ỦY BAN NHÂN DÂN TỈNH NINH BÌNH	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 48 /2024/QĐ-UBND	*Ninh Bình, ngày 18 tháng 7 năm 2024*

QUYẾT ĐỊNH

Ban hành Quy chế bảo đảm an toàn thông tin mạng tỉnh Ninh Bình

ỦY BAN NHÂN DÂN TỈNH NINH BÌNH

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

Căn cứ 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 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 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 An ninh mạng ngày 12 tháng 6 năm 2018;

Căn cứ Luật Bảo vệ bí mật nhà nước ngày 15 tháng 11 năm 2018;

Căn cứ Luật Giao dịch điện tử ngày 22 tháng 6 năm 2023;

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

Căn cứ Nghị định số 72/2013/NĐ-CP ngày 15 tháng 7 năm 2013 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng;

Căn cứ 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 Nghị định số 53/2022/NĐ-CP ngày 15 tháng 8 năm 2022 của Chính phủ Quy định chi tiết một số điều của Luật An ninh mạng;

Căn cứ Nghị định số 13/2023/NĐ-CP ngày 17 tháng 4 năm 2023 của Chính phủ về bảo vệ dữ liệu cá nhân;

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 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 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 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 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về việc bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Thông tư số 19/2023/TT-BTTTT ngày 25 tháng 12 năm 2023 của Bộ trưởng Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Quyết định số 08/2023/QĐ-TTg ngày 05 tháng 4 năm 2023 của Thủ tướng Chính phủ về Mạng truyền số liệu chuyên dùng phục vụ các cơ quan Đảng, Nhà nước;

Theo đề nghị của Giám đốc Sở Thông tin và Truyền thông tại Tờ trình số 1225/TTr-STTTT ngày 28 tháng 6 năm 2024.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn thông tin mạng tỉnh Ninh Bình.

Điều 2. Hiệu lực thi hành

1. Quyết định này có hiệu lực kể từ ngày 01 tháng 8 năm 2024.

2. Bãi bỏ Quyết định số 15/2016/QĐ-UBND ngày 06 tháng 7 năm 2016 của Ủy ban nhân dân tỉnh Ninh Bình ban hành Quy chế đảm bảo an toàn, an ninh thuộc lĩnh vực công nghệ thông tin trong hoạt động của các cơ quan nhà nước thuộc phạm vi quản lý của tỉnh Ninh Bình.

Điều 3. Tổ chức thực hiện

Chánh Văn phòng Ủy ban nhân dân tỉnh, Giám đốc Công an tỉnh, Giám đốc Sở Thông tin và Truyền thông; Thủ trưởng các sở, ban, ngành, đoàn thể của tỉnh; Chủ tịch Ủy ban nhân dân các huyện, thành phố; Chủ tịch Ủy ban nhân dân các xã, phường, thị trấn và các cơ quan, tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Bộ Thông tin và Truyền thông;
- Cục Kiểm tra văn bản QPPL-Bộ Tư pháp;
- Thường trực Tỉnh ủy;
- Thường trực HĐND tỉnh;
- Đoàn ĐBQH và HĐND tỉnh;
- Ủy ban MTTQ Việt Nam tỉnh;
- Lãnh đạo UBND tỉnh;
- Báo Ninh Bình, Đài PT&TH tỉnh;
- VNPT, Viettel Ninh Bình, Bưu điện tỉnh;
- Cổng TTĐT tỉnh, Công báo tỉnh;
- Lưu: VT, VP6.

HP_VP6_QĐ

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

Tống Quang Thìn

ỦY BAN NHÂN DÂN TỈNH NINH BÌNH	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc

QUY CHẾ
Bảo đảm an toàn thông tin mạng tỉnh Ninh Bình

(Kèm theo Quyết định số /2024/QĐ-UBND ngày tháng 7 năm 2024 của Ủy ban nhân dân tỉnh Ninh Bình)

Chương I
QUY ĐỊNH CHUNG

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

1. Phạm vi điều chỉnh

Quy chế này quy định về bảo đảm an toàn thông tin mạng của cơ quan nhà nước trên địa bàn tỉnh Ninh Bình.

2. Đối tượng áp dụng

a) Các sở, ban, ngành, đoàn thể của tỉnh; các đơn vị sự nghiệp công lập trực thuộc UBND tỉnh; UBND các huyện, thành phố; UBND các xã, phường, thị trấn; các cơ quan được ngân sách nhà nước bảo đảm kinh phí hoạt động có sử dụng các hệ thống thông tin của tỉnh (viết tắt là cơ quan, đơn vị).

b) Cán bộ, công chức, viên chức, người lao động (viết tắt là cán bộ, công chức, viên chức) và các cá nhân, tổ chức có liên quan tham gia vận hành, khai thác các hệ thống thông tin tại các cơ quan, đơn vị quy định tại điểm a khoản 2 Điều này.

c) Các doanh nghiệp cung cấp dịch vụ viễn thông, công nghệ thông tin, Internet; các doanh nghiệp, tổ chức, cá nhân có tham gia vào các hoạt động ứng dụng công nghệ thông tin, chuyển đổi số của các cơ quan, đơn vị thuộc điểm a khoản 2 Điều này.

d) Khuyến khích các cơ quan, đơn vị khác thực hiện các hoạt động ứng dụng và phát triển công nghệ thông tin, chuyển đổi số trên địa bàn tỉnh Ninh Bình áp dụng 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.

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 định tại khoản 7 Điều 3 Nghị định số 64/2007/NĐ-CP.

