

**QUYẾT ĐỊNH**  
**Về việc ban hành Quy chế hoạt động**  
**của Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Bắc Kạn**

**ỦY BAN NHÂN DÂN TỈNH BẮC KẠN**

Căn cứ Luật Tổ chức chính quyền địa phương năm 2015; Luật sửa đổi, bổ sung một số điều của Luật Tổ chức Chính phủ và Luật Tổ chức chính quyền địa phương năm 2019;

Căn cứ Luật An toàn thông tin mạng năm 2015;

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ 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 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;

Căn cứ Công văn số 4258/BTTTT-CATTT ngày 26/10/2021 của Bộ Thông tin và Truyền thông về việc hướng dẫn tổ chức, hoạt động của Đội ứng cứu sự cố an toàn thông tin mạng;

Căn cứ Quyết định số 2029/QĐ-BTTTT ngày 23/10/2023 của Bộ trưởng Bộ Thông tin và Truyền thông về việc ban hành “Mô hình đánh giá mức độ trưởng thành của Đội ứng cứu sự cố an toàn thông tin mạng”;

Căn cứ Quyết định số 293/QĐ-UBND ngày 28/02/2024 của UBND tỉnh Bắc Kạn về việc kiện toàn, đổi tên Đội ứng cứu sự cố mạng, máy tính tỉnh Bắc Kạn;

Theo đề nghị của Sở Thông tin và Truyền thông tại Tờ trình số 14/TTr-STTTT ngày 20/3/2024.

**QUYẾT ĐỊNH:**

**Điều 1.** Ban hành kèm theo Quyết định này Quy chế hoạt động của Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Bắc Kạn.

**Điều 2.**

1. Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Bắc Kạn và các cơ quan, tổ chức, cá nhân liên quan trong hoạt động điều phối, ứng cứu sự cố mạng, máy tính trên địa bàn tỉnh có trách nhiệm thực hiện các quy định trong Quy chế hoạt động của Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Bắc Kạn ban hành kèm theo Quyết định này, đảm bảo chất lượng, hiệu quả.

2. Quyết định này có hiệu lực kể từ ngày ký và thay thế Quyết định số 1195/QĐ-UBND ngày 15/8/2017 của UBND tỉnh Bắc Kạn về việc ban hành Quy chế hoạt động của Đội ứng cứu sự cố mạng, máy tính tỉnh Bắc Kạn.

**Điều 3.** Chánh Văn phòng UBND tỉnh; Thủ trưởng các sở, ban, ngành tỉnh; Chủ tịch UBND các huyện, thành phố; Thành viên Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Bắc Kạn và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

***Nơi nhận:***

- Như Điều 3 (t/h);
- Bộ Thông tin và Truyền thông (báo cáo);
- CT, PCT UBND tỉnh (Ô. Hưng);
- Sở Thông tin và Truyền thông;
- CVP;
- Lưu: VT, Huyện, Nhung

**TM. ỦY BAN NHÂN DÂN  
CHỦ TỊCH**

**Nguyễn Đăng Bình**

**QUY CHẾ**

**Hoạt động của Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Bắc Kạn**  
(Kèm theo Quyết định số          /QĐ-UBND ngày      /3/2024 của UBND tỉnh Bắc Kạn)

**Chương I**  
**QUY ĐỊNH CHUNG****Điều 1. Phạm vi và đối tượng áp dụng**

1. Quy chế này quy định về nhiệm vụ, quyền hạn, trách nhiệm, nguyên tắc và chế độ hoạt động của Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Bắc Kạn (sau đây gọi tắt là *Đội ứng cứu sự cố*).

2. Quy chế này được áp dụng cho *Đội ứng cứu sự cố* và các cơ quan, tổ chức, cá nhân có liên quan trong hoạt động điều phối, ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh Bắc Kạn.

**Điều 2. Giải thích từ ngữ**

1. *Đội ứng cứu sự cố an toàn thông tin mạng* là tổ chức/đơn vị do Chủ quản hệ thống thông tin thành lập nhằm triển khai các hoạt động, giải pháp sẵn sàng ứng phó hoặc ứng phó với các đe dọa, rủi ro, các lỗ hổng, điểm yếu và các sự cố đối với các hệ thống, cơ sở hạ tầng thông tin và không gian mạng trong phạm vi quản lý.

