UỶ BAN NHÂN DÂN **TỈNH VĨNH PHÚC**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**
Số: 33 /2023/QĐ-UBND	*Vĩnh Phúc, ngày 12 tháng 9 năm 2023*

QUYẾT ĐỊNH

Ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước tỉnh Vĩnh Phúc

ỦY BAN NHÂN DÂN TỈNH VĨNH PHÚC

Căn cứ Luật Tổ chức chính quyền địa phương ngày 19 tháng 6 năm 2015 và 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 16 tháng 6 năm 2018;

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

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 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;

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 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 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Thông báo số 180/TB-UBND, ngày 28/8/2023 Về Kết qủa phiên họp UBND tỉnh tháng 8 năm 2023;

Theo đề nghị của Giám đốc Sở Thông tin và Truyền thông tại Tờ trình số 65/TTr-STTTT, ngày 25 tháng 7 năm 2023; Báo cáo thẩm định số 198/BC-STP ngày 12/7/2023 của Sở Tư pháp.

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 của cơ quan nhà nước tỉnh Vĩnh Phúc.

Điều 2. Quyết định này có hiệu lực từ ngày 01 tháng 10 năm 2023 và thay thế Quyết định số 31/2018/QĐ-UBND ngày 17 tháng 12 năm 2018 của UBND tỉnh ban hành Quy chế bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước tỉnh Vĩnh Phúc.

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 và các cá nhân, đơn vị liên quan có trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- *Văn phòng Chính phủ (B/c);*
- *Bộ Thông tin và Truyền thông;*
- *Cục KTVBQPPL - Bộ Tư pháp;*
- *TTTU, HĐND, Đoàn ĐBQH tỉnh;*
- *Chủ tịch, các PCT UBND;*
- *CPVP UBND;*
- *Như Điều 3;*
- *UB MTTQ, các tổ chức đoàn thể;*
- *Báo Vĩnh Phúc, Đài PTTH , Cổng TT-GTĐT;*
- *Trung tâm Tin học - Công báo tỉnh;*
- *Lưu: VT, VX3.(H- b)*

TM.ỦY BAN NHÂN DÂN
KT.CHỦ TỊCH
PHÓ CHỦ TỊCH

Vũ Chí Giang

UỶ BAN NHÂN DÂN **TỈNH VĨNH PHÚC**	**CỘNG HÒA 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 của các cơ quan nhà nước tỉnh Vĩnh Phúc

(Ban hành kèm theo Quyết định số 33 /2023/QĐ-UBND ngày 12 tháng 9 năm 2023 của Ủy ban nhân dân tỉnh Vĩnh Phúc)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng

1. Phạm vi điều chỉnh:

Quy chế này quy định về bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước tỉnh Vĩnh Phúc (sau đây gọi là các cơ quan).

2. Đối tượng áp dụng:

a) Quy chế này được áp dụng đối với các cơ quan nhà nước tỉnh Vĩnh Phúc và các tổ chức, cá nhân liên quan đến hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước tỉnh Vĩnh Phúc.

b) Khuyến khích các tổ chức, doanh nghiệp, cá nhân khác trên địa bàn tỉnh thực hiện Quy chế này.

Điều 2. Giải thích từ ngữ

Trong Quy chế này, các từ ngữ dưới đây được hiểu như sau:

1. *An toàn thông tin mạng* được quy định tại Khoản 1 Điều 3 Luật An toàn thông tin mạng số 86/2015/QH13 ngày 19 tháng 11 năm 2015.

2. *Hệ thống thông tin* được quy định tại Khoản 3 Điều 3 Luật An toàn thông tin mạng.

3. *Hạ tầng kỹ thuật* được quy dịnh tại Khoản 7 Điều 3 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.

4. *Phần mềm độc hại* (mã độc) được quy định tại Khoản 11 Điều 3 Luật An toàn thông tin mạng.

5. *Đơn vị vận hành hệ thống thông tin* được quy định tại Khoản 3 Điều 3 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 (sau đây gọi tắt là Nghị định số 85/2016/NĐ-CP).

6. *Giám sát an toàn hệ thống thông tin* được quy định tại Khoản 1 Điều 24 Luật An toàn thông tin mạng.

7. *Sự cố an toàn thông tin mạng* được quy định tại Khoản 7 Điều 3 Luật An toàn thông tin mạng.

8. *Ứng cứu sự cố an toàn thông tin mạng* được quy định tại Khoản 2 Điều 2 Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 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.

9. *Mật khẩu mạnh* là mật khẩu có độ dài tối thiểu 10 ký tự, trong đó kết hợp bao gồm ký tự hoa, thường, chữ số và ký tự đặc biệt.

Điều 3. Nguyên tắc bảo đảm an toàn thông tin mạng

Bảo đảm an toàn, an ninh thông tin mạng tuân thủ các nguyên tắc chung quy định tại Điều 4 Luật An toàn thông tin mạng và Điều 4 Nghị định số 85/2016/NĐ-CP.

Điều 4. Các hành vi bị cấm

Các hành vi bị cấm được quy định tại Điều 7, Luật An toàn thông tin mạng và Điều 8, Luật An ninh mạng số 24/2018/QH14 ngày 12 tháng 6 năm 2018.

Chương II
AN TOÀN THÔNG MẠNG TIN TRONG THIẾT KẾ, XÂY DỰNG, VẬN HÀNH HỆ THỐNG THÔNG TIN

Điều 5. An toàn thông tin trong thiết kế, xây dựng mới hệ thống thông tin

1. Các hoạt động liên quan đến xây dựng mới, nâng cấp, mở rộng hệ thống thông tin phải thực hiện xác định cấp độ và phương án bảo đảm an toàn thông tin theo quy định tại Nghị định số 85/2016/NĐ-CP và 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 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

2. Thiết kế, xây dựng các giải pháp bảo đảm an toàn thông tin phải tuân thủ nguyên tắc đồng bộ, có thể dùng chung, chia sẻ để tối ưu hiệu năng thiết bị và hiệu quả đầu tư.

3. Trước khi đưa vào vận hành, khai thác hệ thống thông tin, đơn vị được giao chủ đầu tư phải phối hợp với tổ chức chuyên môn có đủ năng lực, được cơ

quan có thẩm quyền cấp phép thực hiện đánh giá, kiểm định an toàn thông tin mạng. Tổ chức hiệu chỉnh theo kết quả đánh giá, kiểm định để hạn chế, phòng ngừa rủi ro, nguy cơ xảy ra mất an toàn thông tin mạng.

