa bàn tỉnh Lào Cai.

Điều 2. Quyết định có hiệu lực kể từ ngày 15 tháng 01 năm 2022 và thay thế Quyết định số 18/2014/QĐ-UBND ngày 16 tháng 6 năm 2014 của Ủy ban nhân dân tỉnh Lào Cai về việc ban hành quy định bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin trên địa bàn tỉnh Lào Cai.

Điều 3. Chánh Văn phòng Ủy ban nhân dân tỉnh; Thủ trưởng các sở, ban, ngành tỉnh; Chủ tịch Ủy ban nhân dân các huyện, thị xã, thành phố và các cơ quan, tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3 (QĐ);
- Văn phòng Chính phủ;
- Bộ Thông tin và Truyền thông;
- Cục Kiểm tra văn bản QPPL-Bộ Tư pháp;
- TT: TU, HĐND, UBND tỉnh;
- TT Đoàn ĐBQH tỉnh;
- Các Ban xây dựng Đảng Tỉnh ủy;
- VP: TU, HĐND, Đoàn ĐBQH tỉnh;
- Các cơ quan ngành dọc tại tỉnh;
- Sở Tư pháp; Công báo, Cổng TTĐT tỉnh;
- Báo Lào Cai, Đài PT-TH tỉnh;
- LĐ Văn phòng UBND tỉnh;
- Lưu: VT, Các CV.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Trịnh Xuân Trường

ỦY BAN NHÂN DÂN TỈNH LÀO CAI	CỘNG HOÀ 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 trong các cơ quan nhà nước trên địa bàn tỉnh Lào Cai

(Ban hành kèm theo Quyết định số 61 /2021/QĐ-UBND ngày 31 tháng 12 năm 2021 của Ủy ban nhân dân tỉnh Lào Cai)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định việc bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin (sau đây viết tắt là CNTT) trong các cơ quan nhà nước trên địa bàn tỉnh Lào Cai.

Điều 2. Đối tượng áp dụng

1. Các sở, ban, ngành, ủy ban nhân dân (sau đây viết tắt là UBND) các huyện, thị xã, thành phố; các cơ quan Đảng, đoàn thể và tổ chức chính trị xã hội; các cơ quan ngành dọc đóng trên địa bàn tỉnh; các đơn vị sự nghiệp trực thuộc UBND tỉnh; UBND các xã, phường, thị trấn (sau đây viết tắt là các cơ quan, đơn vị).

2. Các tổ chức, cá nhân, doanh nghiệp có tham gia quản lý, cung cấp, vận hành, khai thác, ứng dụng CNTT trong hoạt động của các cơ quan, đơn vị nêu tại khoản 1 Điều này.

3. Cán bộ, công chức, viên chức, người lao động đang công tác trong các cơ quan, đơn vị nêu tại khoản 1 Điều này.

Điều 3. Mục đích, nguyên tắc bảo đảm an toàn thông tin mạng

1. 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 toàn thông tin trong quá trình ứng dụng CNTT trong hoạt động của các cơ quan, đơn vị.

2. Hoạt động ứng dụng CNTT 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 (sau đây viết tắt là Luật an toàn thông tin mạng), cụ thể như sau:

a) Cơ quan, tổ chức, cá nhân có trách nhiệm bảo đảm an toàn thông tin mạng. Hoạt động an toàn thông tin mạng của cơ quan, tổ chức, cá nhân phải đúng quy định của pháp luật, bảo đảm quốc phòng, an ninh quốc gia, bí mật nhà nước, giữ vững ổn định chính trị, trật tự, an toàn xã hội và thúc đẩy phát triển kinh tế - xã hội;

b) Tổ chức, cá nhân không được xâm phạm an toàn thông tin mạng của tổ chức, cá nhân khác;

c) Việc xử lý sự cố an toàn thông tin mạng phải bảo đảm quyền và lợi ích hợp pháp của tổ chức, cá nhân, không xâm phạm đến đời sống riêng tư, bí mật cá nhân, bí mật gia đình của cá nhân, thông tin riêng của tổ chức;

d) Hoạt động an toàn thông tin mạng phải được thực hiện thường xuyên, liên tục, kịp thời và hiệu quả.

Điều 4. Các hành vi bị nghiêm cấm

Các hành vi bị nghiêm cấm thực hiện theo quy định tại Điều 7 Luật an toàn thông tin mạng và Điều 8 Luật an ninh mạng.