2. *Chủ quản *Đội ứng cứu sự cố** là cơ quan ra quyết định thành lập *Đội ứng cứu sự cố*. Chủ quản *Đội ứng cứu sự cố* có thẩm quyền quyết định mô hình tổ chức, quyết định phân bổ nhân lực, vật lực và kinh phí hoạt động của *Đội ứng cứu sự cố* theo quy định pháp luật có liên quan.

3. *Vị trí chuyên trách về an toàn thông tin (ATTT)*: Đảm nhiệm nhóm công việc đặc trưng khác biệt, có cùng độ phức tạp, thuộc lĩnh vực an toàn thông tin; thường sử dụng cùng nhóm kiến thức và kỹ năng. Khác với vị trí việc làm chuyên môn, cơ quan nào cũng có như: Quản lý nhân sự, tài chính,...

4. *Sự cố an toàn thông tin mạng* là sự kiện đã, đang xảy ra gây mất an toàn thông tin trên môi trường mạng (*LAN, WAN, INTERNET*) được phát hiện thông qua việc giám sát, đánh giá, phân tích của các cơ quan, tổ chức, cá nhân có liên quan hoặc được cảnh báo từ các chuyên gia, tổ chức về lĩnh vực an toàn thông tin mạng trong nước và trên thế giới.

5. *Sự cố có tính chất nghiêm trọng* là sự cố có một hoặc nhiều tính chất sau: Có khả năng xảy ra trên diện rộng, thời gian xảy ra nhanh; có khả năng phá hoại hệ thống mạng máy tính; lấy cắp dữ liệu, có thể gây thiệt hại lớn cho các hệ thống thông tin trên mạng, các hệ thống thông tin quan trọng của tỉnh như: Hệ thống thông tin quản lý hành chính cấp tỉnh, Công thông tin điện tử tỉnh, Hệ thống thư công vụ tỉnh, các hệ thống chuyên ngành, Trung tâm dữ liệu,... đòi hỏi sự phối hợp của nhiều cơ quan, đơn vị trong tỉnh và cần có sự hỗ trợ của các cơ quan chuyên trách quốc gia để giải quyết.

6. *Ứng cứu sự cố ATTT mạng* là hoạt động nhằm xử lý, khắc phục sự cố gây mất ATTT mạng, gồm: Theo dõi, thu thập, phân tích, phát hiện, cảnh báo, kiểm tra, xác minh sự cố, ngăn chặn sự cố, khôi phục dữ liệu và khôi phục hoạt động bình thường của hệ thống thông tin.

### **Điều 3. Tổ chức Đội ứng cứu sự cố**

1. Đội ứng cứu sự cố do UBND tỉnh Bắc Kạn kiện toàn tại Quyết định số 293/QĐ-UBND ngày 28/02/2024. Đội ứng cứu sự cố gồm 01 đội trưởng, 02 đội phó và các thành viên.

2. Đội ứng cứu sự cố sử dụng con dấu của Sở Thông tin và Truyền thông để giao dịch thực hiện nhiệm vụ. Bộ phận thường trực của Đội ứng cứu sự cố đặt tại Phòng Công nghệ thông tin-Bưu chính, Viễn thông, Sở Thông tin và Truyền thông (*Địa chỉ: Tổ 7, phường Đức Xuân, thành phố Bắc Kạn, tỉnh Bắc Kạn; thư điện tử: [Csirt@backan.gov.vn](mailto:Csirt@backan.gov.vn); số điện thoại thường trực: 02093.878.777; 02093.871.626; địa chỉ Diễn đàn ATTT mạng tỉnh Bắc Kạn: <https://attt.backan.gov.vn>*).

### **Điều 4. Nguyên tắc điều phối, ứng cứu sự cố**

1. Tuân thủ các quy định pháp luật về điều phối, ứng cứu sự cố an toàn thông tin mạng.

2. Chủ động, kịp thời, nhanh chóng, chính xác, đồng bộ và hiệu quả.

3. Phối hợp chặt chẽ, chính xác, đồng bộ và hiệu quả giữa các cơ quan tổ chức, doanh nghiệp trong nước và nước ngoài.

4. Ứng cứu sự cố trước hết phải được thực hiện, xử lý bằng lực lượng tại chỗ và trách nhiệm chính của chủ quản hệ thống thông tin.