Điều 6. An toàn thông tin mạng đối với thuê dịch vụ công nghệ thông tin

1. Khi ký kết hợp đồng thuê dịch vụ công nghệ thông tin, cơ quan chủ trì thuê dịch vụ phải xác định rõ phạm vi, trách nhiệm, quyền hạn và nghĩa vụ của các bên về bảo đảm an toàn thông tin mạng, điều kiện xử lý vi phạm quy định bảo đảm an toàn thông tin mạng và trách nhiệm bồi thường thiệt hại do hành vi vi phạm của bên cung cấp dịch vụ gây ra.

2. Trong quá trình sử dụng dịch vụ công nghệ thông tin, cơ quan chủ trì thuê dịch vụ có trách nhiệm:

a) Yêu cầu bên cung cấp dịch vụ phải bảo mật thông tin, dữ liệu, mã nguồn, tài liệu thiết kế hệ thống thông tin; triển khai các biện pháp bảo đảm an toàn thông tin mạng tuân thủ phương án bảo đảm an toàn thông tin được cấp có thẩm quyền phê duyệt, các quy định tại Quy chế này, Luật An toàn thông tin mạng và các quy định khác của pháp luật có liên quan;

b) Quản lý thông tin, dữ liệu phát sinh từ dịch vụ đã thuê; bảo đảm bên cung cấp dịch vụ không được truy cập để quản trị dữ liệu thuộc phạm vi nhà nước quản lý lưu trữ trên hệ thống thuê;

c) Giám sát, giới hạn quyền của bên cung cấp dịch vụ khi cho phép truy cập vào hệ thống thông tin để xử lý sự cố hoặc hỗ trợ nâng cấp, quản trị, vận hành.

3. Khi phát hiện bên cung cấp dịch vụ có dấu hiệu vi phạm quy định bảo đảm an toàn thông tin mạng, cơ quan chủ trì thuê dịch vụ có trách nhiệm:

a) Tạm dừng hoặc đình chỉ hoạt động của hệ thống thông tin tùy theo mức độ vi phạm và thông báo cho bên cung cấp dịch vụ;

b) Thu hồi quyền truy cập hệ thống thông tin đã cấp cho bên cung cấp dịch vụ (nếu có);

c) Kiểm tra, xác định, mức độ vi phạm và thiệt hại xảy ra; thông báo cho bên cung cấp dịch vụ; tiến hành các thủ tục xử lý vi phạm và bồi thường thiệt hại hoặc xử lý theo các quy định của pháp luật.

4. Kết thúc thời gian thuê dịch vụ, cơ quan chủ trì thuê dịch vụ có trách nhiệm:

a) Yêu cầu bên cung cấp dịch vụ chuyển giao đầy đủ thông tin, dữ liệu và các công cụ cần thiết để bảo đảm có thể khai thác sử dụng được thông tin, dữ liệu kể cả trong trường hợp thay đổi bên cung cấp dịch vụ.

b) Thu hồi và thay đổi mật khẩu hoặc hủy bỏ tài khoản truy cập hệ thống thông tin đã cấp cho bên cung cấp dịch vụ;

Điều 7. Giám sát an toàn hệ thống thông tin

1. Đối với các hệ thống thông tin được lưu ký tại các trung tâm dữ liệu của các doanh nghiệp hoặc sử dụng máy chủ riêng đặt tại trụ sở, cơ quan chủ đầu tư hệ thống thông tin có trách nhiệm tự tổ chức giám sát an toàn hệ thống thông tin.

2. Đối với các hệ thống thông tin lưu ký tại Trung tâm dữ liệu tỉnh:

a) Trường hợp hệ thống thông tin do các cơ quan thực hiện đầu tư, có sử dụng máy chủ riêng hoặc sử dụng hạ tầng kỹ thuật dùng chung của tỉnh, Sở Thông tin và Truyền thông có trách nhiệm tổ chức giám sát an toàn hệ thống thông tin. Cơ quan chủ đầu tư có trách nhiệm bảo đảm an toàn thông tin cho hạ tầng máy chủ, phần mềm cài đặt trên máy chủ; Sở Thông tin và Truyền thông có trách nhiệm tổ chức bảo đảm an toàn thông tin cho hạ tầng mạng, bảo mật và các nền tảng dùng chung.

b) Trường hợp hệ thống thông tin do các cơ quan thuê dịch vụ công nghệ thông tin, có sử dụng hạ tầng kỹ thuật dùng chung của tỉnh, Sở Thông tin và Truyền thông có trách nhiệm tổ chức giám sát an toàn hệ thống thông tin. Cơ quan chủ trì thuê dịch vụ phối hợp với đơn vị cung cấp dịch vụ cho thuê có trách nhiệm bảo đảm an toàn thông tin cho hạ tầng máy chủ, phần mềm cài đặt trên máy chủ; Sở Thông tin và Truyền thông có trách nhiệm tổ chức bảo đảm an toàn thông tin cho hạ tầng mạng, bảo mật và các nền tảng dùng chung.

Điều 8. Kiểm tra, đánh giá an toàn thông tin mạng

1. Trong quá trình vận hành hệ thống thông tin, các cơ quan, đơn vị vận hành hệ thống thông tin có trách nhiệm tổ chức kiểm tra, đánh giá an toàn thông tin mạng đối với hệ thống thông tin do cơ quan mình quản lý.

2. Nội dung, tần suất kiểm tra đánh giá thực hiện theo Điều 11, Điều 12 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 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

3. Việc kiểm tra, đánh giá an toàn thông tin mạng phải do tổ chức chuyên môn được cơ quan có thẩm quyền cấp phép; tổ chức sự nghiệp nhà nước có chức năng, nhiệm vụ phù hợp hoặc do tổ chức chuyên môn được cấp có thẩm quyền chỉ định thực hiện.