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

5. Giám sát an toàn hệ thống thông tin được quy định tại khoản 1 Điều 24 Luật An toàn thông tin mạng.

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

7. Ứng cứu sự cố an toàn thông tin mạng được quy định tại khoản 2 Điều 2 Thông tư số 20/2017/TT-BTTTT.

8. Mật khẩu mạnh là mật khẩu có độ dài tối thiểu 8 ký tự, trong đó kết hợp bao gồm ký tự hoa, thường, chữ số và ký tự đặc biệt.

9. Chủ quản hệ thống thông tin trên địa bàn tỉnh là UBND tỉnh.

10. Đơn vị chuyên trách về an toàn thông tin của tỉnh là Sở Thông tin và Truyền thông.

11. Đơn vị vận hành hệ thống thông tin là các cơ quan, đơn vị trên địa bàn tỉnh được UBND tỉnh giao nhiệm vụ quản lý, vận hành hệ thống thông tin. Trong trường hợp thuê dịch vụ công nghệ thông tin thì doanh nghiệp, tổ chức cung cấp dịch vụ đóng vai trò đơn vị vận hành hệ thống thông tin.

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

1. Bảo đảm an toàn thông tin mạng đối với các hoạt động ứng dụng công nghệ thông tin, giao dịch điện tử, chuyển đổi số của tỉnh 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 và các quy định pháp luật khác có liên quan.

2. Xác định rõ quyền hạn, trách nhiệm của thủ trưởng cơ quan, đơn vị và cá nhân trực tiếp liên quan đối với công tác bảo đảm an toàn thông tin mạng và an ninh mạng; bố trí nhân sự để sẵn sàng xử lý sự cố an toàn thông tin mạng đối với các hệ thống thông tin do đơn vị mình quản lý.

3. Thông tin có bí mật nhà nước được thực hiện theo quy định của Luật Bảo vệ bí mật nhà nước và các quy định pháp luật về bảo vệ bí mật nhà nước có liên quan.

4. Xử lý sự cố an toàn thông tin phải phù hợp với trách nhiệm, quyền hạn và bảo đảm lợi ích hợp pháp của cơ quan, đơn vị, cá nhân liên quan và theo quy định của pháp luật.

Điều 4. Các hành vi bị cấm

1. Các hành vi bị nghiêm cấm về an toàn, an ninh thông tin mạng và giao dịch điện tử quy định tại Điều 7 Luật An toàn thông tin mạng, Điều 8 Luật An ninh mạng, Điều 5 Luật Bảo vệ bí mật nhà nước, Điều 6 Luật Giao dịch điện tử.

2. Các hành vi bị cấm trong thực hiện việc quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng quy định tại Điều 5 Nghị định số 72/2013/NĐ-CP, Điều 3 Thông tư số 24/2014/TT-BTTTT và điểm d khoản 2 Điều 2 Nghị định số 27/2018/NĐ-CP.

3. Hành vi khác bị nghiêm cấm theo quy định của pháp luật.

Chương II
QUY ĐỊNH BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Điều 5. Yêu cầu bảo đảm an toàn hệ thống thông tin theo cấp độ

1. Việc đảm bảo an toàn hệ thống thông tin theo cấp độ trong hoạt động của cơ quan, đơn vị phải được thực hiện thường xuyên, liên tục từ khâu thiết kế, xây dựng, vận hành đến khi hủy bỏ; tuân thủ theo tiêu chuẩn, quy chuẩn kỹ thuật. Nội dung yêu cầu bảo đảm an toàn hệ thống thông tin theo cấp độ thực hiện theo quy định tại Điều 9 Thông tư số 12/2022/TT-BTTTT.

2. Đánh giá, phân loại cấp độ an toàn thông tin của hệ thống thông tin

a) Chủ quản hệ thống thông tin có trách nhiệm chỉ đạo, tổ chức thực hiện phương án đảm bảo an toàn hệ thống thông tin theo cấp độ theo quy định tại Nghị định số 85/2016/NĐ-CP.

b) Đơn vị vận hành hệ thống thông tin của các cơ quan, đơn vị trên địa bàn tỉnh thực hiện xác định cấp độ (từ cấp độ 1 đến cấp độ 3) và lập hồ sơ đề xuất cấp độ bao gồm các tài liệu thuyết minh được quy định tại Điều 7, 8, 9, 15 Nghị định số 85/2016/NĐ-CP và Điều 8 Thông tư số 12/2022/TT-BTTTT gửi đơn vị chuyên trách về an toàn thông tin của tỉnh thẩm định, phê duyệt hồ sơ đề xuất cấp độ an toàn thông tin.

3. Hệ thống thông tin khi được đầu tư xây dựng mới hoặc mở rộng, nâng cấp cần được kiểm thử về tính an toàn, bảo mật trước khi nghiệm thu, bàn giao đưa vào khai thác, sử dụng theo quy định tại điểm b khoản 3 Điều 10 của Thông tư số 24/2020/TT-BTTTT.

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, đơn vị sử dụng 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. Trong hợp đồng phải bao gồm các điều

khoản về việc xử lý vi phạm quy định bảo đảm an toàn thông tin và trách nhiệm bồi thường thiệt hại do hành vi vi phạm của bên cung cấp dịch vụ gây ra.

2. Trách nhiệm của cơ quan, đơn vị trong quá trình sử dụng dịch vụ công nghệ thông tin

a) Yêu cầu bên cung cấp dịch vụ phải bảo mật thông tin, dữ liệu, mã nguồn, tài liệu thiết kế; triển khai các biện pháp bảo đảm an toàn thông tin theo quy định tại Quy chế này, Luật An toàn thông tin mạng, Luật An ninh mạng và các quy định khác có liên quan.

b) Giám sát chặt chẽ và giới hạn quyền truy cập của bên cung cấp dịch vụ khi cho phép truy cập vào hệ thống thông tin của cơ quan, đơn vị.