5. Tuân thủ các điều kiện, nguyên tắc ưu tiên về duy trì hoạt động của hệ thống thông tin đã được cấp thẩm quyền phê duyệt trong kế hoạch ứng phó sự cố.

6. Thông tin trao đổi trong mạng lưới phải được kiểm tra, xác thực đối tượng trước khi thực hiện các bước tác nghiệp tiếp theo.

7. Bảo đảm bí mật thông tin trong quá trình tham gia, thực hiện các hoạt động ứng cứu sự cố theo yêu cầu của Cơ quan điều phối quốc gia hoặc cơ quan tổ chức, cá nhân gặp sự cố.

## **Chương II**

### **TRÁCH NHIỆM, QUYỀN HẠN, QUY TẮC, CHẾ ĐỘ HOẠT ĐỘNG VÀ KINH PHÍ HOẠT ĐỘNG**

### **Điều 5. Trách nhiệm, quyền hạn của Đội ứng cứu sự cố**

Thực hiện theo các quy định tại Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia; Khoản 1 Điều 6, Khoản 2 Điều 10 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 và Mục 2.4 Công văn số 4258/BTTTT-CATTT ngày 26/10/2021 của Bộ Thông tin và Truyền thông về việc hướng dẫn tổ chức, hoạt động của Đội ứng cứu sự cố an toàn thông tin mạng.

### **Điều 6. Các quy tắc hoạt động của Đội ứng cứu sự cố**

Đội ứng cứu sự cố đảm bảo xây dựng, duy trì và tuân thủ các quy tắc, quy định tối thiểu sau:

- Bộ quy tắc ứng xử.
- Quy định phân loại thông tin.
- Quy định cung cấp thông tin.
- Quy định truyền thông.
- Quy định an toàn thông tin.
- Quy định đối với lỗi do con người.

### **Điều 7. Chế độ làm việc**

1. Các thành viên Đội ứng cứu sự cố làm việc theo chế độ kiêm nhiệm và được hưởng các chế độ theo quy định hiện hành; khi xảy ra sự cố, các thành viên phải ưu tiên cho hoạt động của Đội ứng cứu sự cố, tuân thủ việc triệu tập, điều phối của Đội trưởng hoặc Đội phó được ủy quyền.

2. Đội trưởng triệu tập thành viên Đội ứng cứu sự cố, tổ chức phiên họp thường kỳ 06 tháng/lần hoặc triệu tập họp đột xuất theo yêu cầu nhiệm vụ và yêu cầu của cơ quan cấp trên. Thời gian và địa điểm họp do Đội trưởng quyết định. Bộ phận thường trực Đội ứng cứu sự cố có trách nhiệm chuẩn bị các điều kiện cần thiết để chuẩn bị các cuộc họp, tổng hợp biên bản họp và các nội dung khác theo yêu cầu của Đội trưởng.

3. Đội trưởng triệu tập và điều phối các thành viên khi có sự cố đột xuất xảy ra, hoặc ủy quyền cho 01 Đội phó thực hiện thẩm quyền của mình khi vắng mặt. Đội phó khi được ủy quyền được sử dụng thẩm quyền của Đội trưởng để điều phối các hoạt động và chịu trách nhiệm về các quyết định của mình trước Đội trưởng và pháp luật hiện hành liên quan.

4. Hoạt động trao đổi công việc giữa các thành viên Đội ứng cứu sự cố trên môi trường mạng được thực hiện thông qua hệ thống thư công vụ, thư điện tử theo quy định.

5. Thẩm quyền ký ban hành văn bản của Đội ứng cứu sự cố thực hiện theo quy định của pháp luật hoặc theo phân công, ủy quyền.

### **Điều 8. Kinh phí hoạt động**

1. Kinh phí hoạt động của Đội ứng cứu sự cố được bố trí trong nguồn ngân sách nhà nước cấp hàng năm qua Sở Thông tin và Truyền thông.

2. Hàng năm, Đội ứng cứu sự cố hoặc Sở Thông tin và Truyền thông (*Đơn vị chuyên trách về ATTT*) căn cứ trách nhiệm, quyền hạn của Đội ứng cứu sự cố xây dựng kế hoạch, dự toán kinh phí thực hiện theo quy định.