Chương II
ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG

Điều 5. 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 khi được phân công nắm giữ, đồng thời phải thay đổi ngay mật khẩu tài khoản khi mới được cấp và tự chịu trách nhiệm trong việc quản lý, bảo vệ mật khẩu của tài khoản, không được cho người khác sử dụng tài khoản cá nhân hoặc của cơ quan, đơn vị;

b) Không đặt chế độ tự động ghi nhớ mật khẩu của các trình duyệt trong mọi trường hợp sử dụng;

c) Thiết lập mật mã truy cập và chế độ tự động bảo vệ màn hình sau 10 phút 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 (có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự hoa, ký tự số hoặc ký tự đặc biệt như: !, @, #, $, %) và phải được thay đổi 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) Các cơ quan, đơn vị cần 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) Khi sử dụng các ứng dụng dùng chung của tỉnh mọi người phải có ý thức tự bảo vệ thông tin cá nhân của mình; nghiêm cấm việc tiết lộ tài khoản đăng nhập của mình cho người không có thẩm quyền hoặc sử dụng trái phép tài khoản của người khác để truy cập trái phép vào hệ thống các phần mềm dùng chung của tỉnh;

h) Người sử dụng phải thay đổi mật khẩu mới sau lần đăng nhập đầu tiên đối với các tài khoản được cung cấp để truy cập các phần mềm, cơ sở dữ liệu dùng chung của tỉnh; không sử dụng chế độ ghi nhớ mật khẩu;

i) Khi khai thác, sử dụng các phần mềm ứng dụng dùng chung của tỉnh tại các điểm truy cập Internet công cộng, tuyệt đối không đặt chế độ ghi nhớ mật khẩu trong các trình duyệt;

k) Đối với cán bộ, công chức, viên chức đã nghỉ việc, chuyển công tác, phải có biện pháp khóa hoặc hủy tài khoản, quyền truy nhập các hệ thống dùng chung, thu hồi các thiết bị công nghệ thông tin liên quan.

2. Đối với các hệ thống thông tin dùng chung của tỉnh:

a) Bảo đảm mỗi tài khoản của tổ chức, cá nhân truy cập vào hệ thống thông tin là duy nhất;

b) Các hệ thống thông tin cần giới hạn số lần đăng nhập sai liên tiếp vào hệ thống (từ 03 đến 05 lần). Hệ thống tự động khóa tài khoản trong một khoảng thời gian nhất định nếu liên tục đăng nhập sai vượt quá số lần quy định trước khi tiếp tục cho đăng nhập và có phương thức hỗ trợ cấp lại mật khẩu tài khoản;

c) Đơn vị quản lý, vận hành các hệ thống dùng chung sẽ không chịu trách nhiệm về những thiệt hại do phía người dùng không tuân thủ các quy định về bảo vệ bí mật tài khoản dẫn đến thông tin cá nhân bị đánh cắp hay bị sửa đổi, các ứng dụng bị sử dụng mạo danh hay các hậu quả tiêu cực khác.

Điều 6. Quản lý nhật ký trong quá trình vận hành các hệ thống thông tin

1. Các cơ quan, đơn vị 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 và 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 7. Phòng chống phần mềm độc hại

1. Tất cả các máy trạm, máy chủ phải được trang bị phần mềm phòng chống phần mềm độc hại. Các phần mềm phòng chống phần mềm độc hại phải được thiết lập chế độ tự động cập nhật; chế độ tự động quét phần mềm độc hại 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, viên chức và người lao động 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 trong cơ quan.

4. Tất cả các máy tính của 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 di động.

5. Các máy tính xách tay, thiết bị di động (điện thoại thông minh, máy tính bảng,...) trước khi kết nối vào mạng LAN nội bộ của 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 ra 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, tình trạng này lặp đi lặp lại nhiều lần, ở các vị trí khác nhau; quan trọng nhất là có dấu hiệu mất dữ liệu..., người sử dụng phải tắt máy, ngắt kết nối từ máy tính đến mạng LAN nội bộ, mạng WAN nội tỉnh, mạng Internet,... và báo trực tiếp cho bộ phận có trách nhiệm của đơn vị để xử lý.

9. Hạn chế tối đa việc sử dụng các thiết bị lưu trữ ngoài để sao chép, di chuyển dữ liệu. Việc sử dụng các thiết bị lưu trữ ngoài, như: ổ cứng di động, các loại thẻ nhớ, thiết bị lưu trữ USB,... phải quét virus trước khi đọc hoặc sao chép dữ liệu.

Điều 8. Bảo đảm an toàn với các đơn vị có hệ thống thông tin riêng

1. Các cơ quan, đơn vị phải bố trí phòng máy chủ độc lập, phân công bộ phận chuyên trách hoặc cán bộ chuyên trách CNTT trực tiếp quản lý. Áp dụng các biện pháp và kiểm soát ra vào thích hợp.

