

QUYẾT ĐỊNH

**Về việc ban hành Kế hoạch ứng phó sự cố an toàn thông tin mạng
trên địa bàn tỉnh Cao Bằng năm 2021**

CHỦ TỊCH ỦY BAN NHÂN DÂN TỈNH CAO BẰNG

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

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

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 cơ quan Nhà nước;

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

Căn cứ Quyết định số 1017/QĐ-TTg ngày 14 tháng 8 năm 2018 của Thủ tướng Chính phủ Phê duyệt đề án giám sát an toàn thông tin mạng đối với hệ thống, dịch vụ công nghệ thông tin phục vụ Chính phủ điện tử đến năm 2020, định hướng đến năm 2025;

Căn cứ Chỉ thị số 14/CT-TTg ngày 25 tháng 5 năm 2018 của Thủ tướng Chính phủ về việc nâng cao năng lực phòng, chống phần mềm độc hại;

Căn cứ Chỉ thị số 14/CT-TTg ngày 07 tháng 6 năm 2019 của Thủ tướng Chính phủ về tăng cường đảm bảo an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam;

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 thông tin theo cấp độ;

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

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Kế hoạch ứng phó sự cố an toàn thông tin mạng trên địa bàn tỉnh Cao Bằng năm 2021.

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

Điều 3. Chánh Văn phòng Ủy ban nhân dân tỉnh; Thủ trưởng các sở, ban, ngành; Chủ tịch Ủy ban nhân dân các huyện, thành phố; Thủ trưởng các cơ quan đơn vị liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:

- Như Điều 3;
- Bộ Thông tin và Truyền thông;
- Chủ tịch, các PCT UBND tỉnh;
- Thành viên BCĐ xây dựng CQĐT tỉnh;
- VP UBND tỉnh: LĐVP, TTTT;
- Các doanh nghiệp Viễn thông – CNTT;
- Lưu: VT, VX. *h*

**KT. CHỦ TỊCH
PHÓ CHỦ TỊCH**



[Handwritten signature]
Lê Hải Hòa

KẾ HOẠCH

Ứng phó sự cố an toàn thông tin mạng trên địa bàn tỉnh Cao Bằng năm 2021
(Ban hành kèm theo Quyết định số 1519/QĐ-UBND ngày 18 tháng 8 năm 2020
của Chủ tịch Ủy ban nhân dân tỉnh)

I. CĂN CỨ XÂY DỰNG KẾ HOẠCH

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

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

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01/07/2016 của Chính phủ về bảo đảm an toàn thông tin theo cấp độ;

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16/03/2017 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 Quyết định số 1017/QĐ-TTg ngày 14/8/2018 của Thủ tướng Chính phủ Phê duyệt đề án giám sát an toàn thông tin mạng đối với hệ thống, dịch vụ công nghệ thông tin phục vụ Chính phủ điện tử đến năm 2020, định hướng đến năm 2025;

Căn cứ Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ về việc nâng cao năng lực phòng, chống phần mềm độc hại;

Căn cứ Chỉ thị số 14/CT-TTg ngày 07/6/2019 của Thủ tướng Chính phủ về tăng cường đảm bảo an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam;

Căn cứ Thông tư số 03/2017/TT-BTTTT ngày 24/04/2017 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 thông tin theo cấp độ.

II. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Bảo đảm an toàn thông tin cho các hệ thống thông tin dùng chung của tỉnh; có khả năng thích ứng một cách chủ động, linh hoạt và giảm thiểu các nguy cơ, đe dọa mất an toàn thông tin trên mạng; ngăn ngừa phát sinh các sự cố mất an toàn thông tin mạng trên địa bàn tỉnh.

- Đánh giá được hiệu quả các giải pháp bảo đảm an toàn thông tin, kịp thời điều chỉnh phương án phòng chống phù hợp với yêu cầu thực tiễn.

- Đạt được mô hình đảm bảo an toàn thông tin trong cơ quan nhà nước tỉnh theo mô hình “4 lớp”.

- Bảo đảm hoạt động, nâng cao kỹ năng, tính sẵn sàng của Đội Ứng cứu sự cố an toàn thông tin mạng của tỉnh.