Điều 9. Xử lý rủi ro an toàn thông tin

Trên cơ sở báo cáo kết quả kiểm tra, đánh giá an toàn thông tin mạng hoặc cảnh báo nguy cơ gây mất an toàn thông tin mạng từ Sở Thông tin và Truyền thông hoặc các cơ quan có thẩm quyền khác, Đơn vị vận hành hệ thống thông tin có trách nhiệm tự khắc phục hoặc lựa chọn đơn vị đủ năng lực để triển khai

các phương án khắc phục. Kết thúc xử lý, báo cáo kết quả thực hiện về Sở Thông tin và Truyền thông để theo dõi, tổng hợp.

Điều 10. Ứng cứu xử lý sự cố an toàn thông tin mạng

1. Nguyên tắc ứng cứu xử lý sự cố:

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

b) Phối hợp chặt chẽ, tuân thủ quy định của pháp luật về điều phối ứng cứu sự cố an toàn thông tin mạng.

c) Ưu tiên ứng cứu, xử lý sự cố bằng lực lượng tại chỗ và trách nhiệm chính của Đơn vị vận hành hệ thống thông tin.

d) Việc xử lý sự cố an toàn thông tin mạng phải bảo đảm quyền và lợi ích hợp pháp của cơ quan, cá nhân; bảo mật thông tin cá nhân, thông tin riêng của cơ quan khi tham gia các hoạt động ứng cứu xử lý sự cố.

2. Phân loại sự cố an toàn thông tin mạng:

a) Sự cố do bị tấn công mạng: tấn công từ chối dịch vụ; tấn công giả mạo; tấn công sử dụng mã độc; tấn công truy cập trái phép, chiếm quyền điều khiển; tấn công thay đổi giao diện; tấn công mã hóa phần mềm, dữ liệu, thiết bị; tấn công phá hoại thông tin, dữ liệu, phần mềm; tấn công nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu; các hình thức tấn công khác.

b) Sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật.

c) Sự cố do lỗi của cán bộ quản trị, vận hành hệ thống.

d) Sự cố do các thảm họa tự nhiên.

3. Phân loại mức độ sự cố:

a) Thấp: Sự cố gây ảnh hưởng cá nhân và không làm gián đoạn hay đình trệ hoạt động chính của cơ quan.

b) Trung bình: Sự cố ảnh hưởng đến một nhóm người dùng nhưng không gây gián đoạn hay đình trệ hoạt động chính của cơ quan.

c) Cao: Sự cố tác động đến khả năng vận hành của hệ thống thông tin, ảnh hưởng đến dữ liệu, thiết bị, gây ảnh hưởng đến hoạt động chung của cơ quan và hoạt động cung cấp dịch vụ công cho người dân, doanh nghiệp.

d) Nghiêm trọng: Sự cố gây gián đoạn hoặc đình trệ hệ thống trong một khoảng thời gian ngắn, ảnh hưởng nghiêm trọng đến dữ liệu, thiết bị của hệ thống, gây thiệt hại nghiêm trọng cho cơ quan, người dân, doanh nghiệp.

đ) Đặc biệt nghiêm trọng: Sự cố làm tê liệt toàn bộ hoạt động của hệ thống, gây thiệt hại đặc biệt nghiêm trọng cho cơ quan, người dân, doanh nghiệp, đe dọa trật tự an toàn xã hội.

2. Quy trình ứng cứu sự cố thực hiện theo Điều 11 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. Báo cáo ban đầu sự cố và Báo cáo hoàn thành xử lý sự cố khi thực hiện quy trình ứng cứu sự cố được thực hiện theo Mẫu số 01 và Mẫu số 02 tại Phụ lục kèm theo Quy chế này.

3. Trường hợp có sự cố nghiêm trọng ở mức độ cao trở lên hoặc vượt quá khả năng khắc phục của đơn vị, lãnh đạo đơn vị phải báo cáo khẩn cấp cho cơ quan cấp trên quản lý trực tiếp và Sở Thông tin và Truyền thông để được hướng dẫn, hỗ trợ hoặc điều phối ứng cứu sự cố an toàn thông tin mạng.

4. Quá trình xử lý sự cố phải được ghi chép và lưu trữ tại đơn vị; bảo toàn bằng chứng, chứng cứ phục vụ cho việc kiểm tra, xử lý, khắc phục và phòng ngừa sự cố. Trong trường hợp sự cố có liên quan đến các vi phạm pháp luật, đơn vị có trách nhiệm thu thập và cung cấp chứng cứ cho cơ quan có thẩm quyền theo quy định của pháp luật.

Điều 11. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ

Hệ thống thông tin khi kết thúc vận hành, khai thác hoặc thanh lý, hủy bỏ phải tuân thủ các quy định của pháp luật về quản lý tài sản. Thông tin, dữ liệu trên các hệ thống thông tin phải được sao lưu và chuyển sang các hệ thống khác (nếu còn giá trị sử dụng). Thực hiện các biện pháp xóa, hủy dữ liệu trước khi thanh lý, thanh hủy tài sản.

Chương III
BIỆN PHÁP BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Điều 12. Bảo đảm an toàn vật lý và môi trường

1. Các khu vực xử lý, lưu trữ thông tin, phương tiện xử lý thông tin, phương tiện bảo đảm an toàn thông tin mạng phải được đặt ở vị trí an toàn, bảo vệ bằng tường bao và kiểm soát ra vào, bảo đảm chỉ có người có nhiệm vụ mới được vào và phải có nội quy riêng khi làm việc trong các khu vực này.

2. Các khu vực tại Khoản 1 Điều này phải có biện pháp bảo vệ phòng chống cháy nổ, ngập lụt, động đất, chống sét, tác động của môi trường và các thảm họa khác do thiên nhiên và con người gây ra.

3. Bảo đảm thiết bị lưu trữ dữ liệu quan trọng, phần mềm bản quyền lưu trữ trên thiết bị phải được kiểm tra, xóa hoặc ghi đè không có khả năng khôi phục trước khi loại bỏ hoặc tái sử dụng cho mục đích khác.

Điều 13. Quản lý an toàn hạ tầng mạng

1. An toàn cho mạng nội bộ:

a) Phải sử dụng thiết bị tường lửa chuyên dụng hoặc phần mềm tường lửa để ngăn chặn và phát hiện xâm nhập trái phép vào mạng nội bộ của cơ quan khi kết nối với hệ thống bên ngoài.

b) Khi kết nối từ xa vào mạng nội bộ, phải sử dụng giao thức mạng có mã hóa thông tin và thiết lập mật khẩu mạnh.