3. Trách nhiệm của cơ quan, đơn vị khi phát hiện bên cung cấp dịch vụ có dấu hiệu vi phạm quy định bảo đảm an toàn thông tin

a) Tạm dừng hoặc đình chỉ hoạt động của bên cung cấp dịch vụ tùy theo mức độ vi phạm.

b) Thông báo chính thức các hành vi vi phạm của bên cung cấp dịch vụ.

c) Thu hồi ngay lập tức quyền truy cập hệ thống thông tin đã cấp cho bên cung cấp dịch vụ.

d) Kiểm tra, xác định, lập báo cáo mức độ vi phạm và thiệt hại xảy ra; thông báo cho bên cung cấp dịch vụ và tiến hành các thủ tục xử lý vi phạm và bồi thường thiệt hại.

4. Trách nhiệm của cơ quan, đơn vị khi kết thúc sử dụng dịch vụ

a) Thu hồi quyền truy cập hệ thống thông tin và các tài sản khác liên quan đã cấp cho bên cung cấp dịch vụ; thay đổi các khóa, mật khẩu truy cập hệ thống thông tin.

b) Yêu cầu bên cung cấp dịch vụ chuyển giao đầy đủ các thông tin, dữ liệu, mã nguồn, tài liệu thiết kế và các công cụ cần thiết để bảo đảm cơ quan, đơn vị vẫn có thể khai thác sử dụng dịch vụ được liên tục kể cả trong trường hợp thay đổi bên cung cấp dịch vụ.

Điều 7. Giám sát an toàn hệ thống thông tin

1. Nguyên tắc, yêu cầu, phương thức về hoạt động giám sát an toàn hệ thống thông tin thực hiện theo quy định tại Điều 3, 4, 5 Thông tư số 31/2017/TT-BTTTT.

2. Chủ quản hệ thống thông tin chỉ đạo thực hiện giám sát đối với các hệ thống thông tin thuộc phạm vi quản lý.

3. Đơn vị chuyên trách về an toàn thông tin của tỉnh làm đầu mối giám sát, cảnh báo an toàn thông tin mạng của tỉnh; chịu trách nhiệm tổ chức, triển khai, thực hiện giám sát an toàn hệ thống thông tin tập trung trên địa bàn tỉnh và bảo đảm kết nối, chia sẻ thông tin với hệ thống giám sát của Bộ Thông tin và Truyền thông (Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam, Cục An toàn thông tin thuộc Bộ Thông tin và Truyền thông).

4. Các cơ quan, đơn vị cử cá nhân hoặc bộ phận làm đầu mối giám sát, cung cấp, tiếp nhận thông tin cảnh báo, kịp thời với đơn vị chuyên trách về an toàn thông tin của tỉnh, phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao của Công an tỉnh nhằm tăng cường công tác đảm bảo an ninh mạng, an toàn thông tin và phòng, chống tội phạm sử dụng công nghệ cao. Đầu mối giám sát thực hiện bảo đảm các điều kiện cho hoạt động kết nối tại điểm giám sát và triển khai giám sát trong phạm vi hệ thống thông tin của cơ quan, đơn vị mình.

Điều 8. Ứng cứu sự cố an toàn thông tin

1. Nguyên tắc ứng cứu xử lý sự cố

Nguyên tắc ứng cứu xử lý sự cố thực hiện theo quy định tại khoản 3 Điều 4, khoản 2 Điều 13 Luật An toàn thông tin mạng và Điều 4 Thông tư số 20/2017/TT-BTTTT.

2. Phân loại sự cố an toàn thông tin mạng

a) Sự cố do bị tấn công mạng.

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.

e) 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.

4. Quy trình ứng cứu sự cố thực hiện theo Điều 11 Thông tư số 20/2017/TT-BTTTT. 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.

5. 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 cơ quan, đơn vị phải báo cáo ngay cho cơ quan cấp trên quản lý trực tiếp và đơn vị chuyên trách về an toàn thông tin của tỉnh để được hướng dẫn, hỗ trợ hoặc điều phối ứng cứu sự cố an toàn thông tin mạng.

6. 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.

7. Đơn vị/bộ phận chuyên trách về an toàn thông tin có trách nhiệm

a) Xây dựng phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng, ứng phó sự cố an toàn thông tin mạng.

b) Xây dựng quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng theo quy định.

c) Phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an toàn thông tin; yêu cầu bên cung cấp dịch vụ cung cấp đầy đủ quy trình xử lý sự cố đối với dịch vụ thực hiện.

d) Tổ chức diễn tập phương án xử lý sự cố an toàn thông tin theo chỉ đạo của thủ trưởng cơ quan, đơn vị.

Điều 9. 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, 12 Thông tư số 12/2022/TT-BTTTT.