2. Phòng máy chủ phải đảm bảo các điều kiện cho những thiết bị đặt trong đó hoạt động ổn định, các điều kiện tối thiểu, gồm: được bố trí ở khu vực có điều kiện an ninh tốt; khô ráo, có điều hòa không khí; nguồn cung cấp điện ổn định và có dự phòng; có bình chữa cháy hoặc hệ thống tự động cảnh báo, chữa cháy khẩn cấp; phòng, chống sét; có nội quy hướng dẫn làm việc trong khu vực an toàn bảo mật.

3. Thiết lập cơ chế bảo vệ mạng nội bộ bảo đảm an toàn thông tin khi có kết nối mạng nội bộ với mạng ngoài, như: Internet, mạng cơ quan khác; cần sử dụng hệ thống bảo vệ mạng nội bộ, như: hệ thống tường lửa, hệ thống chống xâm nhập trái phép...

4. Xây dựng và áp dụng các biện pháp bảo vệ, giám sát, ghi nhật ký hoạt động và quản lý hạ tầng kỹ thuật, hệ thống thông tin nhằm phòng ngừa, ngăn chặn và phát hiện sớm các truy cập trái phép.

5. Kiểm soát chặt chẽ việc cài đặt các phần mềm lên các máy chủ và máy trạm, đảm bảo tuân thủ quy định quản lý an toàn, an ninh thông tin của cơ quan, đơn vị và các quy định khác có liên quan.

Điều 9. Bảo đảm an toàn dữ liệu, cơ sở dữ liệu và phần mềm ứng dụng công nghệ thông tin

1. Các hệ thống phần mềm ứng dụng, cơ sở dữ liệu phải có cơ chế sao lưu dữ liệu dự phòng, dữ liệu được lưu trữ tại nơi an toàn đồng thời phải thường xuyên kiểm tra để đảm bảo sẵn sàng phục hồi khi có sự cố an toàn thông tin mạng xảy ra.

2. Sử dụng mật mã để bảo đảm an toàn và bảo mật dữ liệu trong lưu trữ và giao dịch theo quy định của Nhà nước về mật mã.

3 Quản lý chặt chẽ các thiết bị tin học lưu trữ dữ liệu, nghiêm cấm việc di chuyển, thay đổi vị trí khi chưa được phép của người có thẩm quyền. Trước khi thanh lý các máy tính, thiết bị công nghệ thông tin trong các cơ quan nhà nước, cán bộ chuyên trách công nghệ thông tin phải dùng các biện pháp kỹ thuật xoá bỏ vĩnh viễn dữ liệu trong ổ cứng máy tính.

4. Quản lý và phân quyền truy cập phần mềm ứng dụng và cơ sở dữ liệu phù hợp với chức năng, nhiệm vụ của người sử dụng.

5. Phần mềm hệ quản trị cơ sở dữ liệu phải được thiết lập cơ chế tự động cập nhật bản vá lỗ hổng bảo mật từ nhà sản xuất.

6. Bảo đảm an toàn cho Cổng/Trang thông tin điện tử: các cơ quan, đơn vị trong quá trình quản lý, khai thác và cung cấp thông tin trên Cổng/Trang thông tin điện tử của mình phải thường xuyên theo dõi, cập nhật phiên bản vá lỗi nhằm tránh các lỗi đã được công bố; thiết lập và cấu hình hệ thống máy chủ cài đặt Cổng/Trang thông tin điện tử an toàn giảm thiểu khả năng bị tin tặc tấn công. Tổ chức mô hình mạng hợp lý cũng như thiết lập các hệ thống phòng thủ quan trọng như tường lửa (firewall), thiết bị phát hiện, phòng, chống xâm nhập.

7. Các thiết bị CNTT dùng để soạn thảo, in ấn văn bản, lưu trữ thông tin bí mật nhà nước trong các cơ quan, đơn vị phải được bố trí riêng, tiến hành ở nơi đảm bảo bí mật, an toàn; không được kết nối vào mạng LAN của đơn vị. Đặc biệt là không được sử dụng máy tính đã nối mạng Internet đánh máy, in, sao tài liệu mật. Trên máy tính này phải thực hiện các chế độ mã hóa, phân quyền và đặt mật khẩu cho người được giao sử dụng để đảm bảo an toàn, bảo mật thông tin. 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.

