ỦY BAN NHÂN DÂN TỈNH CAO BẰNG	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 2840/KH-UBND	*Cao Bằng, ngày 02 tháng 11 năm 2022*

KẾ HOẠCH
Ứng phó sự cố an toàn thông tin mạng trên địa bàn tỉnh Cao Bằng năm 2023

I. CĂN CỨ BAN HÀNH KẾ HOẠCH

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

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;

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;

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

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;

Quyết định số 1907/QĐ-TTg ngày 23 tháng 11 năm 2020 của Thủ tướng Chính phủ Phê duyệt đề án Đề án "Tuyên truyền, nâng cao nhận thức và phổ biến kiến thức về an toàn thông tin giai đoạn 2021 - 2025";

Quyết định số 21/QĐ-TTg ngày 06 tháng 01 năm 2021 của Thủ tướng Chính phủ về Phê duyệt Đề án "Đào tạo và phát triển nguồn nhân lực an toàn thông tin giai đoạn 2021 - 2025";

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;

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;

Chỉ thị số 18/CT-TTg ngày 13 tháng 10 năm 2022 của Thủ tướng Chính phủ về đẩy mạnh triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng Việt Nam;

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;

Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 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 01/7/2016 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 và hệ thống thông tin của các cơ quan nhà nước, đảm bảo 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; chủ động phòng ngừa, ngăn chặn và đề ra các giải pháp ứng phó khi xảy ra sự cố mất an toàn thông tin mạng trên địa bàn tỉnh.

- Đảm bảo các nguồn lực và các điều kiện cần thiết để sẵn sàng triển khai kịp thời, hiệu quả các phương án ứng cứu khẩn cấp sự cố an toàn thông tin mạng.

- Nâng cao kỹ năng, hoạt động và 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 cho cán bộ, công chức, viên chức cơ quan nhà nước và người dân.

- Kiểm tra, đánh giá được hiệu quả các chính sách, phương án bảo đảm an toàn thông tin đối với các hệ thống thông tin được phê duyệt cấp độ an toàn hệ thống thông tin, kịp thời điều chỉnh phương án phòng chống phù hợp với cấp độ tương ứng.

2. Yêu cầu

- Triển khai, tổ chức thực hiện đầy đủ, hiệu quả các quy định về bảo đảm an toàn thông tin theo tinh thần chỉ đạo của Chính phủ, Thủ tướng Chính phủ, hướng dẫn của Bộ Thông tin và Truyền thông.

- Các nhiệm vụ thuộc Kế hoạch cần được triển khai thực hiện nghiêm túc, phát huy vai trò của Đội Ứng cứu sự cố an toàn thông tin mạng của tỉnh, có sự tham gia, phối hợp, hỗ trợ của các cơ quan, đơn vị liên quan.

- Chuyển đổi nhận thức, xác định thông tin và dữ liệu là tài sản quan trọng; việc thiết lập, khai thác, sử dụng thông tin, dữ liệu số cần bảo đảm an toàn thông tin trong quá trình chuyển đổi số, phát triển chính quyền số, kinh tế số và xã hội số.

- Các hệ thống thông tin thuộc quyền quản lý được triển khai đầy đủ phương án đảm bảo an toàn thông tin theo cấp độ.

III. NỘI DUNG VÀ GIẢI PHÁP 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 kịch bản tấn công, các nguy cơ, tình huống sự cố có khả năng xảy ra (lỗi hệ thống, thiết bị, phần mềm, hạ tầng hoặc

các tình huống liên quan đến các thảm họa tự nhiên như bão, lũ lụt, hỏa hoạn...) đối với các hệ thống thông tin của tỉnh. Từ đó, xây dựng phương án về nguồn lực, trang thiết bị, kinh phí để thực hiện đối phó, ứng cứu, khắc phục sự cố đối với tình huống sự cố cụ thể;

- Đồng thời quan tâm công tác tổ chức, điều hành, phối hợp với các lực lượng, các tổ chức về đảm bảo an toàn thông tin trong việc đối phó, ngăn chặn, ứng cứu, khắc phục sự cố.