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 10. Quản lý rủi ro, lỗ hổng, điểm yếu an toàn an thông tin

1. Các cơ quan, đơn vị phối hợp với đơn vị chuyên trách về an toàn thông tin của tỉnh tổ chức quản lý lỗ hổng, điểm yếu an toàn thông tin mạng

a) Lập danh sách toàn bộ thiết bị, phần mềm công nghệ thông tin đang sử dụng trong phạm vi quản lý của chủ quản hệ thống thông tin: nhãn hiệu phần cứng, tên phần mềm và phiên bản (hệ điều hành, cơ sở dữ liệu, ứng dụng, các tiện ích khác).

b) Thiết lập, duy trì kênh tiếp nhận thông tin về lỗ hổng, điểm yếu an toàn thông tin mạng từ các cơ quan, tổ chức có chức năng cảnh báo về an toàn an thông tin mạng; các đơn vị cung cấp thiết bị, phần mềm công nghệ thông tin thuộc phạm vi điểm a khoản này.

c) Quản lý, giám sát việc cài đặt bản vá lỗ hổng, điểm yếu an toàn thông tin mạng. Sử dụng và cập nhật liên tục các công cụ dò quét lỗ hổng, điểm yếu an toàn thông tin mạng để các công cụ này có thể phát hiện được các lỗ hổng bảo mật mới nhất; hoặc sử dụng kết quả kiểm tra, đánh giá an toàn thông tin mạng để xác định các lỗ hổng, điểm yếu của hệ thống thông tin.

d) Triển khai cài đặt bản vá lỗ hổng, điểm yếu an toàn thông tin mạng sau khi bản vá được phát hành; áp dụng các biện pháp bảo vệ tạm thời trong trường hợp bản vá bảo mật chưa được phát hành hoặc chưa đủ điều kiện để triển khai.

2. Các cơ quan, đơn vị phối hợp với đơn vị chuyên trách về an toàn thông tin, đơn vị vận hành hệ thống thông tin và cơ quan, tổ chức có liên quan triển khai quản lý rủi ro an toàn thông tin mạng trên cơ sở quản lý lỗ hổng, điểm yếu an toàn thông tin mạng theo quy định tại khoản 1 Điều này và theo hướng dẫn của Bộ Thông tin và Truyền thông, Bộ Công an.

3. 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 đơn vị chuyên trách về an toàn thông tin của tỉnh hoặc các cơ quan có thẩm quyền khác, chủ quản 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 đơn vị chuyên trách về an toàn thông tin của tỉnh để theo dõi, tổng hợp.

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, sử dụng tài sản công và được các cấp có thẩm quyền cho phép dừng sử dụng. 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, hủy tài sản.

Điều 12. Bảo đảm an toàn, an ninh thông tin trong quản lý tài sản công nghệ thông tin

1. Phân loại tài sản công nghệ thông tin

a) Tài sản phần cứng (vật lý): Là các máy móc, trang thiết bị phần cứng, phương tiện truyền thông và các trang thiết bị phục vụ cho hoạt động của hệ thống thông tin.

b) Tài sản phần mềm: Là các phần mềm hệ thống, phần mềm thương mại, phần mềm nội bộ, phần mềm ứng dụng, phần mềm quản trị cơ sở dữ liệu và công cụ phát triển phần mềm.

c) Tài sản thông tin: Là các thông tin, cơ sở dữ liệu, dữ liệu ở dạng số hóa.

2. Yêu cầu về quản lý tài sản công nghệ thông tin

a) Giao, gắn trách nhiệm cho cá nhân hoặc tập thể quản lý, sử dụng tài sản công nghệ thông tin.

b) Quy định các quy tắc sử dụng, giữ gìn bảo vệ tài sản công nghệ thông tin trong các trường hợp như: Mang ra khỏi cơ quan, trang thiết bị công nghệ thông tin liên quan đến dữ liệu bảo mật, thông tin cài đặt và cấu hình.

c) Tài sản phần cứng có lưu trữ dữ liệu quan trọng khi thay đổi mục đích sử dụng hoặc thanh lý, đơn vị phải phối hợp với bộ phận chuyên trách về công nghệ thông tin thực hiện các biện pháp xóa, tiêu hủy dữ liệu đó bảo đảm không có khả năng phục hồi. Trường hợp không thể tiêu hủy được dữ liệu, đơn vị phải thực hiện tiêu hủy cấu phần lưu trữ dữ liệu trên trang thiết bị đó.

d) Trang thiết bị công nghệ thông tin có bộ phận lưu trữ dữ liệu hoặc thiết bị lưu trữ dữ liệu khi mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài hoặc ngừng sử dụng phải tháo bộ phận lưu trữ khỏi thiết bị và để lại cơ quan, đơn vị hoặc xóa thông tin, dữ liệu lưu trữ trên thiết bị. Khi thanh lý thiết bị phải xóa dữ liệu lưu trữ bằng phần mềm hoặc thiết bị hủy dữ liệu chuyên dụng.

e) Các đơn vị có trách nhiệm bảo dưỡng, bảo trì và hướng dẫn cách sử dụng, quản lý, vận hành hệ thống hạ tầng kỹ thuật của mình; chỉ định bộ phận thực hiện quản lý, vận hành và định kỳ kiểm tra, sửa chữa, bảo trì thiết bị (bao gồm thiết bị đang hoạt động và thiết bị dự phòng).

Điều 13. Bảo đảm an toàn vật lý và môi trường vận hành

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, tại các phòng chuyên biệt và phải được thiết lập cơ chế bảo vệ, theo dõi phát hiện xâm nhập, biện pháp kiểm soát truy cập, kết nối vật lý phù hợp với từng khu vực, bảo đảm

chỉ người có nhiệm vụ mới được vào và phải có nội quy riêng khi làm việc trong các khu vực này.