### **Chương III**

## **TỔ CHỨC ỨNG CỨU SỰ CỐ**

### **Điều 9. Tiếp nhận và xử lý thông báo, báo cáo sự cố**

#### 1. Các hình thức thông báo, báo cáo sự cố

a) Hình thức thông báo sự cố: Bằng công văn, fax, thư điện tử, nhắn tin đa phương tiện, hệ thống điều phối sự cố quốc gia irlab.vn...;

b) Hình thức báo cáo sự cố: Bằng văn bản giấy hoặc văn bản điện tử (có ký tên, đóng dấu hoặc chữ ký số của người có thẩm quyền).

2. Khi gặp sự cố không tự khắc phục được, các cơ quan, đơn vị, địa phương có trách nhiệm thông báo hoặc báo cáo sự cố kịp thời tới Bộ phận thường trực của Đội ứng cứu sự cố hoặc thành viên Đội ứng cứu sự cố theo mẫu tại Phụ lục I, II kèm theo Quy chế này.

3. Bộ phận thường trực của Đội ứng cứu sự cố và cá nhân thành viên trong Đội khi tiếp nhận được thông báo sự cố từ cơ quan, đơn vị, địa phương phải thông tin, báo ngay cho Đội trưởng hoặc các Đội phó Đội ứng cứu sự cố để kịp thời chỉ đạo, giải quyết, khắc phục.

4. Khi nhận được thông báo, Đội trưởng hoặc các Đội phó Đội ứng cứu sự cố quyết định điều phối các thành viên trong Đội tham gia xử lý sự cố. Trong trường hợp xảy ra sự cố phức tạp, Đội trưởng triệu tập cuộc họp và huy động các nguồn lực để xử lý sự cố.

### **Điều 10. Quy trình ứng cứu sự cố an toàn thông tin mạng**

1. Quy trình ứng cứu sự cố an toàn thông tin mạng thông thường thực hiện theo văn bản hướng dẫn, quy định của Bộ Thông tin và Truyền thông và Cơ quan điều phối quốc gia.

2. Quy trình ứng cứu sự cố an toàn thông tin mạng nghiêm trọng được xử lý theo các phương án ứng cứu khẩn cấp quy định tại Điều 10 Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia.

### **Chương IV**

## **TRÁCH NHIỆM CỦA CÁC TỔ CHỨC, CÁ NHÂN**

### **Điều 11. Sở Thông tin và Truyền thông**

1. Được quyền điều động các thành viên Đội ứng cứu sự cố nhằm thực hiện hoặc phối hợp thực hiện việc ngăn chặn, xử lý, khắc phục sự cố ATTT mạng.

2. Đầu mối liên lạc ứng cứu sự cố trên địa bàn tỉnh và trong mạng lưới ứng cứu sự cố ATTT mạng trên toàn quốc.

3. Theo dõi, cập nhật, thông báo kịp thời thông tin liên hệ của thành viên Đội ứng cứu sự cố của các cơ quan, đơn vị trên địa bàn tỉnh. Đề xuất, trình cấp có thẩm quyền kiện toàn khi có sự thay đổi nhân sự.

4. Chỉ đạo Bộ phận thường trực của Đội ứng cứu sự cố (*Phòng Công nghệ thông tin-Bưu chính, Viễn thông*) chủ trì, phối hợp với các thành viên trong Đội xây dựng kế hoạch, dự toán kinh phí hoạt động của Đội; triển khai công tác đảm bảo an toàn thông tin nhằm phòng ngừa, phát hiện và xử lý các sự cố mạng, máy tính trên địa bàn tỉnh; thông báo kết quả tham gia hoạt động của thành viên Đội ứng cứu sự cố cho cơ quan chủ quản để phối hợp quản lý; thực hiện chế độ báo cáo, thống kê theo quy định.

5. Thực hiện báo cáo định kỳ và đột xuất khi có yêu cầu về hoạt động tiếp nhận và xử lý sự cố cho UBND tỉnh, Ban Chỉ đạo về chuyển đổi số tỉnh, Cơ quan điều phối cấp trên, Bộ Thông tin và Truyền thông và cơ quan cấp trên khác có thẩm quyền.

### **Điều 12. Đội trưởng Đội ứng cứu sự cố**

1. Chịu trách nhiệm trước UBND tỉnh, Chủ tịch UBND tỉnh về toàn bộ hoạt động của Đội; kịp thời báo cáo, đề xuất, tham mưu cho UBND tỉnh, Chủ tịch UBND tỉnh xem xét, chỉ đạo, giải quyết những vấn đề vượt thẩm quyền được giao.