- Nâng cao nhận thức, kỹ năng về bảo đảm an toàn thông tin mạng trong cán bộ công chức và toàn xã hội.

2. Yêu cầu

Triển khai, tổ chức thực hiện đầy đủ, hiệu quả các quy định về bảo đảm an toàn thông tin mạng tại các văn bản của Chính phủ, Thủ tướng Chính phủ, Bộ Thông tin và Truyền thông, bao gồm:

- Quyết định số 05/2017/QĐ-TTg ngày 16/03/2017 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.

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

- Thông tư số 03/2017/TT-BTTTT ngày 24/04/2017 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.

- Quyết định số 1017/QĐ-TTg ngày 14/8/2018 của Thủ tướng Chính phủ Phê duyệt đề án giám sát an toàn thông tin mạng đối với hệ thống, dịch vụ công nghệ thông tin phục vụ Chính phủ điện tử đến năm 2020, định hướng đến năm 2025;

- Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ về việc nâng cao năng lực phòng, chống phần mềm độc hại; Chỉ thị số 14/CT-TTg ngày 07/6/2019 của Thủ tướng Chính phủ về tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam.

III. NỘI DUNG THỰC HIỆN

1. Tổ chức nghiên cứu, xây dựng các kịch bản tấn công, các nguy cơ, tình huống sự cố có khả năng xảy ra, từ đó đề ra các phương án ứng cứu, đối phó, ngăn chặn

Tổ chức nghiên cứu, xây dựng các tình huống, kịch bản tấn công, các nguy cơ, sự cố cụ thể có khả năng xảy ra đối với các hệ thống thông tin hiện có của tỉnh. Trên cơ sở đó, xây dựng phương án đối phó, ứng cứu, khắc phục sự cố tương ứng.

2. Triển khai các giải pháp giám sát an toàn thông tin mạng, phát hiện, cảnh báo sớm, kiểm tra, rà quét, đánh giá an toàn thông tin; phòng, chống mã độc cho các hệ thống của tỉnh

a) Triển khai bảo đảm an toàn thông tin cho hệ thống thông tin tỉnh theo mô hình “4 lớp”:

- “Lớp 1” Lực lượng tại chỗ: Kiện toàn Đội ứng cứu sự cố an toàn thông tin mạng; tham mưu, tổ chức, thực thi và kiểm tra, đôn đốc thực hiện các quy định của pháp luật về đảm bảo an toàn, an ninh mạng.

- “Lớp 2” Tổ chức hoặc thuê doanh nghiệp giám sát, bảo vệ chuyên nghiệp: Tự thực hiện giám sát, ứng cứu sự cố an toàn thông tin mạng, bảo vệ hệ thống thông tin thuộc quyền quản lý hoặc thuê tổ chức, doanh nghiệp có đủ năng lực để thực hiện cung cấp dịch vụ giám sát an toàn thông tin và thực hiện thường xuyên công tác giám sát an toàn thông tin cho các hệ thống của tỉnh, phát hiện sớm nguy cơ, sự cố.

- “Lớp 3” Tổ chức hoặc thuê doanh nghiệp độc lập với tổ chức, doanh nghiệp giám sát, bảo vệ để định kỳ kiểm tra, đánh giá an toàn thông tin mạng đối với hệ thống thông tin mạng cấp 3 trở lên của tỉnh hoặc kiểm tra, đánh giá đột xuất báo cáo Bộ Thông tin và Truyền thông theo quy định của pháp luật.

- “Lớp 4” Kết nối, chia sẻ thông tin với Trung tâm Giám sát an toàn không gian mạng quốc gia trực thuộc Cục An toàn thông tin, Bộ Thông tin và Truyền thông, cung cấp các dải địa chỉ IP Public của các hệ thống thông tin trong cơ quan, tổ chức nhà nước trên địa bàn tỉnh.

b) Kiểm tra, đánh giá an toàn thông tin các hệ thống thông tin; rà quét, phân tích, xử lý, bóc gỡ mã độc.

c) Duy trì bản quyền phần mềm và mở rộng Hệ thống phòng, chống mã độc mô hình quản trị tập trung cho các hệ thống thông tin và máy tính cá nhân có kết nối mạng nội bộ và mạng Internet, đáp ứng các mục tiêu theo Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ về nâng cao năng lực phòng chống phần mềm độc hại.