2. Trung tâm Dữ liệu của tỉnh là khu vực hạn chế tiếp cận, chỉ những cá nhân có quyền, nhiệm vụ theo quy định và được sự cho phép của cơ quan quản lý là Sở Thông tin và Truyền thông mới được vào Trung tâm Dữ liệu. Việc vào, ra Trung tâm Dữ liệu phải thực hiện theo Nội quy quy định, được hệ thống kiểm soát vào ra (quẹt thẻ, vân tay, nhận dạng sinh trắc học…).

3. Các khu vực quy định tại khoản 1, 2 Điều này phải có biện pháp đảm bảo nguồn điện và dự phòng điện, 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.

4. Các đường truyền dữ liệu, đường truyền Internet và hệ thống dây dẫn các hệ thống mạng diện rộng (WAN), hệ thống mạng nội bộ (LAN) phải được lắp đặt trong ống, máng che đậy kín, hạn chế khả năng tiếp cận trái phép. Ngắt các cổng kết nối không sử dụng, đặc biệt là ở khu vực làm việc chung của các cơ quan, đơn vị.

5. Thiết lập cơ chế dự phòng đối với các thiết bị hạ tầng kỹ thuật quan trọng; có kế hoạch kiểm tra, bảo dưỡng định kỳ và duy trì thông số kỹ thuật các thiết bị này hoặc có phương án sửa chữa, thay thế đáp ứng yêu cầu về tính khả dụng.

6. Cơ quan, đơn vị có trách nhiệm xây dựng quy trình bảo dưỡng, bảo trì và hướng dẫn cách sử dụng, quản lý, vận hành hệ thống hạ tầng kỹ thuật của mình; chỉ định bộ phận chuyên trách về an toàn thông tin mạng thực hiện quản lý, vận hành và định kỳ kiểm tra, sửa chữa, bảo trì thiết bị (bao gồm thiết bị đang hoạt động và thiết bị dự phòng).

Điều 14. Quản lý an toàn hạ tầng mạng

1. An toàn cho mạng nội bộ (LAN)

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 03 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 nhà sản xuất.

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

Điều 15. Quản lý an toàn máy chủ và ứng dụng

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

a) Máy chủ phải được cài đặt, sử dụng phần mềm phòng chống mã độc, phần mềm phải được cập nhật thường xuyên và 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.

e) 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.

f) 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.

2. Cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống trước khi đưa vào sử dụng, 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, 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 16. Bảo đảm an toàn thông tin Trung tâm Dữ liệu của tỉnh

1. Đơn vị vận hành Trung tâm Dữ liệu là đơn vị chuyên trách về an toàn thông tin Trung tâm Dữ liệu; chịu trách nhiệm xây dựng, thực thi các quy định về an toàn bảo mật thông tin mạng, quản lý, khai thác và vận hành Trung tâm Dữ liệu. Phối hợp với các cơ quan, tổ chức có thẩm quyền về quản lý an toàn thông tin mạng, công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin mạng, tham gia hoạt động đảm bảo an toàn thông tin mạng. Tùy theo mức độ sự cố, phối hợp với các đơn vị có liên quan thực hiện hướng dẫn xử lý, ứng cứu sự cố an toàn thông tin mạng cho các hệ thống thông tin dùng chung của tỉnh.

2. Cơ quan, đơn vị có hệ thống thông tin được cài đặt, duy trì vận hành tại Trung tâm Dữ liệu có trách nhiệm bảo đảm an toàn thông tin cho máy chủ, ứng dụng, các trang thiết bị công nghệ thông tin hoặc các thành phần đặc biệt khác phục vụ hệ thống thông tin của cơ quan, đơn vị mình. Phối hợp triển khai các biện pháp bảo đảm an toàn thông tin mạng theo yêu cầu của đơn vị vận hành Trung tâm Dữ liệu.

3. Các cơ quan, đơn vị thực hiện tích hợp, kết nối, sử dụng hạ tầng, dịch vụ của Trung tâm Dữ liệu chịu trách nhiệm nếu để tin tặc kiểm soát máy tính và truy cập trái phép vào Trung tâm Dữ liệu của tỉnh, tuân thủ nghiêm các quy định tại Quy chế quản lý, khai thác và vận hành Trung tâm Dữ liệu tỉnh Ninh Bình ban hành kèm theo Quyết định số 07/2022/QĐ-UBND ngày 04/3/2022 của UBND tỉnh; các quy định, chính sách về an toàn bảo mật thông tin trong quản lý, vận hành và khai thác Trung tâm Dữ liệu tỉnh.

Điều 17. 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) Tài khoản quản trị hệ thống (mạng, hệ điều hành, thiết bị kết nối mạng, phần mềm, ứng dụng, cơ sở dữ liệu) phải tách biệt với tài khoản truy cập của người dùng thông thường. Tài khoản hệ thống phải được giao đích danh cá nhân làm công tác quản trị. Hạn chế dùng chung tài khoản quản trị.

e) 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 06 tháng phải bị khóa hoặc xóa bỏ (sau khi trao đổi, xác nhận với cơ quan, đơn vị sử dụng).

2. Cơ quan, đơn vị phải thực hiện bảo vệ thông tin, dữ liệu liên quan đến hoạt động công vụ, thông tin có nội dung quan trọng, nhạy cảm hoặc không phải là thông tin công khai bằng các biện pháp như: Thiết lập phương án bảo đảm tính bí mật, nguyên vẹn và khả dụng của thông tin, dữ liệu; mã hóa thông tin, dữ liệu khi lưu trữ trên hệ thống/thiết bị lưu trữ dữ liệu di động; sử dụng chữ ký số để xác thực và bảo mật thông tin, dữ liệu; xây dựng quy trình quản lý và phân công cán bộ quản lý.