2. Chủ trì các cuộc họp, điều phối, quyết định tổ chức ứng cứu; triệu tập các thành viên để xử lý và khắc phục sự cố an toàn thông tin mạng.

3. Liên hệ, phối hợp với Trung tâm ứng cứu khẩn cấp máy tính Việt Nam - VNCERT, các doanh nghiệp cung cấp dịch vụ Internet và các đơn vị liên quan.

4. Quyết định hình thức điều phối các hoạt động ứng cứu sự cố và chịu trách nhiệm về các yêu cầu điều phối.

### **Điều 13. Đội phó Đội ứng cứu sự cố**

1. Giúp Đội trưởng điều hành các hoạt động của Đội ứng cứu sự cố, chịu trách nhiệm trước Đội trưởng về nhiệm vụ được giao; đề xuất kế hoạch, biện pháp kỹ thuật tăng cường công tác đảm bảo ATTT mạng.

2. Chỉ đạo các thành viên trong các hoạt động phòng ngừa, ngăn chặn và xử lý sự cố mạng máy tính theo thẩm quyền và nhiệm vụ được phân công; thay mặt Đội trưởng điều hành các hoạt động của Đội ứng cứu sự cố khi được ủy quyền.

3. Thực hiện các nhiệm vụ do Đội trưởng phân công và tham gia xây dựng Kế hoạch hoạt động hằng năm của Đội ứng cứu sự cố.

### **Điều 14. Thành viên Đội ứng cứu sự cố**

1. Thực hiện nhiệm vụ do Đội trưởng giao.

2. Tiếp nhận và xử lý các thông báo sự cố hoặc văn bản triệu tập xử lý sự cố từ Đội trưởng.

3. Tham gia đầy đủ các cuộc họp định kỳ, đột xuất và hoạt động ứng cứu sự cố do Đội trưởng triệu tập, điều phối.

4. Kịp thời báo cáo, đề xuất giải quyết khó khăn, vướng mắc trong quá trình thực hiện nhiệm vụ với Đội trưởng hoặc Đội phó để kịp thời chỉ đạo, xử lý.

5. Phối hợp, hỗ trợ các thành viên khác trong Đội ứng cứu sự cố, cán bộ phụ trách công nghệ thông tin của các cơ quan, đơn vị trong việc áp dụng các biện pháp, giải pháp kỹ thuật nhằm bảo đảm ATTT mạng cho các hệ thống thông tin;

thường xuyên thực hiện quét virus trong hệ thống máy tính nhằm phòng, chống sự cố mạng tại cơ quan, đơn vị.

6. Tiếp nhận đầy đủ, chính xác thông tin về sự cố và thông báo kịp thời cho Đội trưởng để thực hiện công tác điều phối ứng cứu sự cố.

7. Tham gia góp ý, đề xuất xây dựng Kế hoạch hoạt động hằng năm của Đội ứng cứu sự cố; tham gia các hoạt động diễn tập ứng cứu sự cố, các khóa đào tạo, bồi dưỡng về ATTT và ứng cứu sự cố do Sở Thông tin và Truyền thông triệu tập. Tham mưu cho lãnh đạo thực hiện tốt công tác đảm bảo ATTT tại cơ quan, đơn vị.

8. Kịp thời thông báo sự cố xảy ra gửi về Đội ứng cứu sự cố để phối hợp xử lý; định kỳ (06 tháng, 01 năm) báo cáo tổng hợp về hoạt động tiếp nhận và xử lý sự cố theo mẫu tại Phụ lục III kèm theo Quy chế này.

### **Điều 15. Bộ phận thường trực của Đội ứng cứu sự cố**

1. Thực hiện nhiệm vụ đầu mối liên lạc, tiếp nhận thông tin điều phối ứng cứu sự cố ATTT mạng của tỉnh; các phản ánh sự cố, điều phối xử lý sự cố từ Trung tâm ứng cứu khẩn cấp máy tính Việt Nam - VNCERT; giúp Đội trưởng điều phối ứng cứu sự cố trên địa bàn tỉnh.