3. Tổ chức huấn luyện, diễn tập các phương án đối phó, ứng cứu sự cố

a) Trên cơ sở các kịch bản tấn công, các nguy cơ, tình huống sự cố có khả năng xảy ra xây dựng kịch bản diễn tập ở quy mô cấp tỉnh; tiến hành tổ chức diễn tập với lực lượng nòng cốt là Đội Ứng cứu xử lý sự cố an toàn thông tin mạng của tỉnh, phối hợp với các cơ quan, đơn vị, doanh nghiệp trong tỉnh.

b) Cử lực lượng tham gia huấn luyện, diễn tập vùng, miền, quốc gia, quốc tế.

4. Bảo đảm lực lượng, điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố

a) Mua sắm, nâng cấp, gia hạn bản quyền trang thiết bị, phần mềm, công cụ, phương tiện phục vụ ứng cứu, khắc phục sự cố.

b) Chuẩn bị các điều kiện bảo đảm, dự phòng nhân lực, vật lực, tài chính để sẵn sàng đối phó, ứng cứu, khắc phục khi sự cố xảy ra.

c) Xây dựng, ban hành quy chế tổ chức hoạt động của Đội Ứng cứu xử lý sự cố an toàn thông tin mạng của tỉnh.

d) Tổ chức tập huấn nâng cao kỹ năng, kiến thức về an toàn thông tin cho đội ngũ nhân lực phụ trách công tác an toàn thông tin các cơ quan trong tỉnh; Tham gia các khóa tập huấn, bồi dưỡng do Bộ Thông tin và Truyền thông và Cụm thành viên mạng lưới ứng cứu sự cố số 1 triển khai.

đ) Tham gia các hoạt động của Mạng lưới ứng cứu sự cố an toàn thông tin mạng khu vực và quốc gia.

5. Triển khai các hoạt động nghiệp vụ đặc thù bảo đảm an toàn thông tin mạng cho các hệ thống thông tin thuộc phạm vi quản lý

a) Xác định hệ thống thông tin và cấp độ an toàn hệ thống thông tin:

Xác định hệ thống thông tin và cấp độ an toàn hệ thống thông tin cho các hệ thống thông tin của cơ quan nhà nước trên địa bàn tỉnh theo quy định tại Nghị định 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

b) Triển khai hoạt động thường trực, điều phối, xử lý, ứng cứu sự cố:

Triển khai các hoạt động thuộc trách nhiệm của các cơ quan, đơn vị liên quan theo quy định tại Điều 11, Điều 12, Điều 13, Điều 14 và các nội dung liên quan khác tại Quyết định số 05/2017/QĐ-TTg ngày 16/03/2017 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.

6. Tuyên truyền, nâng cao nhận thức về công tác an toàn thông tin mạng

a) Tổ chức Hội nghị phổ biến kiến thức, nâng cao nhận thức về an toàn thông tin cho cán bộ, công chức, viên chức trong các cơ quan nhà nước.

b) Tuyên truyền trên các phương tiện truyền thông, mạng xã hội các nguy cơ, rủi ro, giải pháp phòng chống về mất an toàn thông tin, các quy định của pháp luật về an toàn và an ninh thông tin.

V. GIẢI PHÁP VÀ KINH PHÍ THỰC HIỆN

1. Giải pháp thực hiện Kế hoạch

- Bám sát các nội dung quy định tại các văn bản quy định về bảo đảm an toàn thông tin mạng làm cơ sở triển khai các thực hiện các nhiệm vụ của Kế hoạch.

- Xác định nhiệm vụ đảm bảo an toàn thông tin cho các hệ thống thông tin của cơ quan nhà nước tỉnh là nhiệm vụ thường xuyên, liên tục.