Điều 10. Bảo đảm an toàn thông tin Trung tâm tích hợp dữ liệu của tỉnh

1. Xây dựng phương án đảm bảo an toàn thông tin mạng cho Trung tâm tích hợp dữ liệu của tỉnh; bảo đảm an toàn và thuận lợi đối với quá trình quản lý và sử dụng các dịch vụ.

2. Các cơ quan, đơn vị đặt dữ liệu hoặc kết nối vào Trung tâm tích hợp dữ liệu của tỉnh phải tuân thủ các chính sách an toàn thông tin mạng liên quan đến việc kết nối vào Trung tâm tích hợp dữ liệu của tỉnh.

3. Các cơ quan, đơn vị khi kết nối vào Trung tâm tích hợp dữ liệu phải bảo vệ thiết bị đầu cuối của mình, chịu trách nhiệm nếu để tin tặc kiểm soát máy tính và truy cập trái phép vào Trung tâm tích hợp dữ liệu của tỉnh.

Điều 11. Phát triển nguồn nhân lực an toàn thông tin

1. Cán bộ chuyên trách về CNTT trong các cơ quan, đơn vị được tạo điều kiện trang bị các thiết bị tin học, phương tiện kỹ thuật làm việc phù hợp với chuyên môn; tham dự đầy đủ các khóa đào tạo và bồi dưỡng kiến thức, nghiệp vụ cho cán bộ quản lý, kỹ thuật về an toàn thông tin mạng.

2. Các cơ quan, đơn vị xác định nhu cầu về đào tạo nguồn nhân lực bảo đảm an toàn thông tin tại cơ quan, đơn vị mình gửi Sở Thông tin và Truyền thông tổng hợp, xây dựng trình UBND tỉnh phê duyệt kế hoạch dài hạn, kế hoạch hàng năm về đào tạo, bồi dưỡng nghiệp vụ an toàn, an ninh thông tin cho cán bộ, công chức, viên chức và người lao động của tỉnh và thực hiện tổ chức đào tạo theo kế hoạch đã phê duyệt.

3. Các cơ quan, đơn vị phải thường xuyên tổ chức các hoạt động tuyên truyền, phổ biến nâng cao nhận thức về bảo đảm an toàn, an ninh thông tin mạng đến toàn thể bộ cán bộ, công chức, viên chức và người lao động tại cơ quan, đơn vị mình.

4. Sở Thông tin và Truyền thông xây dựng, trình UBND tỉnh kế hoạch tuyên truyền, phổ biến nâng cao nhận thức về an toàn, an ninh thông tin mạng trên địa bàn tỉnh và thực hiện các nội dung theo kế hoạch đã được phê duyệt.

5. Khuyến khích các cơ quan, đơn vị liên kết với tổ chức, cá nhân, doanh nghiệp CNTT uy tín mở các khóa đào tạo nhân lực trong lĩnh vực an toàn thông tin mạng.

Điều 12. 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 số 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 (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 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 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 13. Sao lưu dữ liệu dự phòng

1. Đối với các cơ quan, đơn vị 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 tháng đối với các dữ liệu quan trọng, bao gồm: cơ sở dữ liệu và các dữ liệu quan trọng được triển khai, lưu trữ (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 (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 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 14. Quản lý, diễn tập, ứng phó sự cố

1. Ban chỉ đạo, đơn vị chuyên trách ứng cứu khẩn cấp sự cố an toàn thông tin mạng:

a) Ban chỉ đạo xây dựng chính quyền điện tử tỉnh đảm nhiệm chức năng Ban chỉ đạo ứng cứu khẩn cấp sự cố an toàn thông tin mạng. Trách nhiệm và quyền hạn của Ban chỉ đạo ứng cứu khẩn cấp sự cố an toàn thông tin mạng được quy định tại khoản 2, Điều 5 Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 2017 của Thủ tướng Chính phủ (sau đây viết tắt là Quyết định số 05/2017/QĐ-TTg).

b) Sở Thông tin và Truyền thông là đơn vị chuyên trách về điều phối, ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh. Bộ phận chuyên trách về an toàn thông tin mạng tại các cơ quan, đơn vị trên địa bàn tỉnh đảm nhiệm vai trò chuyên trách về ứng cứu sự cố an toàn thông tin mạng trong phạm vi quản lý CNTT của cơ quan, đơn vị. Đơn vị chuyên trách về ứng cứu sự cố an toàn thông tin mạng thực hiện trách nhiệm quy định tại khoản 2, Điều 6 Quyết định số 05/2017/QĐ-TTg.

c) Sở Thông tin và Truyền thông trình UBND tỉnh thành lập Đội ứng cứu sự cố của tỉnh và Tổ chức ứng cứu sự cố trên phạm vi toàn tỉnh. Các cơ quan, đơn vị có trách nhiệm phối hợp với Sở Thông tin và Truyền thông thực hiện nhiệm vụ về ứng cứu sự cố tại các cơ quan, đơn vị.