3. Không soạn thảo, lưu giữ tài liệu chứa bí mật nhà nước trên máy tính, các thiết bị khác đã kết nối hoặc đang kết nối với mạng Internet, mạng máy tính, mạng viễn thông, trừ trường hợp lưu giữ bí mật nhà nước theo quy định của pháp luật về cơ yếu.

4. Các cơ quan, đơn vị phải thường xuyên kiểm tra, giám sát các hoạt động chia sẻ, gửi, nhận thông tin, dữ liệu trong hoạt động nội bộ của mình; khuyến cáo việc chia sẻ, gửi, nhận thông tin trên môi trường mạng cần phải sử dụng mật khẩu mạnh để bảo vệ thông tin.

5. Giao dịch trực tuyến phải được truyền đầy đủ, đúng địa chỉ, tránh bị sửa đổi, tiết lộ hoặc nhân bản một cách trái phép; sử dụng các cơ chế xác thực mạnh, chữ ký số khi tham gia giao dịch, sử dụng các giao thức truyền thông an toàn.

6. Các cơ quan, đơn vị phải đảm bảo thực hiện các quy định về bảo vệ dữ liệu cá nhân và trách nhiệm bảo vệ dữ liệu cá nhân của cơ quan, tổ chức, cá nhân có liên quan theo Nghị định số 13/2023/NĐ-CP; phối hợp với Công an tỉnh, Sở Thông tin và Truyền thông và các đơn vị liên quan trong công tác phòng ngừa, phát hiện, ngăn chặn, xử lý hành vi vi phạm liên quan đến dữ liệu cá nhân theo quy định của pháp luật.

Điều 18. Bảo đảm an toàn thiết bị và người dùng đầu cuối

1. Trên máy tính cá nhân phải thiết lập chế độ tự động cập nhật hệ điều hành trên máy tính, phải thiết lập mật khẩu truy nhập chế độ tự động bảo vệ màn hình khi không sử dụng; sử dụng những trình duyệt an toàn, đáng tin cậy, cài đặt phần mềm phòng chống mã độc; thiết lập chế độ tự động cập nhật phần mềm phòng chống mã độc, chế độ tự động rà quét mã độc khi sao chép, mở các tập tin, chế độ rà quét máy tính định kỳ hằng tuần.

2. Các cơ quan, đơn vị đầu tư, thuê, mua sắm thiết bị đảm bảo an toàn thông tin ưu tiên các sản phẩm, dịch vụ sản xuất trong nước theo quy định tại Thông tư số 40/2020/TT-BTTTT.

3. Kết nối máy tính/thiết bị đầu cuối của người sử dụng vào hệ thống

a) Người sử dụng khi truy cập, sử dụng tài nguyên nội bộ, truy cập mạng và tài nguyên trên Internet phải tuân thủ các quy định của pháp luật về bảo đảm an toàn thông tin và các quy định của cơ quan, tổ chức.

b) Khi cài đặt, kết nối máy tính/thiết bị đầu cuối phải thực hiện theo hướng dẫn/quy trình dưới sự giám sát của bộ phận chuyên trách về an toàn thông tin.

c) Đối với hệ thống thông tin từ cấp độ 3 trở lên, máy tính/thiết bị đầu cuối phải được xử lý điểm yếu an toàn thông tin, cấu hình cứng hóa bảo mật trước khi kết nối vào hệ thống.

4. Trong quá trình sử dụng thiết bị đầu cuối

a) Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác 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) Có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng.

c) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo ngay với cấp trên trực tiếp và bộ phận phụ trách công nghệ thông tin của cơ quan, đơn vị để kịp thời ngăn chặn và xử lý.

Điều 19. Bảo đảm nguồn nhân lực an toàn thông tin mạng

1. Công chức, viên chức, người lao động được tuyển dụng hoặc sắp xếp, giao nhiệm vụ về an toàn thông tin mạng phải có trình độ, chuyên ngành phù hợp yêu cầu đối với các vị trí việc làm về công nghệ thông tin, an toàn thông tin mạng theo hướng dẫn của Bộ Thông tin và Truyền thông.

2. Cán bộ chuyên trách về công nghệ thông tin trong các cơ quan, đơn vị được tạo điều kiện trang bị các thiết bị công nghệ thông tin, phương tiện kỹ thuật làm việc phù hợp với chuyên môn; tham dự đầy đủ các khóa đào tạo, tập huấn và

bồi dưỡng kiến thức, kỹ năng, nghiệp vụ cho cán bộ chuyên trách về an toàn thông tin mạng.

3. Các cơ quan, đơn vị xác định nhu cầu về đào tạo nguồn nhân lực bảo đảm an toàn thông tin tại cơ quan, đơn vị mình gửi Sở Thông tin và Truyền thông tổng hợp, xây dựng trình UBND tỉnh phê duyệt kế hoạch giai đoạn, kế hoạch hàng năm về đào tạo, bồi dưỡng nghiệp vụ bảo đảm an toàn thông tin mạng cho cán bộ, công chức, viên chức và người lao động của tỉnh và thực hiện tổ chức đào tạo theo kế hoạch đã phê duyệt.

4. Các cơ quan, đơn vị phải thường xuyên tổ chức các hoạt động tuyên truyền, phổ biến nâng cao nhận thức về bảo đảm an toàn thông tin mạng và an ninh mạng đến toàn thể bộ cán bộ, công chức, viên chức và người lao động tại cơ quan, đơn vị mình.