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

- Tuyên truyền, phổ biến, nâng cao nhận thức về an toàn thông tin trong chuyển đổi số cho cán bộ, công chức, viên chức và người dân, doanh nghiệp trên địa bàn tỉnh bằng nhiều hình thức.

- Tập huấn, nâng cao kiến thức, kỹ năng kỹ thuật an toàn thông tin cho đội ngũ nhân lực kỹ thuật an toàn thông tin và công nghệ thông tin của các đơn vị và thành viên Đội ứng cứu sự cố an toàn thông tin mạng tỉnh bằng các hình thức phù hợp thực tiễn.

- Tổ chức Hội thảo, bồi dưỡng, nâng cao nhận thức an toàn thông tin cho lãnh đạo cơ quan nhà nước trên địa bàn tỉnh.

3. 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

3.1. 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 số 85/2016/NĐ-CP của Chính phủ, Thông tư số 12/2022/TT-BTTTT của Bộ trưởng Bộ Thông tin và Truyền thông và Kế hoạch số 1020/KH-UBND ngày 05/5/2021 của UBND tỉnh về xác định cấp độ an toàn hệ thống thông tin cho các hệ thống thông tin trong cơ quan nhà nước tỉnh Cao Bằng.

3.2. Kiểm tra, đánh giá an toàn thông tin

Thực hiện nội dung kiểm tra, đánh giá an toàn thông tin các hệ thống thông tin được phê duyệt cấp độ theo quy định tại Chương IV Thông tư số 12/2022/TT-BTTTT; tần suất kiểm tra, đánh giá định kỳ được quy định tại điểm c khoản 2 Điều 20 Nghị định số 85/2016/NĐ-CP[1] và điểm b khoản 1 Chỉ thị số 18/CT-TTg[2], cụ thể:

- Kiểm tra, đánh giá việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ.

- Kiểm tra, đánh giá hiệu quả của các biện pháp bảo đảm an toàn thông tin theo phương án bảo đảm an toàn thông tin được phê duyệt.

---

[1] Định kỳ 02 năm đối với hệ thống cấp độ 1, 2; Hàng năm đối với hệ thống cấp độ 3, 4; 06 tháng đối với hệ thống cấp độ 5; Hoặc đột xuất, theo yêu cầu của các cơ quan chức năng có thẩm quyền.

[2] Rà quét lỗ hổng trên các hệ thống thông tin trong phạm vi quản lý tối thiểu 01 lần/6 tháng.

- Kiểm tra, đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống thông tin.

- Kiểm tra việc xây dựng, ban hành Quy chế bảo đảm an toàn hệ thống thông tin cho hệ thống thuộc quyền quản lý, vận hành đáp ứng các yêu cầu an toàn về quản lý theo cấp độ an toàn hệ thống thông tin tương ứng và được cấp có thẩm quyền phê duyệt theo quy định Thông tư số 12/2022/TT-BTTTT.

3.3. 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 các Điều 11, Điều 12, Điều 13, Điều 14 và các nội dung liên quan khác tại Quyết định 05/2017/QĐ-TTg của Thủ tướng chính phủ.

4. Triển khai, áp dụng, sử dụng 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 thông tin của tỉnh

4.1. Triển khai, duy trì 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" Thuê 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" Thuê doanh nghiệp độc lập, đánh giá an toàn thông tin mạng đối với hệ thống thông tin mạng cấp 3 trở lên của tỉnh, kiểm tra, đánh giá báo cáo Bộ Thông tin và Truyền thông đúng quy định;

- "Lớp 4" Kết nối, chia sẻ thông tin với Trung tâm Giám sát an toàn không gian mạng quốc gia - 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.