2. Mạng không dây để kết nối với mạng nội bộ phải thiết lập mật khẩu mạnh, mã hóa dữ liệu theo cơ chế bảo mật WPA2 hoặc WPA3. Mật khẩu truy cập phải được thay đổi định kỳ 06 tháng/lần.

3. Hệ điều hành, phần mềm tích hợp trên các thiết bị mạng phải thường xuyên được cập nhật các bản vá lỗi theo khuyến nghị của các nhà sản xuất.

4. Phải lưu trữ nhật ký khi thay đổi cấu hình kỹ thuật của các thiết bị mạng.

Điều 14. Quản lý an toàn máy chủ và ứng dụng

1. Quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ:

a) Máy chủ phải được cài đặt, sử dụng phần mềm phòng chống mã độc Phần mềm phòng chống mã độc được cập nhật thường xuyên và phải có tính năng kỹ thuật đáp ứng yêu cầu của Bộ Thông tin và Truyền thông.

b) Bảo đảm cho hệ điều hành, phần mềm cài đặt trên máy chủ hoạt động liên tục, ổn định và an toàn.

c) Thiết lập chế độ tự động cập nhật bản vá hệ điều hành, phần mềm, ứng dụng và hệ quản trị cơ sở dữ liệu được cài đặt trên máy chủ, phải thiết lập mật khẩu truy nhập chế độ tự động bảo vệ màn hình sau 10 phút không sử dụng đối với tất cả máy chủ.

d) Thay đổi các tài khoản, mật khẩu mặc định ngay khi đưa hệ điều hành, phần mềm vào sử dụng.

đ) Thường xuyên kiểm tra cấu hình, các tệp tin nhật ký hoạt động của hệ điều hành, phần mềm nhằm kịp thời phát hiện và xử lý những sự cố nếu có.

e) Thường xuyên cập nhật các bản vá lỗi hệ điều hành, phần mềm từ nhà cung cấp.

g) Loại bỏ các thành phần của hệ điều hành, phần mềm không cần thiết hoặc không còn nhu cầu sử dụng.

h) Bảo đảm các kết nối mạng trên máy chủ hoạt động liên tục, ổn định và an toàn. Cấu hình, kiểm soát các kết nối, các cổng dịch vụ từ bên trong đi ra, bên ngoài đi vào hệ thống.

i) Tất cả máy chủ, thiết bị công nghệ thông tin không được kết nối với Internet trừ trường hợp bắt buộc.

2. Cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống trước khi đưa vào vận hành, khai thác:

a) Xây dựng, áp dụng quy trình cấu hình tối ưu, tăng cường bảo mật cho các máy chủ.

b) Máy chủ phải được rà soát, cấu hình tối ưu, tăng cường bảo mật trước khi đưa hệ thống vào vận hành khai thác.

3. Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố:

a) Triển khai hệ thống/phương tiện lưu trữ độc lập với hệ thống lưu trữ trên các máy chủ dịch vụ để sao lưu dự phòng; phân loại và quản lý thông tin, dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau; thực hiện sao lưu, dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

b) Phải thực hiện lưu trữ thay đổi cấu hình kỹ thuật của máy chủ, hệ điều hành, phần mềm.

4. Nghiêm cấm sử dụng các tài nguyên tính toán, gồm: các máy chủ và các cổng dịch vụ môi trường mạng để xây dựng các hệ thống thực hiện các hành vi đào tiền ảo, rà quét các lỗ hổng bảo mật, hoặc tham gia các hoạt động bất hợp pháp khác trên môi trường mạng.

Điều 15. Bảo đảm an toàn dữ liệu

1. Quản lý tài khoản truy cập:

a) Khi cấp tài khoản lần đầu cho người dùng, đơn vị vận hành hệ thống thông tin phải thông báo cho người dùng. Người dùng có trách nhiệm thay đổi mật khẩu sau khi đăng nhập thành công lần đầu. Chậm nhất là 03 ngày, các tài khoản không tuân thủ việc thay đổi mật khẩu phải được tự động vô hiệu hóa.

b) Các hệ thống thông tin phải thiết lập giới hạn số lần đăng nhập không hợp lệ tối đa không quá 05 lần; tự động kết thúc phiên làm việc nếu quá 30 phút người dùng không tương tác với hệ thống.

c) Khi cá nhân thay đổi vị trí công tác, chuyển công tác, thôi việc, nghỉ hưu, đơn vị quản lý cá nhân đó phải thông báo cho đơn vị vận hành hệ thống thông tin để điều chỉnh, thu hồi hoặc hủy bỏ tài khoản.

d) Không thiết lập cùng một mật khẩu cho nhiều tài khoản quản trị của hệ thống thông tin.

đ) Tài khoản quản trị, tài khoản người dùng phải được rà soát hàng năm, đảm bảo các tài khoản và quyền truy cập hệ thống được cấp phát đúng. Các tài khoản không sử dụng trong thời gian 01 năm phải bị khóa hoặc xóa bỏ.

e) Không sử dụng tài khoản thư điện tử công vụ (***@vinhphuc.gov.vn) để giao dịch, đăng ký trên mạng xã hội và hệ thống thông tin công cộng.

2. Tên miền (***.vinhphuc.gov.vn) khi không còn sử dụng, các cơ quan phải có văn bản đề nghị thu hồi tên miền.

3. Các hệ thống thông tin lưu ký tại các nhà cung cấp dịch vụ khi không còn sử dụng, phải thực hiện lưu trữ dữ liệu ra thiết bị lưu trữ ngoài và yêu cầu đơn vị cung cấp dịch vụ lưu ký xóa hoàn toàn dữ liệu trên các máy chủ.

4. Khi chia sẻ tài nguyên trên máy chủ hoặc máy trạm phải sử dụng mật khẩu để bảo vệ thông tin, dữ liệu; không thiết lập chế độ chia sẻ toàn bộ ổ cứng; kết thúc chia sẻ tài nguyên khi hoàn thành.

5. Khi bảo hành, bảo dưỡng, sửa chữa máy chủ, máy trạm, thiết bị công nghệ thông tin bên ngoài cơ quan, phải tháo bỏ bộ phận lưu trữ dữ liệu khỏi thiết bị để lại cơ quan, hoặc phá hủy dữ liệu lưu trữ trên thiết bị.