Chương III
TRÁCH NHIỆM BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Điều 20. Trách nhiệm của Sở Thông tin và Truyền thông

1. Tham mưu giúp UBND tỉnh về công tác bảo đảm an toàn thông tin trên địa bàn tỉnh và chịu trách nhiệm trước UBND tỉnh trong việc bảo đảm an toàn thông tin cho Trung tâm Dữ liệu của tỉnh.

2. Thực hiện theo dõi, đôn đốc, hướng dẫn, kiểm tra, giám sát công tác bảo đảm an toàn thông tin mạng, thẩm định, phê duyệt hồ sơ cấp độ an toàn thông tin và phương án bảo đảm an toàn cho các hệ thống thông tin theo quy định của Luật An toàn thông tin mạng và các văn bản hướng dẫn thi hành Luật An toàn thông tin mạng.

3. Chủ trì, phối hợp với Công an tỉnh và các cơ quan, đơn vị có liên quan tiến hành thanh tra, kiểm tra công tác bảo đảm an toàn thông tin mạng định kỳ hàng năm hoặc đột xuất khi có yêu cầu của cơ quan nhà nước có thẩm quyền.

4. Hàng năm, xây dựng và triển khai các kế hoạch đào tạo, tập huấn về công tác bảo đảm an toàn thông tin mạng cho cán bộ, công chức, viên chức chuyên trách về công nghệ thông tin; đào tạo, tập huấn chuyên sâu về an toàn thông tin mạng cho lực lượng bảo đảm an toàn thông tin mạng của các cơ quan, đơn vị. Tổ chức các hội nghị, hội thảo chuyên đề và tuyên truyền về an toàn thông tin mạng trong công tác quản lý nhà nước trên địa bàn tỉnh.

5. Phối hợp với Công an tỉnh trong công tác phòng ngừa, phát hiện, ngăn chặn và xử lý các hành vi vi phạm pháp luật trên môi trường mạng, nhất là trên các cổng/trang thông tin điện tử, mạng xã hội theo thẩm quyền.

6. Là cơ quan đầu mối, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin; tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin mạng trên địa bàn tỉnh.

7. Định kỳ hàng năm 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.

8. Tổng hợp và báo cáo về tình hình an toàn thông tin mạng theo định kỳ cho Bộ Thông tin và Truyền thông, UBND tỉnh và các cơ quan, đơn vị có liên quan. Đề nghị UBND tỉnh khen thưởng hoặc phê bình thủ trưởng cơ quan, đơn vị trong thực hiện chỉ đạo về bảo đảm an toàn thông tin mạng.

9. Chỉ đạo Trung tâm Công nghệ thông tin và Truyền thông (đơn vị vận hành Trung tâm Dữ liệu tỉnh) triển khai thực hiện công tác giám sát, bảo đảm an toàn thông tin mạng đối với các hệ thống thông tin đang cài đặt, vận hành tại Trung tâm Dữ liệu tỉnh, các hệ thống thông tin của các cơ quan, đơn vị có kết nối đến Trung tâm Dữ liệu tỉnh theo quy định; kịp thời cung cấp các thông tin, dữ liệu có liên quan cho các cơ quan chức năng có thẩm quyền để phục vụ công tác điều tra, xác minh an toàn thông tin mạng khi có yêu cầu.

10. Tham gia mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia và thực hiện trách nhiệm, quyền hạn của thành viên mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia theo quy định tại Quyết định số 05/2017/QĐ-TTg.

Điều 21. 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 phát hiện, 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. Kịp thời thông báo các phương thức, thủ đoạn mới của các loại tội phạm công nghệ cao.

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

3. 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.

4. Tham mưu Tiểu ban an toàn an ninh mạng tổ chức Hội nghị tuyên truyền, phổ biến về An ninh mạng, an toàn thông tin theo chức năng, thẩm quyền được giao.

Điều 22. Trách nhiệm của Sở Tài chính, Sở Kế hoạch và Đầu tư

1. Sở Tài chính chủ trì, phối hợp với Sở Thông tin và Truyền thông và các cơ quan, đơn vị có liên quan, căn cứ khả năng cân đối ngân sách tỉnh, tham mưu

cho cấp có thẩm quyền phân bổ kinh phí chi thường xuyên ngân sách tỉnh để thực hiện các nhiệm vụ bảo đảm an toàn thông tin mạng của tỉnh theo quy định của Luật Ngân sách Nhà nước và các văn bản hướng dẫn có liên quan.

2. Sở Kế hoạch và Đầu tư tham mưu báo cáo UBND tỉnh bố trí nguồn vốn đầu tư xây dựng cơ bản để thực hiện các dự án bảo đảm an toàn thông tin mạng theo đúng quy định.

Điều 23. Trách nhiệm của Sở Nội vụ

a) Tham mưu UBND tỉnh có cơ chế chính sách để thu hút các chuyên gia về an toàn an ninh thông tin làm việc tại tỉnh. Bố trí cán bộ chuyên trách về an toàn an ninh thông tin trong các cơ quan, đơn vị để triển khai hiệu quả công tác bảo đảm an toàn hệ thống thông tin theo cấp độ, công tác bảo đảm an toàn thông tin theo mô hình 4 lớp, đặc biệt là đối với Trung tâm Dữ liệu và các hệ thống thông tin quan trọng, dùng chung của tỉnh.

b) Phối hợp với Sở Thông tin và Truyền thông triển khai tổ chức các lớp đào tạo, bồi dưỡng nâng cao kiến thức về Chính quyền điện tử, Chính quyền số, chuyển đổi số và đảm bảo an toàn, an ninh thông tin cho cán bộ, công chức, viên chức của tỉnh.