2. Diễn tập và ứng phó sự cố an toàn thông tin mạng:

a) Chủ quản hệ thống thông tin tổ chức diễn tập ứng cứu sự cố theo kế hoạch ứng phó sự cố được phê duyệt.

b) Sở Thông tin và Truyền thông chủ trì, phối hợp với các cơ quan, đơn vị trên địa bàn tỉnh tham gia các cuộc diễn tập quốc gia, quốc tế do cơ quan điều phối quốc gia, Bộ Thông tin và Truyền thông tổ chức và tổ chức diễn tập ứng cứu sự cố trong phạm vi tỉnh Lào Cai theo tần suất quy định tại điểm b, nhiệm vụ 4, mục II Điều 1 Quyết định số 1622/QĐ-TTg ngày 25 tháng 10 năm 2017 của Thủ tướng Chính phủ.

c) Sở Thông tin và Truyền thông tham mưu xây dựng, trình UBND tỉnh phê duyệt và hướng dẫn các cơ quan, đơn vị thực hiện kế hoạch ứng phó sự cố cho các hệ thống thông tin trên địa bàn tỉnh theo đề cương tại Phụ lục II Quyết định số 05/2017/QĐ-TTg (bao gồm các điều chỉnh do Bộ Thông tin và Truyền thông ban hành nếu có) và tổ chức triển khai kế hoạch sau khi phê duyệt.

d) Kế hoạch ứng phó sự cố được rà soát và điều chỉnh hàng năm (nếu cần thiết) trước ngày 31 tháng 10, làm cơ sở để xây dựng kế hoạch bảo đảm an toàn, an ninh thông tin năm tiếp theo.

3. 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 trực tiếp quản lý thì thực hiện tiếp Bước 2. Nếu hệ thống có nguy cơ mất an toàn thông tin mạng thuộc các hệ thống được triển khai tập trung tại Trung tâm tích hợp 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. 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 Trưởng Bộ Thông tin và Truyền thông (sau đây viết tắt là Thông tư số 20/2017/TT-BTTTT) và thực hiện tiếp Bước 4.

d) Bước 4: Phối hợp với Sở Thông tin và Truyền thông, Tổ ứng cứu an toàn thông tin mạng của tỉnh 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, 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.

4. Trường hợp có sự cố nghiêm trọng, 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.

Điều 15. Xác định cấp độ và phương án bảo đảm an toàn hệ thống thông tin

1. Chủ quản hệ thống thông tin:

a) UBND tỉnh là chủ quản hệ thống thông tin đối với các hệ thống do UBND tỉnh quyết định đầu tư. UBND tỉnh ủy quyền cho các đơn vị thuộc quản lý trực tiếp các hệ thống do UBND tỉnh làm chủ quản.

b) Các đơn vị trực thuộc UBND tỉnh là chủ quản hệ thống thông tin do đơn vị được cấp có thẩm quyền quyết định đầu tư dự án xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin; là chủ quản hệ thống thông tin do đơn vị được cấp có thẩm quyền phê duyệt đề cương, dự toán chi tiết; quản lý trực tiếp các hệ thống do UBND tỉnh ủy quyền theo quy định tại điểm a khoản này.

c) Chủ quản hệ thống thông tin (hoặc đơn vị được ủy quyền quản lý trực tiếp) thực hiện trách nhiệm theo quy định tại Điều 20 Nghị định số 85/2016/NĐ-CP.

2. Đơn vị vận hành hệ thống thông tin:

a) Giao Sở Thông tin và Truyền thông là đơn vị quản lý, vận hành các hệ thống thông tin, cơ sở dữ liệu dùng chung của tỉnh Lào Cai.

b) Chủ quản hệ thống thông tin khác chịu trách nhiệm phân công đơn vị vận hành hệ thống thông tin.

c) Các hệ thống thông tin trước khi đưa vào khai thác, sử dụng phải được giao cho đơn vị quản lý, vận hành. Đơn vị vận hành hệ thống thông tin theo quy định tại Điều 6 Thông tư số 03/2017/TT-BTTTT.

3. Đơn vị chuyên trách về an toàn thông tin:

a) Sở Thông tin và Truyền thông là đơn vị chuyên trách về an toàn thông tin của tỉnh Lào Cai.

b) Đơn vị chuyên trách về CNTT tại các cơ quan, đơn vị đồng thời là đơn vị chuyên trách về an toàn thông tin.