6. Quản lý sao lưu dự phòng:

a) Lập danh sách hệ thống thông tin theo mức độ quan trọng cần được sao lưu kèm tần suất sao lưu, phương pháp sao lưu, thời gian lưu trữ và thời gian kiểm tra phục hồi hệ thống từ dữ liệu sao lưu.

b) Dữ liệu của các hệ thống thông tin phải có phương án sao lưu phù hợp với tần suất thay đổi của dữ liệu.

c) Đối với các hệ thống thông tin cấp độ 3 trở lên, dữ liệu sao lưu phải được lưu trữ ra phương tiện lưu trữ ngoài; kiểm tra, phục hồi dữ liệu sao lưu từ phương tiện lưu trữ ngoài tối thiểu 01 lần/năm.

Điều 16. Bảo đảm an toàn thiết bị và người dùng đầu cuối

1. Máy tính cá nhân phải đặt mật khẩu truy cập và chế độ tự động bảo vệ màn hình sau 10 phút không sử dụng; thường xuyên cập nhật bản vá lỗ hổng bảo mật hệ điều hành và phần mềm ứng dụng; cài đặt phần mềm phòng chống mã độc và thiết lập chế độ tự động cập nhật mẫu mã độc mới, tự động rà quét khi sao chép, mở các tập tin. Phần mềm phòng chống mã độc phải có tính năng kỹ thuật đáp ứng yêu cầu của Bộ Thông tin và Truyền thông.

2. Khi sử dụng máy tính, thiết bị đầu cuối trong mạng nội bộ cơ quan để xử lý công việc mang tính chất công vụ phải tuân thủ các quy định sau:

a) Không cài đặt các phần mềm không rõ nguồn gốc, không liên quan đến công việc chuyên môn trên máy tính của cơ quan.

b) Cán bộ, công chức, viên chức và người lao động phải tự đặt mật khẩu đăng nhập vào các hệ thống thông tin; thường xuyên thay đổi để tăng cường công tác bảo mật.

c) Không tự ý gỡ bỏ phần mềm phòng chống mã độc trên máy tính. Tất cả các tập tin, thư mục khi sao chép vào máy tính từ thiết bị ngoại vi phải được quét mã độc trước khi thực hiện.

d) Chỉ sử dụng thư điện tử công vụ để trao đổi, gửi, nhận tài liệu công vụ.

e) Khi phát hiện dấu hiệu máy tính nhiễm mã độc phải kịp thời thông báo cho bộ phận có trách nhiệm của cơ quan để xử lý.

3. Cá nhân khi mang máy tính, thiết bị di động thuộc sở hữu riêng kết nối với mạng nội bộ để xử lý công việc phải được sự đồng ý của thủ trưởng cơ quan và tuân thủ các quy định tại Khoản 1, Khoản 2 Điều này.

4. Chấm dứt hoặc thay đổi công việc:

a) Cán bộ, công chức, viên chức, người lao động nghỉ việc hoặc thay đổi công việc phải thu hồi các tài khoản, quyền truy cập hệ thống, thiết bị phần cứng, phần mềm và các tài sản công nghệ thông tin khác thuộc sở hữu của cơ quan.

b) Cơ quan có cán bộ, công chức, viên chức, người lao động xin nghỉ việc có trách nhiệm chủ trì, phối hợp với Đơn vị vận hành hệ thống thông tin thu hồi tài khoản, vô hiệu hóa các quyền truy hệ thống. Thời gian thu hồi chậm nhất tối đa sau 05 ngày làm việc.

Chương IV
TRÁCH NHIỆM BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Điều 17. 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 tham mưu bảo đảm an toàn thông tin mạng cho các hệ thống thông tin của tỉnh.

2. Chỉ đạo, tổ chức bảo đảm an toàn thông tin mạng cho hạ tầng kỹ thuật của Trung tâm dữ liệu tỉnh.

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 công nghệ thông tin của cơ quan nhà nước trên địa bàn tỉnh theo quy định.

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

5. Định kỳ tổ chức diễn tập ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh, tham gia diễn tập quốc gia và quốc tế do Bộ Thông tin và Truyền thông tổ chức.

6. Chỉ đạo, hướng dẫn về nghiệp vụ về bảo đảm an toàn thông tin mạng; hỗ trợ giải quyết sự cố khi có yêu cầu.

7. Chủ trì, phối hợp với các cơ quan 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.

8. 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.

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

Điều 18. 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 phòng ngừa, đấu tranh, ngăn chặn 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 thông tin mạng trong cơ quan nhà nước trên địa bàn tỉnh.

2. Kịp thời thông báo các phương thức, thủ đoạn mới của các loại tội phạm công nghệ cao; chịu trách nhiệm quản lý, phòng ngừa, đấu tranh, ngăn chặn các loại tội phạm lợi dụng hệ thống mạng gây hại đến an toàn thông tin mạng của cơ quan, cá nhân.

3. Phối hợp với Sở Thông tin và Truyền thông trong công tác thanh tra, kiểm tra về an toàn thông tin mạng.

4. Chủ trì, phối hợp với các cơ quan, đơn vị có liên quan điều tra và xử lý các trường hợp vi phạm an toàn thông tin mạng theo thẩm quyền và theo quy định của pháp luật.

Điều 19. Trách nhiệm của các cơ quan

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 Ủy ban nhân dân tỉnh trong công tác bảo đảm an toàn thông tin mạng của đơn vị mình.

2. Thực hiện trách nhiệm của đơn vị vận hành hệ thống thông tin theo quy định tại Khoản 1 Điều 21 Quy chế này.

3. 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; xác định các yêu cầu, trách nhiệm đảm bảo an toàn thông tin mạng đối với các vị trí cần tuyển dụng hoặc phân công.

4. Ban hành quy chế nội bộ về bảo đảm an toàn thông tin mạng phù hợp với Quy chế này và các quy định của pháp luật.

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 06 tháng (trước ngày 15/7) và hàng năm (trước ngày 15/01 năm tiếp theo) báo cáo tình hình an toàn thông tin mạng của cơ quan theo Mẫu số 03 tại Phụ lục kèm theo Quy chế này, gửi Sở Thông tin và Truyền thông tổng hợp, báo cáo Ủy ban nhân dân tỉnh.