- Phân tích, đánh giá các nguy cơ, các tình huống sự cố có nhiều khả năng gây ảnh hưởng nhất đối với hệ thống thông tin theo thứ tự ưu tiên từ cao xuống thấp, từ đó lựa chọn tổ chức huấn luyện, diễn tập ứng cứu, đối phó, ngăn chặn sự cố an toàn thông tin đối với từng tình huống cụ thể theo thứ tự ưu tiên, tình huống có khả năng gây ảnh hưởng cao hơn sẽ được tổ chức huấn luyện, diễn tập trước.

- Thiết lập cơ chế phối hợp điều hành giữa các cơ quan, đơn vị, địa phương để triển khai công tác ứng phó sự cố an toàn thông tin mạng trên phạm vi toàn tỉnh.

2. Nguồn lực và điều kiện đảm bảo thực hiện kế hoạch

- Ưu tiên bố trí các nguồn lực (nhân lực, vật lực) để thực hiện kế hoạch, dành một phần kinh phí nhất định để triển khai nhiệm vụ ứng cứu sự cố, an toàn thông tin mạng.

- Quan tâm phát triển nguồn nhân lực chuyên môn về an toàn thông tin phục vụ công tác đảm bảo an toàn thông tin của tỉnh.

- Tổ chức tham vấn chuyên gia về an toàn thông tin mạng nhằm hỗ trợ, tư vấn, đề xuất cho tỉnh xây dựng các phương án ứng cứu, đối phó, ngăn chặn sự cố an toàn thông tin.

3. Kinh phí và nguồn vốn triển khai kế hoạch

Kinh phí thực hiện Kế hoạch Ứng phó sự cố an toàn thông tin mạng trên địa bàn tỉnh Cao Bằng năm 2021 do ngân sách nhà nước đảm bảo và được cân đối trong dự toán được cấp có thẩm quyền giao cho các đơn vị để triển khai thực hiện.

VI. TỔ CHỨC THỰC HIỆN

1. Sở Thông tin và Truyền thông

- Chủ trì, phối hợp với các cơ quan, đơn vị liên quan tham mưu UBND tỉnh thực hiện các nhiệm vụ kế hoạch.

- Chủ trì lập dự toán kinh phí thực hiện các nhiệm vụ, trình cấp có thẩm quyền thẩm định, phê duyệt.

- Thực hiện nhiệm vụ đơn vị chuyên trách ứng cứu sự cố an toàn thông tin mạng của tỉnh, làm cơ quan đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin mạng trên địa bàn tỉnh.

- Chủ trì, phối hợp với các cơ quan, đơn vị tổ chức kiểm tra công tác bảo đảm an toàn thông tin mạng đối với các cơ quan nhà nước trong tỉnh.

- Thẩm định, phê duyệt hoặc cho ý kiến về mặt chuyên môn đối với hồ sơ đề xuất cấp độ an toàn hệ thống thông tin theo thẩm quyền quy định tại khoản 1, khoản 2 Điều 12 và khoản 5 Điều 15 Nghị định số 85/2016/NĐ-CP của Chính phủ và theo hướng dẫn tại Thông tư số 03/2017/TT-BTTTT của Bộ trưởng Bộ Thông tin và Truyền thông.

2. Sở Tài chính

Trên cơ sở danh mục nhiệm vụ thuộc Kế hoạch này và dự toán kinh phí do Sở Thông tin và Truyền thông đề xuất, tổ chức thẩm định dự toán, tham mưu UBND tỉnh bố trí kinh phí để triển khai thực hiện.

3. Các sở, ban, ngành; Ủy ban nhân dân các huyện, thành phố

- Tổ chức triển khai các giải pháp bảo đảm an toàn thông tin; xây dựng thành một nội dung thực hiện trong Kế hoạch Ứng dụng công nghệ thông tin hàng năm của cơ quan, đơn vị.

- Bố trí cán bộ, công chức phụ trách về an toàn thông tin mạng tại cơ quan, địa phương.

- Cử cán bộ tham gia các khóa đào tạo, tập huấn đảm bảo an toàn thông tin mạng đúng đối tượng, thành phần triệu tập.

- Phối hợp với Sở Thông tin và Truyền thông và các đơn vị liên quan thực hiện công tác ứng phó sự cố an toàn thông tin mạng.