4.2. Quản lý, triển khai hoạt động có hiệu quả hệ thống giám sát an toàn thông tin (SOC) tỉnh.

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

- Trên cơ sở các kịch bản tấn công, lựa chọn các nguy cơ, tình huống sự cố có khả năng xảy ra xây dựng kịch bản diễn tập ở quy mô cấp tỉnh, cấp đơn vị. Tiến hành tổ chức diễn tập thực chiến với lực lượng nòng cốt là Đội Ứng cứu xử lý sự cố an toàn thông tin mạng của tỉnh/Bộ phận chuyên trách về an toàn thông tin của đơn vị và các cơ quan, đơn vị, doanh nghiệp trong tỉnh.

- Cử lực lượng tham gia huấn luyện, diễn tập vùng, miền, quốc gia, quốc tế theo hướng dẫn, chỉ đạo của Đơn vị ứng phó sự cố quốc gia (Trung tâm ứng

cứu khẩn cấp không gian mạng Việt Nam - VNCERT, Cục An toàn thông tin, Bộ Thông tin và Truyền thông).

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

- 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.

- 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.

- Kiện toàn Đội ứng cứu sự cố theo hướng chuyên nghiệp, cơ động, có tối thiểu 05 chuyên gia an toàn thông tin mạng (bao gồm cả thuê chuyên gia ngoài và nhân lực có sẵn trong tỉnh nếu có) đáp ứng chuẩn kỹ năng về an toàn thông tin do Bộ Thông tin và Truyền thông quy định; 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.

- 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.

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

7. Giải pháp thực hiện kế hoạch

- Bám sát các nội dung quy định tại Quyết định số 05/2017/QĐ-TTg, Quyết định số 1907/QĐ-TTg, Quyết định số 1907/QĐ-TTg, Chỉ thị số 14/CT-TTg, Chỉ thị số 18/CT-TTg và các văn bản khác 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 quan trọng, thực hiện 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.

- Tuyên truyền, phổ biến, nâng cao nhận thức, trách nhiệm và các kỹ năng cơ bản bảo đảm an toàn thông tin trên không gian mạng qua các phương tiện thông tin đại chúng, truyền thông xã hội, các hệ thống thông tin cơ sở, trong trường học, người cao tuổi và thanh thiếu niên.

IV. KINH PHÍ THỰC HIỆN

1. 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, giải pháp đối phó, ngăn chặn sự cố an toàn thông tin.

2. Kinh phí thực hiện

Kinh phí thực hiện Kế hoạch Ứng phó sự cố an toàn thông tin mạng trên địa bàn tỉnh Cao Bằng năm 2023 do ngân sách nhà nước đảm bảo, được tổng hợp trong danh mục Kế hoạch phát triển Chính quyền số và đảm bảo an toàn thông tin mạng tỉnh Cao Bằng năm 2023.

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 chỉ đạo, đôn đốc, theo dõi các cơ quan, đơn vị triển khai thực hiện các nhiệm vụ kế hoạch.

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

- Chỉ đạo, giao nhiệm vụ đơn vị chuyên môn 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; phương án đảm bảo an toàn thông tin của các Hệ thống thông tin được phê duyệt đảm bảo an toàn thông tin theo cấp độ.

- 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 và hướng dẫn tại Thông tư số 12/2022/TT-BTTTT của Bộ trưởng Bộ Thông tin và Truyền thông.

- Có trách nhiệm theo dõi, đôn đốc các đơn vị thực hiện Kế hoạch này.

2. Sở Tài chính

Phối hợp với các Sở, Ban ngành liên quan căn cứ khả năng ngân sách tham mưu cho UBND tỉnh cân đối kinh phí thường xuyên để triển khai thực

hiện các nhiệm vụ tại kế hoạch theo quy định hiện hành.

3. Công an tỉnh, các Sở, Ban ngành, UBND các huyện, thành phố

- Tổ chức triển khai các giải pháp bảo đảm an toàn thông tin, lồng ghép thành một nội dung trong Kế hoạch Ứng dụng công nghệ thông tin, phát triển chính quyền số, chuyển đổi số và đảm bảo an toàn 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.