Điều 20. Trách nhiệm của đơn vị vận hành hệ thống thông tin

1. Trách nhiệm của các cơ quan, đơn vị được cấp có thẩm quyền giao vận hành hệ thống thông tin:

a) Thực hiện xác định cấp độ an toàn hệ thống thông tin theo quy định tại Điều 14 Nghị định số 85/2016/NĐ-CP.

b) Thực hiện bảo vệ hệ thống thông tin theo Quy chế này, các quy định của pháp luật và hướng dẫn, tiêu chuẩn, quy chuẩn an toàn thông tin.

c) Định kỳ đánh giá hiệu quả của các biện pháp bảo đảm an toàn thông tin mạng, báo cáo Ủy ban nhân dân tỉnh Điều chỉnh nếu cần thiết.

d) Định kỳ hoặc đột xuất báo cáo công tác thực thi bảo đảm an toàn hệ thống thông tin theo yêu cầu của Ủy ban nhân dân tỉnh hoặc cơ quan quản lý nhà nước chuyên ngành có thẩm quyền.

đ) Phối hợp, thực hiện theo yêu cầu của cơ quan chức năng liên quan của Bộ Thông tin và Truyền thông trong công tác bảo đảm an toàn thông tin.

e) Kịp thời thông báo sự cố an toàn thông tin mạng và phối hợp ứng cứu xử lý sự cố an toàn thông tin mạng với các cơ quan, đơn vị liên quan.

2. Trường hợp hệ thống thông tin do các cơ quan thực hiện đầu tư: Cơ quan chủ đầu tư đóng vai trò là Đơn vị vận hành hệ thống thông tin thực hiện các quy định tại Khoản 1 Điều này.

3. Trường hợp hệ thống thông tin do các cơ quan thực hiện thuê dịch vụ công nghệ thông tin (đã có hợp đồng thuê): Đơn vị cung cấp dịch vụ đóng vai trò là Đơn vị vận hành hệ thống thông tin, có trách nhiệm thực hiện các quy định tại Khoản 1 Điều này; phối hợp chặt chẽ với cơ quan chủ trì thuê dịch vụ trong quá trình thực hiện; tổng hợp báo cáo Ủy ban nhân dân tỉnh hoặc cơ quan nhà nước có thẩm quyền thông qua đơn vị chủ trì thuê dịch vụ.

Điều 21. Trách nhiệm của đơn vị vận hành Trung tâm dữ liệu tỉnh

1. Giám sát an toàn thông tin mạng cho các hệ thống thông tin lưu ký tại Trung tâm dữ liệu tỉnh; trực tiếp bảo đảm an toàn thông tin mạng cho hạ tầng kỹ thuật Trung tâm dữ liệu tỉnh.

2. Thực hiện trách nhiệm của đơn vị vận hành hệ thống thông tin theo quy định tại Khoản 1 Điều 21 Quy chế này.

3. Thường xuyên cập nhật các nguy cơ gây mất an toàn thông tin mạng và thông báo cho các cơ quan, đơn vị biết để có biện pháp phòng ngừa, ngăn chặn, xử lý kịp thời.

4. Là đầu mối để tiếp nhận điều phối ứng cứu các sự cố mất an toàn thông tin mạng của tỉnh.

Điều 22. Trách nhiệm của cán bộ, công chức, viên chức và người lao động

1. Trách nhiệm của cán bộ, công chức, viên chức và người lao động:

a) Chấp hành Quy chế này, quy chế nội bộ của cơ quan và các quy định 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) Cán bộ, công chức, viên chức và người lao động có trách nhiệm tự quản lý, bảo quản, bảo đảm an toàn thông tin mạng cho tài khoản, các thiết bị mà mình được giao sử dụng;

c) Khi phát hiện sự cố mất an toàn thông tin mạng phải thông báo ngay với cấp trên và cán bộ chuyên trách, phụ trách công nghệ thông tin hoặc phụ trách an toàn thông tin của cơ quan để kịp thời ngăn chặn, xử lý;

d) Tham gia nghiêm túc các chương trình đào tạo, tập huấn về an toàn thông tin mạng do Ủy ban nhân dân tỉnh chỉ đạo hoặc cơ quan chuyên trách về an toàn thông tin mạng tổ chức.

2. Trách nhiệm của cán bộ phụ trách công nghệ thông tin/an toàn thông tin:

Ngoài các quy định tại Khoản 1 Điều này, cán bộ phụ trách công nghệ thông tin/an toàn thông tin có trách nhiệm

a) Chủ trì tham mưu với lãnh đạo cơ quan thực hiện các quy định của Quy chế này và các quy định pháp luật có liên quan đến an toàn thông tin mạng;

b) Tham mưu lãnh đạo cơ quan ban hành các quy định nội bộ và triển khai các giải pháp kỹ thuật bảo đảm an toàn thông tin mạng;

c) Trực tiếp thiết lập hoặc tham mưu các biện pháp kỹ thuật bảo đảm an toàn cho hạ tầng kỹ thuật, hệ thống thông tin trong cơ quan, đơn vị mình; hướng dẫn cán bộ, công chức, viên chức và người lao động trong cơ quan, đơn vị tuân thủ các biện pháp bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin;

d) Thực hiện việc giám sát, đánh giá, ghi nhật ký và báo cáo ngay thủ trưởng cơ quan các sự cố mất an toàn thông tin mạng và mức độ nghiêm trọng của các sự cố đó;

đ) Phối hợp với cá nhân, đơn vị có liên quan trong việc kiểm soát, phát hiện và khắc phục các sự cố an toàn thông tin mạng.

Chương V
TỔ CHỨC THỰC HIỆN

Điều 23. Trách nhiệm tổ chức thực hiện

Thủ trưởng sở, ban, ngành, Chủ tịch Ủy ban nhân dân các huyện, thành phố, tổ chức triển khai Quy chế này tại cơ quan, đơn vị, địa phương mình.

Điều 24. Trách nhiệm của Sở Tài chính, Sở Kế hoạch và Đầu tư

Sở Tài chính, Sở Kế hoạch và Đầu tư phối hợp tham mưu, đề xuất với Ủy ban nhân dân tỉnh ưu tiên bố trí kinh phí để thực hiện các nhiệm vụ bảo đảm an toàn thông tin mạng của tỉnh; kịp thời tham mưu ủy ban nhân dân tỉnh bổ sung kinh phí ngoài dự toán khi phát sinh sự cố khẩn cấp, bảo đảm hệ thống nhanh chóng được khắc phục.

