

**ỦY BAN NHÂN DÂN  
TỈNH CAO BẰNG**

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

Số: *2917* /UBND-VX

Cao Bằng, ngày *10* tháng *11* năm *2022*

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

Kính gửi:

- Các Sở, Ban, ngành;
- Ủy ban nhân dân các huyện, thành phố;
- Các doanh nghiệp viễn thông<sup>1</sup>.

Thực hiện Chỉ thị số 18/CT-TTg ngày 13/10/2022 của Thủ tướng Chính phủ về việc đẩy mạnh triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng Việt Nam; nhằm triển khai thực hiện nghiêm túc, hiệu quả các hoạt động ứng cứu sự cố an toàn thông tin mạng, bảo đảm an toàn thông tin mạng trong thực hiện chuyển đổi số, xây dựng chính quyền điện tử hướng tới chính quyền số, kinh tế số, xã hội số trên địa bàn tỉnh, Chủ tịch Ủy ban nhân dân (UBND) tỉnh chỉ đạo như sau:

1. Thủ trưởng các Sở, Ban ngành; Chủ tịch UBND các huyện, thành phố:

- Tổ chức quán triệt tới tất cả các tổ chức, cá nhân thuộc phạm vi quản lý nguyên tắc “*Ứng cứu sự cố an toàn thông tin mạng là hoạt động quan trọng nhằm phát hiện, ngăn chặn, xử lý và khắc phục kịp thời sự cố an toàn thông tin mạng*”; chỉ đạo triển khai nghiêm túc các nội dung của Chỉ thị số 18/CT-TTg và chịu trách nhiệm trước Chủ tịch UBND tỉnh nếu lơ là trong công tác ứng cứu sự cố an toàn thông tin mạng, để xảy ra hậu quả, thiệt hại nghiêm trọng tại cơ quan, đơn vị thuộc phạm vi quản lý.

- Hoạt động ứng cứu sự cố an toàn thông tin mạng phải chuyển từ bị động sang chủ động, bao gồm: chủ động phối hợp với Sở Thông tin và Truyền thông và các cơ quan chức năng thực hiện rà soát, phát hiện 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; ban hành phương án, kịch bản ứng cứu sự cố cho hệ thống thông tin thuộc đơn vị quản lý **trước ngày 31/12/2022** và cập nhật kịp thời khi có thay đổi; tham gia diễn tập thực chiến theo đề nghị của cơ quan chuyên môn của UBND tỉnh và Đội ứng cứu sự cố an toàn thông tin mạng tỉnh. Trường hợp phát hiện điểm yếu, lỗ hổng bảo mật cho phép xâm nhập và kiểm soát hệ thống thì thực hiện đồng thời khắc phục điểm yếu, lỗ hổng và săn lùng mối nguy hại.

- Tham gia bảo đảm an toàn thông tin mạng trong 11 lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng<sup>2</sup> theo hướng dẫn của Bộ, ngành

<sup>1</sup> VNPT Cao Bằng, Viettel Cao Bằng, FPT Cao Bằng, Mobifone Cao Bằng.

<sup>2</sup> Theo Quyết định số 632/QĐ-TTg ngày 10/5/2017 của Thủ tướng Chính phủ Ban hành danh mục lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng và hệ thống thông tin quan trọng quốc gia.

Trung ương; 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 lĩnh vực (CERT lĩnh vực).

- Bố trí nhân lực có chuyên môn, nghiệp vụ thực hiện công tác ứng cứu sự cố an toàn thông tin mạng trong phạm vi, lĩnh vực quản lý.

- Nghiêm túc thực hiện việc 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.

- Có biện pháp kiểm soát nguy cơ mất an toàn thông tin mạng gây ra bởi bên thứ ba và các chuỗi cung ứng công nghệ thông tin và truyền thông.

- Nghiêm túc thực hiện các quy định về báo cáo sự cố an toàn thông tin mạng; đẩy mạnh tuyên truyền cho người dân về việc báo cáo, cung cấp thông tin về sự cố; khuyến khích triển khai các chiến dịch nâng cao ý thức cảnh giác của người dùng thiết bị đầu cuối đối với các cuộc tấn công mạng.

## 2. Sở Thông tin và Truyền thông có trách nhiệm:

- Là cơ quan đầu mối chuyên trách về an toàn thông tin của tỉnh; hướng dẫn các cơ quan, đơn vị triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh theo chỉ đạo của Chính phủ, các Bộ, ngành Trung ương; thúc đẩy hoạt động diễn tập thực chiến an toàn thông tin mạng tại các cơ quan, tổ chức.