- Tích cực tuyên truyền, phổ biến, nâng cao nhận thức về an toàn thông tin trong chuyển đổi số cho cán bộ, công chức, viên chức và người dân trên địa bàn.

- Nghiêm túc thực hiện rà soát, phát hiện và khắc phục các lỗ hổng, điểm yếu theo cảnh báo của cơ quan chức năng; chủ động theo dõi, phát hiện sớm các nguy cơ mất an toàn thông tin mạng để kịp thời xử lý, khắc phục.

- Chủ động rà soát tất cả các hệ thống thông tin thuộc trách nhiệm quản lý đảm bảo an toàn thông tin theo cấp độ được quy định tại Nghị định số 85/2016/NĐ-CP, Thông tư số 12/2022/TT-BTTTT của Bộ trưởng Bộ Thông tin và Truyền thông, Kế hoạch số 1020/KH-UBND của UBND tỉnh và hướng dẫn của Sở Thông tin và Truyền thông.

- 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.

- Các cơ quan, đơn vị theo chức năng, nhiệm vụ, quyền hạn trong 11 lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng *(theo Quyết định số 632/QĐ-TTg ngày 10/5/2017 của Thủ tướng Chính phủ)* thực hiện công tác đảm bảo an toàn thông tin theo quy định, chú trọng hoạt động chia sẻ thông tin về các nguy cơ, sự cố mất an toàn thông tin mạng cho các cơ quan, tổ chức, doanh nghiệp quản lý, vận hành hệ thống thông tin thuộc lĩnh vực và phục vụ kịp thời, hiệu quả cho Đội ứng cứu sự cố của từng lĩnh vực (CERT lĩnh vực) *(được Quy định tại Chỉ thị số 18/CT-TTg và phạm vi quản lý được quy định tại Chương IV Nghị định số 85/2016/NĐ-CP)*.

4. Các doanh nghiệp cung cấp dịch vụ viễn thông, công nghệ thông tin cho cơ quan nhà nước tỉnh

- 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.

- Có trách nhiệm triển khai các giải pháp đảm bảo an toàn hệ thống thông tin theo cấp độ; xây dựng, cập nhật, bổ sung chính sách, quy trình quản lý, vận hành hoạt động của hệ thống; triển khai nâng cấp, cấu hình hệ thống đáp ứng yêu cầu an toàn thông tin theo cấp độ đối với các Hệ thống thông tin

được xác định là đơn vị vận hành hệ thống theo quy định tại Nghị định số 85/2016/NĐ-CP, Thông tư số 12/2022/TT-BTTTT của Bộ trưởng Bộ Thông tin và Truyền thông.

Trên đây là Kế hoạch Ứng phó sự cố an toàn thông tin mạng trên địa bàn tỉnh Cao Bằng năm 2023. Trong quá trình thực hiện, nếu phát sinh khó khăn, vướng mắc, các cơ quan, địa phương kịp thời phản ánh về UBND tỉnh (qua Sở Thông tin và Truyền thông) để tổng hợp, xem xét chỉ đạo./.

Nơi nhận:
- Bộ Thông tin và Truyền thông;
- Chủ tịch, các PCT UBND tỉnh;
- Các Sở, Ban ngành;
- UBND các huyện, thành phố;
- Thành viên BCĐ CĐS tỉnh;
- Các doanh nghiệp VT-CNTT: VNPT Cao Bằng, Viettel Cao Bằng;
- Lưu: VT, VX(M).