2. Thông báo cho các tổ chức, cá nhân gặp sự cố về yêu cầu phối hợp trong quá trình thực hiện điều phối và ứng cứu sự cố; tổng hợp, cập nhật và công bố các cảnh báo về điểm yếu, lỗ hổng bảo mật, các nguồn tấn công trên mạng Internet,... trên Diễn đàn ATTT mạng tỉnh Bắc Kạn: <https://attt.backan.gov.vn>.

3. Chủ trì, phối hợp với các thành viên trong Đội ứng cứu sự cố xây dựng kế hoạch, dự toán kinh phí hoạt động của Đội; triển khai công tác đảm bảo an toàn thông tin nhằm phòng ngừa, phát hiện và xử lý các sự cố mạng, máy tính trên địa bàn tỉnh; thông báo kết quả tham gia hoạt động của thành viên Đội ứng cứu sự cố cho cơ quan chủ quản để phối hợp quản lý; thực hiện chế độ báo cáo, thống kê theo quy định.

4. Tham mưu xây dựng kế hoạch đào tạo, tập huấn ngắn hạn, trung hạn và dài hạn cho cán bộ phụ trách công nghệ thông tin tại các cơ quan, đơn vị của tỉnh, các huyện, thành phố; UBND các xã, phường, thị trấn và các cơ quan chuyên trách công nghệ thông tin trên địa bàn tỉnh. Đồng thời, hướng dẫn công tác đảm bảo an toàn an ninh thông tin cho các cán bộ chuyên trách công nghệ thông tin trên địa bàn tỉnh Bắc Kạn.

5. Theo dõi, cập nhật, thông báo kịp thời thông tin liên hệ của các thành viên Đội ứng cứu sự cố. Đề xuất trình cấp có thẩm quyền kiện toàn thành viên Đội ứng cứu sự cố khi có thay đổi về nhân sự.

### **Điều 16. Trách nhiệm của cơ quan quản lý thành viên Đội ứng cứu sự cố**

1. Thủ trưởng các cơ quan, đơn vị có trách nhiệm tạo điều kiện và ưu tiên cho thành viên Đội ứng cứu sự cố thuộc đơn vị mình quản lý thực hiện các hoạt động của Đội ứng cứu sự cố khi được triệu tập, điều phối.

2. Kịp thời thông báo về Sở Thông tin và Truyền thông cập nhật danh sách thành viên tham gia Đội ứng cứu sự cố khi có thay đổi.



## **Chương V**

### **TỔ CHỨC THỰC HIỆN**

#### **Điều 17. Hướng dẫn, kiểm tra, khen thưởng**

1. Giao Sở Thông tin và Truyền thông chủ trì tổ chức, kiểm tra, hướng dẫn việc thực hiện Quy chế này đối với các thành viên Đội ứng cứu sự cố và các cơ quan, đơn vị, địa phương có liên quan trong tỉnh; kịp thời phát hiện và phối hợp với cơ quan chức năng liên quan tham mưu xử lý những trường hợp vi phạm quy định hiện hành liên quan.

2. Căn cứ kết quả hoạt động của mỗi thành viên Đội ứng cứu sự cố, Bộ phận thường trực Đội ứng cứu sự cố báo cáo, đề nghị UBND tỉnh Bắc Kạn xem xét khen thưởng theo quy định.

#### **Điều 18. Điều khoản thi hành**

Trong quá trình thực hiện Quy chế, nếu có vướng mắc, phát sinh, các cơ quan, đơn vị, địa phương, thành viên Đội ứng cứu sự cố phản ánh về Bộ phận thường trực Đội ứng cứu sự cố để tổng hợp, trình cấp có thẩm quyền xem xét sửa đổi, bổ sung cho phù hợp với các quy định hiện hành./.

---

**Phụ lục I**  
**MẪU BÁO CÁO THÔNG TIN BAN ĐẦU VỀ SỰ CỐ**

Tên tổ chức/cá nhân báo cáo sự cố (\*):.....

Địa chỉ: (\*) .....

Điện thoại (\*) .....

Email (\*):.....

**NGƯỜI LIÊN HỆ**

Họ và tên (\*)..... Chức vụ.....

Điện thoại (\*):.....Email (\*):.....