4. Trình tự, thủ tục xác định cấp độ hệ thống thông tin:

a) Việc xác định, phân loại hệ thống thông tin theo quy định tại Điều 4 Thông tư số 03/2017/TT-BTTTT.

b) Nội dung của hồ sơ đề xuất cấp độ hệ thống thông tin theo quy định tại Điều 15 Nghị định số 85/2016/NĐ-CP.

c) Nội dung, thời gian thẩm định hồ sơ đề xuất cấp độ hệ thống thông tin quy định tại Điều 16 Nghị định số 85/2016/NĐ-CP.

d) Trình tự, thủ tục xác định cấp độ hệ thống thông tin theo quy định tại Điều 13, Điều 14 Nghị định số 85/2016/NĐ-CP và Điều 14, Điều 15, Điều 16 Thông tư số 03/2017/TT-BTTTT.

5. Phương án bảo đảm an toàn hệ thống thông tin:

a) Phương án bảo đảm 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 03/2017/TT-BTTTT, phù hợp với tiêu chuẩn TCVN 11930:2017, các tiêu chuẩn, quy chuẩn kỹ thuật khác và chính sách an toàn thông tin mạng của UBND tỉnh, chính sách an toàn thông tin mạng của các cơ quan, đơn vị (nếu có).

b) Chủ quản hệ thống thông tin hoặc cơ quan, đơn vị được ủy quyền quản lý trực tiếp hệ thống thông tin tổ chức triển khai phương án bảo đảm an toàn hệ thống thông tin sau khi hồ sơ đề xuất cấp độ hoặc phương án bảo đảm an toàn hệ thống được phê duyệt.

c) Đơn vị/bộ phận chuyên trách về an toàn thông tin thuộc cơ quan, đơn vị chịu trách nhiệm giám sát việc triển khai các phương án bảo đảm an toàn thông tin đã được phê duyệt.

Điều 16. Bảo đảm an toàn thông tin khi tiếp nhận, phát triển, vận hành và bảo trì hệ thống thông tin

1. Khi thực hiện nâng cấp, mở rộng, thay thế một phần hệ thống thông tin, phải rà soát cấp độ, phương án bảo đảm an toàn của hệ thống thông tin và thực hiện điều chỉnh, bổ sung hoặc thay mới hồ sơ đề xuất cấp độ trong trường hợp cần thiết.

2. Khi tiếp nhận, phát triển, nâng cấp, bảo trì hệ thống thông tin, đơn vị phải tiến hành phân tích, xác định rủi ro có thể xảy ra, đánh giá phạm vi tác động và phải chuẩn bị các biện pháp hạn chế, loại trừ các rủi ro này và yêu cầu các bên cung cấp, thi công, các cá nhân liên quan thực hiện.

3. Trong quá trình vận hành hệ thống thông tin, đơn vị chủ quản hệ thống thông tin cần thực hiện đánh giá, phân loại hệ thống thông tin theo cấp độ; triển khai phương án bảo đảm an toàn hệ thống thông tin đáp ứng yêu cầu cơ bản trong tiêu chuẩn, quy chuẩn kỹ thuật về bảo đảm an toàn hệ thống thông tin theo cấp độ; thường xuyên kiểm tra, giám sát an toàn hệ thống thông tin; tuân thủ quy trình vận hành, quy trình xử lý sự cố đã xây dựng; ghi lại và lưu trữ đầy đủ thông tin nhật ký hệ thống để phục vụ quản lý, kiểm soát thông tin.

4. Các cơ quan, đơn vị có liên quan đến việc phát triển phần mềm ứng dụng có trách nhiệm yêu cầu các đối tác (nếu có) thực hiện các công tác đảm bảo an toàn thông tin, tránh lộ, lọt mã nguồn và dữ liệu, tài liệu thiết kế, quản trị hệ thống mà đối tác đang xử lý ra bên ngoài.

Điều 17. Giám sát an toàn thông tin mạng

1. Chủ quản hệ thống thông tin và các đơn vị được ủy quyền chủ quản hệ thống thông tin (đối với các hệ thống thông tin do UBND tỉnh là chủ quản) chỉ đạo việc giám sát đối với các hệ thống thông tin thuộc phạm vi quản lý, phối hợp với Sở Thông tin và Truyền thông và các đơn vị chức năng của Bộ Thông tin và Truyền thông giám sát theo quy định.

2. Nguyên tắc, yêu cầu, nội dung, phương thức, hệ thống kỹ thuật phục vụ công tác giám sát thực hiện theo quy định tại Thông tư số 31/2017/TT-BTTTT ngày 15 tháng 11 năm 2017 của Bộ Trưởng Bộ Thông tin và Truyền thông.