4. Các doanh nghiệp cung cấp dịch vụ kết nối mạng

Bảo đảm hạ tầng mạng ổn định, thông suốt phục vụ các hệ thống thông tin của cơ quan nhà nước trên địa bàn tỉnh; có giải pháp phát hiện và ngăn chặn, xử lý kịp thời các nguy cơ gây mất an toàn thông tin.

Trong quá trình thực hiện nếu phát sinh khó khăn, vướng mắc, các cơ quan, địa phương kịp thời phản ánh về Ủy ban nhân dân tỉnh (qua Sở Thông tin và Truyền thông) để tổng hợp, xem xét, chỉ đạo./.

**KT. CHỦ TỊCH
PHÓ CHỦ TỊCH**



Lê Hải Hòa



Phụ lục

DANH MỤC NHIỆM VỤ ỨNG PHÓ SỰ CỐ AN TOÀN THÔNG TIN MẠNG TRÊN ĐỊA BÀN TỈNH CAO BẰNG NĂM 2021

(Kèm theo Quyết định số 1519/QĐ-UBND ngày 18 tháng 8 năm 2020 của Chủ tịch Ủy ban nhân dân tỉnh)

STT	Tên nhiệm vụ	Cơ quan chủ trì	Cơ quan phối hợp	Thời gian
1	Xây dựng phương án đối phó, ứng cứu, khắc phục sự cố đối với các tình huống tấn công mạng	Sở Thông tin và Truyền thông	Các cơ quan, đơn vị liên quan; Đội ứng phó sự cố an toàn thông tin mạng của tỉnh.	Trong năm
2	Triển khai Hệ thống giám sát An toàn thông tin (SOC) mô hình “4 lớp” tỉnh Cao Bằng	Sở Thông tin và Truyền thông	Các cơ quan, đơn vị liên quan	Trong năm
3	Kiểm tra, đánh giá an toàn thông tin các hệ thống thông tin; rà quét, phân tích, xử lý, bóc gỡ mã độc	Sở Thông tin và Truyền thông	Các cơ quan, đơn vị liên quan	Thường xuyên
4	Bổ sung thiết bị phục vụ cho hoạt động của đội ứng cứu sự cố an toàn thông tin mạng (Máy chủ, máy tính xách tay cấu hình cao, máy chiếu)	Sở Thông tin và Truyền thông	Các cơ quan, đơn vị liên quan	Trong năm
5	Duy trì Bản quyền Phần mềm Endpoint Detection & Response cho hệ thống máy trạm, máy chủ năm 2021	Sở Thông tin và Truyền thông	Các cơ quan, đơn vị liên quan	Quý II
6	Mở rộng cài đặt máy trạm kết nối với hệ thống phòng chống mã độc tập trung EDR	Sở Thông tin và Truyền thông	Các cơ quan, đơn vị liên quan	Quý III
7	Tổ chức diễn tập toàn tỉnh về bảo đảm an toàn thông tin	Sở Thông tin và Truyền thông	Các cơ quan, đơn vị liên quan; Đội ứng phó sự cố an toàn thông tin mạng của tỉnh.	Quý II
8	Tham gia các hoạt động an toàn thông tin theo chỉ đạo của Bộ TTTT; Cụm thành viên mạng lưới ứng cứu sự	Sở Thông tin và Truyền thông	Bộ Thông tin và Truyền thông; Trưởng cụm thành viên	Trong năm

STT	Tên nhiệm vụ	Cơ quan chủ trì	Cơ quan phối hợp	Thời gian
	cố số 1 theo qui định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc.	thông	mạng lưới ứng cứu sự cố số 1	
9	Tập huấn, bồi dưỡng về an toàn thông tin	Sở Thông tin và Truyền thông	Các cơ quan, đơn vị liên quan	Quý III, IV năm 2021
10	Xác định cấp độ an toàn hệ thống thông tin cho các hệ thống thông tin của cơ quan nhà nước	Sở Thông tin và Truyền thông	Các cơ quan, đơn vị liên quan	Thường xuyên
11	Hội nghị phổ biến kiến thức, nâng cao nhận thức về an toàn thông tin	Sở Thông tin và Truyền thông	Các cơ quan, đơn vị liên quan	Quý IV năm 2021