Điều 25. Sửa đổi, bổ sung

Trong quá trình thực hiện, nếu có những vấn đề cần sửa đổi, bổ sung, các đơn vị gửi về Sở Thông tin và Truyền thông để tổng hợp, báo cáo Ủy ban nhân dân tỉnh xem xét, quyết định./.

Phụ lục
DANH MỤC BIỂU MẪU

(Ban hành kèm theo Quyết định số: 33 /2023/QĐ-UBND ngày 12 tháng 9 năm 2023 của Ủy ban nhân dân tỉnh Vĩnh Phúc)

Mẫu số 01	Báo cáo ban đầu sự cố an toàn thông tin mạng
Mẫu số 02	Báo cáo hoàn thành xử lý sự cố an toàn thông tin mạng
Mẫu số 03	Báo cáo định kỳ tình hình an toàn thông tin mạng

(Mẫu số 01)

TÊN CƠ QUAN CHỦ QUẢN
TÊN CƠ QUAN
Số: ...../BC-

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc
Vĩnh Phúc, ngày ... tháng ... năm ...

BÁO CÁO BAN ĐẦU SỰ CỐ AN TOÀN THÔNG TIN MẠNG

THÔNG TIN VỀ TỔ CHỨC/CÁ NHÂN BÁO CÁO 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 (*):	*Điền tên đơn vị vận hành hoặc được thuê vận hành hệ thống thông tin*				
Cơ quan quản lý cấp trên:	*Điền tên cơ quan quản lý cấp trên*				
Tên hệ thống bị sự cố	*Điền tên hệ thống bị sự cố và tên miền, địa chỉ ip liên quan*				
Phân loại cấp độ của hệ thống thông tin, (nếu có)	☐ Cấp độ 1	☐ Cấp độ 2	☐ Cấp độ 3	☐ Cấp độ 4	☐ Cấp độ 5
Tổ chức cung cấp dịch vụ an toàn thông tin mạng (nếu có):	*Điền tên nhà cung cấp ở đây*				
Tên nhà cung cấp dịch vụ kết nối bên ngoài (nếu có)	*Điền tên nhà cung cấp ở đây*				
Dải địa chỉ Public IP kết nối với hệ thống bên ngoài:	*Điền thông tin ở đây*				
Mô tả sơ bộ về sự cố (*)					
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. Xác định mức độ nhạy cảm của thông tin liên quan hoặc những đối tượng bị ảnh hưởng bởi sự cố:					

Ngày phát hiện sự cố (*) .../.../..... (dd/mm/yy)	Thời điểm 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 *

☐ Sở Thông tin và Truyền thông

☐ ISP đang trực tiếp cung cấp dịch vụ

☐ Các cơ quan chuyên trách an toàn thông tin mạng khác

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 mạng 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 (IP public), 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)

Nơi nhận:
- Sở TT&TT;
- Lưu: VT,....

THỦ TRƯỞNG CƠ QUAN
(Ký số)

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

(Mẫu số 02)

TÊN CƠ QUAN CHỦ QUẢN
TÊN CƠ QUAN
Số: ...../BC-

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc
Vĩnh Phúc, ngày ... tháng ... năm ...

BÁO CÁO HOÀN THÀNH XỬ LÝ SỰ CỐ AN TOÀN THÔNG TIN MẠNG

THÔNG TIN VỀ TỔ CHỨC/CÁ NHÂN BÁO CÁO

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

VĂN BẢN BÁO CÁO BAN ĐẦU SỰ CỐ:

- Số ký hiệu ..... Ngày ban hành: .../.../.....

THÔNG TIN CHI TIẾT VỀ HỆ THỐNG BỊ SỰ CỐ

Tên đơn vị vận hành hệ thống thông tin (*):	*Điền tên đơn vị vận hành hoặc được thuê vận hành hệ thống thông tin*				
Cơ quan quản lý cấp trên:	*Điền tên cơ quan quản lý cấp trên*				
Tên hệ thống bị sự cố	*Điền tên hệ thống bị sự cố*				
Phân loại cấp độ của hệ thống thông tin, (nếu có)	☐ Cấp độ 1	☐ Cấp độ 2	☐ Cấp độ 3	☐ Cấp độ 4	☐ Cấp độ 5

Tên/Mô tả về sự cố
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. Xác định mức độ nhạy cảm của thông tin liên quan hoặc những đối tượng bị ảnh hưởng bởi sự cố. (Chỉ mô tả những cập nhật mới có thay đổi so với phần mô tả của văn bản thông báo sự cố đã gửi)

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.....)

Nơi nhận:
- Sở TT&TT;
- Lưu: VT,....

THỦ TRƯỞNG CƠ QUAN
(Ký số)

(Mẫu số 03)

TÊN CƠ QUAN CHỦ QUẢN **TÊN CƠ QUAN**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: ...../BC-	*Vĩnh Phúc, ngày ... tháng ... năm ...*

BÁO CÁO ĐỊNH KỲ TÌNH HÌNH AN TOÀN THÔNG TIN MẠNG

1. Về xây dựng chính sách và biện pháp quản lý an toàn thông tin mạng

a) Đã xây dựng Quy chế bảo đảm an toàn thông tin mạng nội bộ?

❍ Có (*ghi số hiệu văn bản)* ❍ Chưa

b) Đã xây dựng Kế hoạch ứng phó sự cố an toàn thông tin mạng thông thường?

❍ Có *(ghi số hiệu văn bản)* ❍ Không

c) Có bộ phận phụ trách an toàn thông tin mạng?

O Có O Không

Nếu có, bộ phận có người phụ trách là:

O Lãnh đạo cơ quan

O Chuyên viên chuyên trách công nghệ thông tin

O Khác: .....

d) Xác định cấp độ an toàn thông tin mạng

- Các hệ thống thông tin đã được phê duyệt cấp độ an toàn thông tin mạng (*liệt kê cụ thể tên hệ thống thông tin, quyết định phê duyệt cấp độ*):

- Các hệ thống thông tin chưa được phê duyệt cấp độ an toàn thông tin mạng (*liệt kê cụ thể tên hệ thống thông tin chưa được phê duyệt*):

đ) Triển khai phương án bảo đảm an toàn thông tin

- Các hệ thống thông tin đã được triển khai phương án bảo đảm an toàn thông tin theo cấp độ (*liệt kê cụ thể tên hệ thống thông tin*):

- Các hệ thống thông tin đã chưa triển khai phương án bảo đảm an toàn thông tin theo cấp độ (*liệt kê cụ thể tên hệ thống thông tin*):

e) Có hệ thống thông tin được lưu ký ngoài Trung tâm dữ liệu tỉnh Vĩnh Phúc?