3. Đơn vị chuyên trách về an toàn thông tin của các đơn vị trực thuộc cơ quan, đơn vị cử 01 lãnh đạo đơn vị và 01 cán bộ (hoặc 01 đơn vị trực thuộc) làm đầu mối giám sát an toàn thông tin mạng để tiếp nhận cảnh báo, cung cấp, trao đổi, chia sẻ thông tin với Sở Thông tin và Truyền thông trong các hoạt động giám sát an toàn thông tin tại các cơ quan, đơn vị trên địa bàn tỉnh.

Điều 18. Kiểm tra, đánh giá an toàn thông tin

1. Sở Thông tin và Truyền thông thực hiện kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ trên địa bàn tỉnh theo quy định tại Điều 11 Thông tư số 03/2017/TT-BTTTT.

2. Đơn vị chủ trì kiểm tra, đánh giá là đơn vị được cấp có thẩm quyền giao nhiệm vụ hoặc được lựa chọn để thực hiện việc kiểm tra, đánh giá. Đối tượng kiểm tra, đánh giá là chủ quản hệ thống thông tin hoặc đơn vị vận hành hệ thống thông tin và các hệ thống thông tin có liên quan.

3. Nội dung, hình thức kiểm tra, đánh giá theo quy định tại Điều 10 Thông tư số 03/2017/TT-BTTTT.

4. Sở Thông tin và Truyền thông, đơn vị chuyên trách về an toàn thông tin của các đơn vị trực thuộc UBND tỉnh thực hiện việc đánh giá hiệu quả của các biện pháp bảo đảm an toàn thông tin theo thẩm quyền. Nội dung đánh giá là cơ sở để điều chỉnh phương án bảo đảm an toàn thông tin cho phù hợp.

Điều 19. Quản lý hạ tầng kỹ thuật, trang thiết bị CNTT

1. Giao, gắn trách nhiệm cho cá nhân hoặc tập thể quản lý, sử dụng hạ tầng kỹ thuật, trang thiết bị CNTT.

2. Quy định các quy tắc sử dụng, giữ gìn bảo vệ trang thiết bị CNTT trong các trường hợp, như: mang ra khỏi cơ quan, trang thiết bị CNTT liên quan đến dữ liệu nhạy cảm, thông tin cài đặt và cấu hình.

3. Trang thiết bị CNTT có lưu trữ dữ liệu quan trọng 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 CNTT đó.

4. Trang thiết bị CNTT có bộ phận lưu trữ dữ liệu hoặc thiết bị lưu trữ dữ liệu khi mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài hoặc ngừng sử dụng phải tháo bộ phận lưu trữ khỏi thiết bị hoặc xóa thông tin, dữ liệu lưu trữ trên thiết bị (trừ trường hợp để khôi phục dữ liệu).

5. Các cơ quan, đơn vị trực có trách nhiệm bảo dưỡng, bảo quản và vận hành hệ thống hạ tầng kỹ thuật của cơ quan, đơn vị mình; chỉ định bộ phận chuyên trách

về CNTT thực hiện quản lý, vận hành và định kỳ kiểm tra, sửa chữa, bảo trì thiết bị (bao gồm thiết bị đang hoạt động và thiết bị dự phòng).

Chương III
TRÁCH NHIỆM BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Điều 20. Trách nhiệm của Sở Thông tin và Truyền thông

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

2. Thực hiện thẩm định hồ sơ đề xuất cấp độ theo quy định của Nghị định số 85/2016/NĐ-CP và Thông tư số 03/2017/TT-BTTTT.

3. Hàng năm xây dựng kế hoạch, tổng hợp nhu cầu của các cơ quan, đơn vị để triển khai công tác an toàn thông tin mạng trong hoạt động ứng dụng CNTT của cơ quan nhà nước trên địa bàn tỉnh theo quy định.

4. 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.

5. Xây dựng và triển khai các chương trình đào tạo, hội nghị tuyên truyền về an toàn thông tin mạng trong hoạt động ứng dụng CNTT của các cơ quan nhà nước trên địa bàn tỉnh.

6. 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.

7. Hướng dẫn, giám sát các cơ quan, đơn vị trên địa bàn tỉnh xây dựng quy định nội bộ và thực hiện việc bảo đảm an toàn thông tin mạng cho hệ thống thông tin theo quy định của Nhà nước.