**THÔNG TIN CHI TIẾT VỀ HỆ THỐNG BỊ SỰ CỐ**

Tên đơn vị vận hành hệ thống thông tin (*):	<i>Điền tên đơn vị vận hành hoặc được thuê vận hành hệ thống thông tin</i>
Cơ quan chủ quản:	<i>Điền tên cơ quan chủ quản</i>
Tên hệ thống bị sự cố	<i>Điền tên hệ thống bị sự cố và tên miền, địa chỉ ip liên quan</i>
Phân loại cấp độ của hệ thống thông tin (nếu có)	<input type="checkbox"/> Cấp độ 1 <input type="checkbox"/> Cấp độ 2 <input type="checkbox"/> Cấp độ 3
Tổ chức cung cấp dịch vụ an toàn thông tin (nếu có):	<i>Điền tên nhà cung cấp ở đây</i>
Tên nhà cung cấp dịch vụ kết nối bên ngoài (nếu có)	<i>Điền tên nhà cung cấp ở đây</i>
Điền tên nhà cung cấp ở đây	<i>Điền thông tin ở đây</i>
<b>Mô tả sơ bộ sự cố (*)</b>	
<i>Đề nghị cung cấp một bản tóm tắt ngắn gọn về sự cố, bao gồm đánh giá sơ bộ cuộc tấn công đã xảy ra chưa và bất kỳ các nguy cơ dẫn đến khả năng phá hoại hoặc gián đoạn dịch vụ. Cũng vui lòng xác định mức độ nhạy cảm của thông tin liên quan hoặc những đối tượng bị ảnh hưởng bởi sự cố:</i>	
.....	
.....	
.....	

.....		
Ngày phát hiện sự cố (*) // (dd/mm/yy)	Thời gian phát hiện (*):	..... giờ.... phút

### HIỆN TRẠNG SỰ CỐ (\*)

- Đã được xử lý  Chưa được xử lý

### CÁCH THỨC PHÁT HIỆN \* (Đánh dấu những cách thức được sử dụng để phát hiện sự cố)

- Qua hệ thống phát hiện xâm nhập  Kiểm tra dữ liệu lưu lại (Log File)
- Nhận được thông báo từ:.....
- Khác, đó là:.....

### ĐÃ GỬI THÔNG BÁO SỰ CỐ CHO \*

- Thành viên mạng lưới chịu trách nhiệm ứng cứu sự cố cho tổ chức, cá nhân
- ISP đang trực tiếp cung cấp dịch vụ
- Cơ quan điều phối

### THÔNG TIN BỔ SUNG VỀ HỆ THỐNG XẢY RA SỰ CỐ

- Hệ điều hành ..... Version.....
- Các dịch vụ có trên hệ thống (Đánh dấu những dịch vụ được sử dụng trên hệ thống)
- Web server  Mail server  Database server
- Dịch vụ khác, đó là:.....
- Các biện pháp an toàn thông tin đã triển khai (Đánh dấu những biện pháp đã triển khai)
- Antivirus  Firewall  Hệ thống phát hiện xâm nhập
- Khác:
- Các địa chỉ IP của hệ thống (Liệt kê địa chỉ IP sử dụng trên Internet, không liệt kê địa chỉ IP nội bộ).....
- Các tên miền của hệ thống.....
- Mục đích chính sử dụng hệ thống.....

Thông tin gửi kèm

Nhật ký hệ thống       Mẫu virus/mã độc       Khác:

■ Các thông tin cung cấp trong thông báo sự cố này đều phải được giữ bí mật:

Có       Không

### **KIẾN NGHỊ, ĐỀ XUẤT HỖ TRỢ**

Mô tả về đề xuất, kiến nghị

*Đề nghị cung cấp tóm lược về các kiến nghị và đề xuất hỗ trợ ứng cứu (nếu có)*

.....

.....

.....

.....

.....

### **THỜI GIAN THỰC HIỆN BÁO CÁO SỰ CỐ\*:**

(ngày/tháng/năm/giờ/phút)

**CÁ NHÂN/NGƯỜI ĐẠI DIỆN  
THEO PHÁP LUẬT**  
(Ký tên, đóng dấu)

*Chú thích:*

1. Phần (\*) là những thông tin bắt buộc. Các phần còn lại có thể loại bỏ nếu không có thông tin.
2. Sử dụng tiêu đề (subject) bắt đầu bằng “[TBSC]” khi gửi thông báo qua email.
3. Tham khảo thêm tại website của VNCERT ([www.vncert.gov.vn](http://www.vncert.gov.vn)).