O Có O Không

Nếu có, báo cáo các nội dung sau:

- Tên hệ thống thông tin:

- Đơn vị cung cấp dịch vụ lưu ký (*tên đơn vị, địa chỉ, số điện thoại*):

g) Có thực hiện kiểm định an toàn thông tin mạng đối với hệ thống thông tin mới được xây dựng trong năm?

O Có O Không

Nếu có, báo cáo các nội dung sau:

- Tên hệ thống thông tin:

- Đơn vị thực hiện kiểm định (*tên đơn vị, địa chỉ, số điện thoại*):

h) Có thực hiện kiểm tra, đánh giá an toàn thông tin mạng trong năm?

O Có O Không

Nếu có, báo cáo các nội dung sau:

- Tên hệ thống thông tin:
- Đơn vị thực hiện đánh giá (*tên đơn vị, địa chỉ, số điện thoại*):
- Các biện pháp đã triển khai xử lý điểm yếu an toàn thông tin:

i) Các công cụ bảo đảm an toàn thông tin mạng đang thực hiện

Công cụ	Tên/phiên bản	Năm đưa vào sử dụng	Mô tả nội dung
1. Phần mềm phòng chống mã độc (antivirus)			
2. Tường lửa			
3. Công cụ mã hóa tập tin			
4. Chữ ký số			
5. Mạng riêng ảo (VPN)			
6. Quản lý Logfile trên thiết bị			
- Thiết bị 1			Nơi lưu trữ
- Thiết bị 2			Nơi lưu trữ
- Thiết bị n			Nơi lưu trữ
7. Quản lý Logfile trên máy chủ			
- Máy chủ 1			Nơi lưu trữ
- Máy chủ 2			Nơi lưu trữ
- Máy chủ n			Nơi lưu trữ
8. Các biện pháp khác:			

2. Về đầu tư cho bảo đảm an toàn thông tin mạng

a) Kinh phí đầu tư cho công tác bảo đảm an toàn thông tin mạng: ..... triệu đồng

b) Tỷ lệ kinh phí trên tổng kinh phí công nghệ thông tin để đầu tư vào việc bảo đảm an toàn thông tin mạng: .....%

c) Đã đầu tư vào lĩnh vực nào dưới đây:

Lĩnh vực	Mô tả nội dung	Kinh phí (đồng)
1. Mua sắm thiết bị, phần mềm chuyên dụng an toàn thông tin mạng	(Mô tả thiết bị, phần mềm)	
2. Mua sắm hệ điều hành, phần mềm bản quyền	(Mô tả hệ điều hành, phần mềm)	

3. Tổ chức đào tạo, tập huấn, hội nghị, hội thảo về an toàn thông tin mạng	(Mô tả nội dung, thời gian, đối tượng đào tạo, tập huấn, hội nghị, hội thảo)	
4. Xây dựng hồ sơ đề xuất cấp độ		
5. Tổ chức kiểm định hệ thống thông tin mới được thiết kế		
6. Tổ chức đánh giá, xử lý rủi ro an toàn thông tin mạng		
7. Tổ chức ứng cứu xử lý sự cố an toàn thông tin mạng		
8. Các lĩnh vực khác:.....		

3. Về phát hiện và xử lý sự cố an toàn thông tin mạng

a) Tổng kết về các sự cố an toàn thông tin mạng đã xảy ra trong năm đối với cơ quan

Sự cố	Số lượng	Biện pháp xử lý
1. Tấn công chiếm quyền điều khiển		
2. Tấn công từ chối dịch vụ		
3. Tấn công mã hóa dữ liệu		
4. Tấn công phá hoại dữ liệu		
5. Tấn công thay đổi giao diện website		
6. Lừa đảo (Phishing)		
7. Thư rác (Spam mail)		
8. Lỗi hạ tầng kỹ thuật, thiết bị, phần mềm		
9. Lỗi quản trị, vận hành		
10. Sự cố khác:		

Biện pháp xử lý: Lựa chọn điền các thông tin sau (1) Không xử lý; (2) Tự xử lý; (3) Báo cáo cơ quan điều phối (Sở TT&TT); (4) Hỗ trợ từ cơ quan khác; (5) Nếu biện pháp khác thì mô tả cụ thể.

b) Mức độ thiệt hại trong năm 20... do các sự cố an toàn thông tin mạng gây ra

☐ Thiệt hại gián tiếp: ..... triệu đồng

☐ Thiệt hại trực tiếp: ..... triệu đồng

☐ Chi phí khắc phục: ..... triệu đồng

c) Công việc cơ quan đã thực hiện sau khi khắc phục được sự cố trong năm qua

☐ Liên kết, để được hỗ trợ từ các đơn vị hoạt động trong lĩnh vực an toàn thông tin

mạng

☐ Sửa đổi chính sách/hướng dẫn/thủ tục

☐ Nâng cao ý thức; ☐ Tăng cường thiết bị

☐ Rà soát lại hệ thống; ☐ Công việc khác (*mô tả cụ thể*):

.....

.....

.....

.....

4. Kiến nghị, đề xuất

.....

.....

.....

.....

Nơi nhận:
- Sở TT&TT;
- Lưu VT.

THỦ TRƯỞNG CƠ QUAN
(Ký số)

***Ghi chú**:*

- Điền thông tin đầy đủ vào các câu hỏi: Để lựa chọn đánh dấu X

- Câu hỏi với ký hiệu ❍ trước mỗi lựa chọn thì chỉ được phép đánh dấu một kết quả (chọn một)

- Câu hỏi với ký hiệu ☐ trước mỗi lựa chọn thì có thể đánh dấu từ không tới nhiều kết quả (chọn nhiều)

- Ký số và gửi liên thông về Sở Thông tin và Truyền thông.