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. Tổng hợp và báo cáo về tình hình an toàn thông tin mạng theo định kỳ cho Bộ Thông tin và Truyền thông, UBND tỉnh và các cơ quan, đơn vị có liên quan.

10. Hướng dẫn, hỗ trợ các cơ quan, đơn vị kiểm tra đánh giá mức độ an toàn thông tin mạng cho hệ thống thông tin thuộc thẩm quyền quản lý theo quy định tại Nghị định số 85/2016/NĐ-CP.

Điều 21. 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, đấu tranh, ngăn chặn các loại tội phạm lợi dụng hệ thống thông tin gây phương hại đến an ninh quốc gia, gây mất an ninh trật tự và 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. Điều tra và xử lý các tổ chức, cá nhân vi phạm pháp luật về an toàn thông tin mạng theo thẩm quyền.

4. Kịp thời thông báo, trao đổi với các cơ quan, đơn vị về phương thức, thủ đoạn mới của các loại tội phạm xâm phạm an toàn, an ninh thông tin để có biện pháp phòng ngừa, đấu tranh, ngăn chặn.

Điều 22. Trách nhiệm của Sở Tài chính, Sở Kế hoạch và Đầu tư

Chủ trì, phối hợp với Sở Thông tin và Truyền thông, hàng năm tham mưu với UBND tỉnh trong việc bố trí kinh phí cho các hoạt động đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng CNTT của các cơ quan nhà nước trên địa bàn tỉnh.

Điều 23. Trách nhiệm của các cơ quan, đơn vị

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 UBND 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 chuyên trách bảo đảm an toàn thông tin mạng của đơn vị; tạo điều kiện để các cán bộ phụ trách an toàn thông tin mạng được học tập, nâng cao trình độ về an toàn thông tin mạng; 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. Các cơ quan, đơn vị 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.

5. 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.

6. 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.

7. Định kỳ mỗi 6 tháng các cơ quan, đơn vị lập báo cáo về tình hình an toàn thông tin mạng, gửi về Sở Thông tin và Truyền thông (theo hướng dẫn của Sở Thông tin và Truyền thông).

8. Các cơ quan, đơn vị 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.

9. Các cơ quan, đơn vị 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.

10. Các cơ quan, đơn vị có trách nhiệm quản lý và thu hồi tài khoản, quyền truy cập các hệ thống thông tin và tất cả các tài sản liên quan tới hệ thống thông tin khi cán bộ chuyển công tác, nghỉ việc, nghỉ theo chế độ.

Điều 24. Trách nhiệm của cán bộ, công chức, viên chức và người lao động trong các cơ quan, đơn vị

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

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

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 thủ trưởng 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.

2. Trách nhiệm của cán bộ, công chức, viên chức và người lao động trong các cơ quan, đơn vị:

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 mạng trong phạm vi trách nhiệm và quyền hạn được giao;

b) Khi tham gia vận hành mạng máy tính của cơ quan, đơn vị 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, viên chức và người lao động 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 Internet;

c) Trong trao đổi thông tin, dữ liệu phục vụ công việc, các cơ quan, đơn vị, cán bộ, công chức, viên 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 Lào Cai (@laocai.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, viên chức và người lao động 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 chuyên 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 tập huấn về an toàn thông tin mạng do các cơ quan, đơn vị chuyên trách an toàn thông tin mạng hoặc Sở Thông tin và Truyền thông tổ chức.

3. Khi cán bộ, công chức, viên chức và người lao động chấm dứt hoặc thay đổi công việc, cơ quan, đơn vị phải:

a) Xác định rõ trách nhiệm của cán bộ, nhân viên và các bên liên quan trong quản lý, sử dụng các tài sản CNTT được giao.

b) Lập biên bản bàn giao tài sản CNTT.

c) Thay đổi hoặc thu hồi tài khoản, quyền truy cập các hệ thống thông tin và các ứng dụng CNTT.

Điều 25. Trách nhiệm của các tổ chức, cá nhân khác

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

Chương IV
ĐIỀU KHOẢN THI HÀNH

Điều 26. Khen thưởng và xử lý vi phạm

1. Hàng năm, Sở Thông tin và Truyền thông căn cứ kết quả kiểm tra, đánh giá, báo cáo công tác bảo đảm an toàn thông tin mạng của các cơ quan, đơn vị đề xuất UBND tỉnh xem xét khen thưởng cho các cá nhân, đơn vị có nhiều thành tích trong công tác bảo đảm an toàn thông tin mạng theo quy định hiện hành.

2. Tổ chức, cá nhân có hành vi vi phạm quy chế này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý theo quy định hiện hành.

Điều 27. Tổ chức thực hiện

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