**Phụ lục II**  
**MẪU BÁO CÁO KẾT THÚC ỨNG PHÓ SỰ CỐ**

**THÔNG TIN VỀ TỔ CHỨC/CÁ NHÂN BÁO CÁO**

- Tên tổ chức/cá nhân báo cáo sự cố (\*)
- Địa chỉ: (\*) .....
- Điện thoại (\*).....
- Email (\*).....

**KÝ HIỆU BÁO CÁO BAN ĐẦU SỰ CỐ:** Số ký hiệu    Ngày báo cáo: / /202..

**THÔNG TIN CHI TIẾT VỀ HỆ THỐNG BỊ SỰ CỐ**

Tên đơn vị vận hành hệ thống thông tin (*):	<i>Điền tên đơn vị vận hành hoặc được thuê vận hành hệ thống thông tin</i>
Cơ quan chủ quản:	<i>Điền tên cơ quan chủ quản</i>
Tên hệ thống bị sự cố	<i>Điền tên hệ thống bị sự cố</i>
Phân loại cấp độ của hệ thống thông tin (nếu có)	<input type="checkbox"/> Cấp độ 1 <input type="checkbox"/> Cấp độ 2 <input type="checkbox"/> Cấp độ 3

<b>Tên/Mô tả về sự cố</b> ..... ..... ..... ..... .....
--

Ngày phát hiện sự cố (*).../.../..... (dd/mm/yy)	Thời gian phát hiện (*):	....giờ.... phút
---	--------------------------	------------------

**Kết quả xử lý sự cố**

*Cung cấp, tóm tắt tổng quát về những gì đã xảy ra và cách thức giải quyết, đề xuất giải pháp ứng cứu ứng sự cố nhằm xử lý nhanh sự cố, giảm nhẹ rủi ro và thiệt hại đối với sự cố tương tự trong tương lai*

.....

.....

.....

.....

**Các tài liệu đính kèm**

*Liệt kê các tài liệu liên quan (báo cáo diễn biến sự cố; phương án xử lý, log file...)*

**CÁ NHÂN/NGƯỜI ĐẠI DIỆN THEO  
PHÁP LUẬT**  
*(Ký tên, đóng dấu)*

*Chú thích: Phần (\*) là những thông tin bắt buộc. Các phần còn lại có thể loại bỏ nếu không có thông tin.*

**Phụ lục III**  
**MẪU BÁO CÁO ĐỊNH KỲ**

Kính gửi: Sở Thông tin và Truyền thông

**BÁO CÁO TỔNG HỢP (06 THÁNG, 01 NĂM VỀ HOẠT ĐỘNG TIẾP NHẬN  
VÀ XỬ LÝ SỰ CỐ**

□ Từ tháng ...../20 ... đến tháng ...../20...

Tên cơ quan/tổ chức:.....

Địa chỉ: .....

1. Số lượng sự cố và cách thức xử lý

<b>Loại sự cố/tấn công mạng</b>	<b>Số lượng</b>	<b>Số sự cố tự xử lý</b>	<b>Số sự cố có sự hỗ trợ xử lý từ các tổ chức khác</b>	<b>Số sự cố có hỗ trợ xử lý từ tổ chức nước ngoài</b>	<b>Số sự cố đề nghị VNCERT hỗ trợ xử lý</b>	<b>Thiệt hại ước tính</b>
Từ chối dịch vụ						
Tấn công giả mạo						
Tấn công sử dụng mã độc						
Truy cập trái phép, chiếm quyền điều khiển						
Thay đổi giao diện						
Mã hóa phần mềm, dữ liệu, thiết bị						
Phá hoại thông tin, dữ liệu, phần mềm						
Nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu						
Tấn công tổng hợp sử dụng kết hợp nhiều hình thức						
Các hình thức tấn công khác						
<b>Tổng số:</b>						

2. Danh sách các tổ chức hỗ trợ xử lý sự cố

.....

3. Danh sách các tổ chức nước ngoài hỗ trợ xử lý sự cố

.....

4. Đề xuất kiến nghị.....

....., ngày .... tháng .... năm .....

**NGƯỜI ĐẠI DIỆN THEO PHÁP LUẬT**  
(Ký tên, đóng dấu)