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

ỦY BAN NHÂN DÂN TỈNH CAO BẰNG

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 2023

(Ban hành kèm theo Kế hoạch số 2840 /KH-UBND ngày 02 tháng 11 năm 2022 của Ủy ban nhân dân tỉnh)

STT	Tên nhiệm vụ	Cơ quan chủ trì	Cơ quan phối hợp	Thời gian
1	Xây dựng phương án ứng cứu, khắc phục sự cố đối với các tình huống tấn công mạng.	Các đơn vị quản lý, vận hành hệ thống thông tin của tỉnh	Sở Thông tin và Truyền thông; đơn vị cung cấp dịch vụ (trường hợp thuê dịch vụ) và các đơn vị liên quan	Quý I
2	Tuyên truyền, phổ biến, nâng cao nhận thức về an toàn thông tin trong chuyển đổi số cho cán bộ, công chức, viên chức và người dân, doanh nghiệp trên địa bàn tỉnh	Sở Thông tin và Truyền thông	Các cơ quan, đơn vị liên quan	Thường xuyên
3	Tập huấn, bồi dưỡng về an toàn thông tin.	Sở Thông tin và Truyền thông	Các cơ quan, đơn vị liên quan	Quý III; Quý IV
4	Hội thảo, bồi dưỡng an toàn thông tin cho lãnh đạo các cơ quan, đơn vị.	Sở Thông tin và Truyền thông	Các Sở, Ban ngành; UBND các huyện, thành phố	Quý IV
5	Xác định hoặc xác định lại cấp độ an toàn hệ thống thông tin cho các hệ thống thông tin của cơ quan nhà nước theo quy định.	Các đơn vị được giao vận hành hệ thống thông tin	Sở Thông tin và Truyền thông	Thường xuyên
6	Đánh giá, kiểm tra an toàn thông tin các hệ thống thông tin đã được phê duyệt cấp độ theo quy định.	Sở Thông tin và Truyền thông	Các cơ quan, đơn vị liên quan	Quý III
7	Thực hiện săn lùng mối nguy hại và rà quét lỗ hổng trên các hệ thống thông tin trong phạm vi quản lý tối thiểu 01 lần/6 tháng.	Các Sở, Ban ngành; UBND các huyện, thành phố.	Sở Thông tin và Truyền thông; các cơ quan, đơn vị liên quan	Quý II; Quý IV

STT	Tên nhiệm vụ	Cơ quan chủ trì	Cơ quan phối hợp	Thời gian
8	Các hệ thống thông tin phục vụ Chính quyền số tỉnh Cao Bằng được đảm bảo an toàn thông tin theo mô hình "4 lớp"	Các đơn vị được giao vận hành hệ thống thông tin	Sở Thông tin và Truyền thông; các cơ quan, đơn vị liên quan	Thường xuyên
9	Quản lý, triển khai hoạt động có hiệu quả hệ thống giám sát an toàn thông tin (SOC) tỉnh	Sở Thông tin và Truyền thông	Các Sở, Ban ngành; UBND các huyện, thành phố; đơn vị cung cấp dịch vụ	Thường xuyên
10	Tổ chức diễn tập thực chiến 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 III
11	Trang bị công cụ 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, phần mềm bản quyền chuyên dụng, máy chiếu…)	Sở Thông tin và Truyền thông	Các cơ quan, đơn vị liên quan	Trong năm
12	Tham gia các hoạt động an toàn thông tin theo chỉ đạo của Bộ TTTT; Cụm thành viên mạng lưới ứng cứu sự cố số 1 theo qui định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc	Sở Thông tin và Truyền thông	Đơn vị trực thuộc Bộ Thông tin và Truyền thông; Trưởng cụm theo phân công hằng năm	Trong năm
13	Tham quan học tập các địa phương trong nước có mô hình đảm bảo an toàn thông tin hiệu quả	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
14	Thuê chuyên gia về an toàn thông tin đáp ứng chuẩn kỹ năng về an toàn thông tin do Bộ Thông tin và Truyền thông quy định tham gia đội ứng cứu sự cố an toàn thông tin mạng của tỉnh	Sở Thông tin và Truyền thông	Các cơ quan, đơn vị liên quan	Thường xuyên