- Chủ trì tổ chức triển khai, hướng dẫn, theo dõi, đôn đốc, kiểm tra và đánh giá việc thực hiện Chỉ thị số 18/CT-TTg trên địa bàn tỉnh; tổng hợp, báo cáo UBND tỉnh kết quả thực hiện.

- Chủ trì, phối hợp với các cơ quan, đơn vị liên quan tham mưu UBND tỉnh kiện toàn Đội ứng cứu sự cố an toàn thông tin mạng tỉnh theo hướng chuyên nghiệp, cơ động, có tối thiểu 05 chuyên gia an toàn thông tin mạng (bao gồm cả chuyên gia thuê ngoài) đáp ứng chuẩn kỹ năng về an toàn thông tin do Bộ Thông tin và Truyền thông quy định. Thời gian hoàn thành: **Trước ngày 31/12/2022.**

- Khẩn trương phối hợp với Văn phòng UBND tỉnh cung cấp thông tin (số điện thoại, thư điện tử hoặc các kênh liên lạc khác), công bố trên Cổng Thông tin điện tử tỉnh để tiếp nhận thông báo sự cố an toàn thông tin mạng và các nhiệm vụ ứng cứu sự cố an toàn thông tin mạng.

- Theo chức năng, nhiệm vụ được giao tổ chức diễn tập thực chiến tối thiểu 01 lần/năm đối với các hệ thống thông tin cấp độ 3 trở lên, nhằm đánh giá khả năng phòng ngừa xâm nhập và khả năng phát hiện kịp thời các điểm yếu về quy trình, công nghệ, con người.

- Chủ trì, phối hợp với Sở Nội vụ và các cơ quan liên quan có giải pháp thu hút nhân lực chất lượng cao, đào tạo, bồi dưỡng nâng cao năng lực chuyên môn, nghiệp vụ cho đội ngũ công chức, viên chức thực hiện nhiệm vụ chuyên

đổi số nói chung, ứng cứu sự cố an toàn thông tin mạng nói riêng tại các cơ quan, đơn vị trên địa bàn tỉnh.

3. Đội ứng cứu sự cố an toàn thông tin mạng tỉnh có trách nhiệm thực hiện các nhiệm vụ thường xuyên sau: Làm đầu mối tiếp nhận, quản lý sự cố; ứng cứu, xử lý sự cố và sẵn lòng mỗi nguy hại; nghiên cứu, theo dõi các nguy cơ tấn công mạng, thông tin về lỗ hổng, điểm yếu; luyện tập các kỹ năng bảo vệ hệ thống thông tin và tham gia các chương trình huấn luyện, diễn tập do Cơ quan điều phối quốc gia chủ trì.

4. Công an tỉnh, Bộ Chỉ huy Quân sự tỉnh triển khai các hoạt động ứng cứu sự cố theo chức năng, nhiệm vụ được giao; phối hợp chặt chẽ với Sở Thông tin và Truyền thông trong hoạt động ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh.

5. Sở Tài chính phối hợp với các cơ quan, đơn vị liên quan căn cứ khả năng ngân sách tham mưu cho UBND tỉnh cân đối kinh phí từ ngân sách nhà nước cho hoạt động ứng cứu sự cố an toàn thông tin mạng.

6. Các doanh nghiệp cung cấp dịch vụ viễn thông, Internet:

- Công bố thông tin đầu mối (số điện thoại, thư điện tử hoặc các kênh liên lạc khác) tiếp nhận thông báo sự cố trên cổng thông tin (website) **trước ngày 15/11/2022**; tuyên truyền cho khách hàng về cách thức phản ánh sự cố mất an toàn thông tin mạng.

- Nghiêm túc tuân thủ các yêu cầu điều phối của Cơ quan điều phối quốc gia trong các hoạt động ứng cứu, xử lý sự cố.

- Cảnh báo cho khách hàng các nguy cơ, sự cố an toàn thông tin mạng trên diện rộng hoặc khi phát hiện nguy cơ, sự cố an toàn thông tin mạng liên quan tới khách hàng; hỗ trợ khách hàng ứng cứu, xử lý sự cố an toàn thông tin mạng liên quan tới dịch vụ do doanh nghiệp cung cấp.

Căn cứ ý kiến chỉ đạo trên, các cơ quan, đơn vị triển khai thực hiện./.

**Nơi nhận:**

- Như trên;
- Văn phòng Chính phủ (b/c);
- Bộ Thông tin và Truyền thông (b/c);
- Chủ tịch, các PCT UBND tỉnh;
- VP UBND tỉnh: LĐVP; TP.VX, TTTT;
- Lưu: VT, VX<sub>(M)</sub>.

*R*

**CHỦ TỊCH**



**Hoàng Xuân Ánh**