Điều 24. Trách nhiệm của các cơ quan, đơn vị

1. Chịu trách nhiệm trong công tác bảo đảm an toàn thông tin mạng của cơ quan, đơn vị mình theo Quy chế này và các quy định nhà nước về an toàn, an ninh thông tin khác.

2. Thực hiện xác định cấp độ an toàn thông tin và bảo đảm an toàn cho hệ thống thông tin của đơn vị quản lý theo quy định tại Luật An toàn thông tin mạng và các văn bản hướng dẫn thi hành Luật An toàn thông tin mạng.

3. Phân công bộ phận hoặc cán bộ, công chức, viên chức chuyên trách về công nghệ thông tin bảo đảm an toàn thông tin của cơ quan, đơn vị; chỉ đạo công chức, viên chức và người lao động nghiêm túc chấp hành các quy định về bảo đảm an toàn thông tin; tạo điều kiện để các cán bộ phụ trách an toàn thông tin được học tập, nâng cao trình độ về an toàn thông tin; thường xuyên tổ chức quán triệt các quy định về an toàn thông tin trong cơ quan, đơn vị; xác định các yêu cầu, trách nhiệm bảo đảm an toàn thông tin đối với các vị trí cần tuyển dụng hoặc phân công.

4. Thường xuyên tổ chức, phổ biến các quy định về đảm bảo an toàn thông tin, nhằm nâng cao nhận thức về trách nhiệm đảm bảo an toàn thông tin cho tổ chức, cá nhân sử dụng hệ thống thông tin do cơ quan, đơn vị quản lý.

5. Ban hành quy chế, quy trình nội bộ về bảo đảm an toàn thông tin mạng gồm các nội dung cơ bản như quy định về quản lý hạ tầng mạng, bảo đảm an toàn

dữ liệu, bảo đảm an toàn thiết bị và người dùng đầu cuối phù hợp với Quy chế này và các quy định của pháp luật.

6. 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 xảy ra một cách kịp thời, nhanh chóng và đạt hiệu quả.

7. Phối hợp chặt chẽ với Công an tỉnh, Sở Thông tin và Truyền thông và các cơ quan, đơn vị liên quan trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn thông tin trên không gian mạng.

8. Hàng năm bố trí kinh phí cho việc ứng dụng công nghệ thông tin nói chung và công tác bảo đảm an toàn thông tin mạng nói riêng trong nội bộ cơ quan, đơn vị mình; lập kế hoạch nâng cấp, bảo trì, sửa chữa, gia hạn bản quyền phần mềm, gia hạn bảo hành cho các hệ thống phần cứng, phần mềm nhằm thực hiện tốt công tác bảo mật, bảo đảm an toàn thông tin mạng.

9. Các cơ quan, đơn vị cử đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin. Phân công lãnh đạo phụ trách công tác đảm bảo an toàn thông tin đối với các hệ thống thông tin và cơ sở dữ liệu do đơn vị quản lý

10. Thực hiện các báo cáo về an toàn thông tin mạng khi được Sở Thông tin và Truyền thông yêu cầu.

Điều 25. Trách nhiệm của đơn vị vận hành hệ thống thông tin

1. Thực hiện trách nhiệm của đơn vị vận hành hệ thống thông tin theo quy định tại Quy chế này và các nhiệm vụ do chủ quản hệ thống thông tin phân công.

2. Chỉ đạo, phân công các bộ phận kỹ thuật thuộc đơn vị (quản lý ứng dụng; quản lý dữ liệu; vận hành hệ thống thông tin; triển khai và hỗ trợ kỹ thuật) triển khai công tác bảo đảm an toàn thông tin trong tất cả các công đoạn liên quan đến hệ thống thông tin.

Điều 26. Trách nhiệm của Đội ứng cứu sự cố an toàn thông tin mạng

1. Triển khai các giải pháp nhằm hỗ trợ các cơ quan, đơn vị trên địa bàn tỉnh về công tác bảo đảm an toàn thông tin mạng, an ninh mạng trong hoạt động ứng dụng công nghệ thông tin, chuyển đổi số.

2. Phối hợp kiểm tra an toàn thông tin, an ninh mạng đối với hệ thống thông tin của các cơ quan, đơn vị.

3. Điều phối các hoạt động ứng cứu sự cố về an toàn thông tin mạng và tổ chức ứng cứu sự cố an toàn thông tin mạng tại các cơ quan, đơn vị trên địa bàn tỉnh.

Điều 27. Trách nhiệm của cán bộ, công chức, viên chức và người lao động trong các cơ quan, đơn vị

1. Trách nhiệm của cán bộ, công chức, viên chức chuyên trách về công nghệ thông tin tại cơ quan, đơn vị

a) Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác của pháp luật về an toàn thông tin mạng. Chịu trách nhiệm về các hành vi làm mất an toàn thông tin mạng do không tuân thủ Quy chế này và các quy định của pháp luật có liên quan.

b) Tham mưu lãnh đạo cơ quan ban hành các quy chế, quy trình nội bộ, triển khai các giải pháp kỹ thuật bảo đảm an toàn thông tin mạng.

c) Thực hiện việc giám sát, đánh giá, báo cáo thủ trưởng cơ quan, đơn vị các rủi ro mất an toàn thông tin mạng và mức độ nghiêm trọng của các rủi ro đó.

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

e) Thường xuyên cập nhật nâng cao kiến thức, trình độ chuyên môn đáp ứng yêu cầu bảo đảm an toàn thông tin mạng của đơn vị.

2. Công chức, viên chức được giao nhiệm vụ quản lý, vận hành truy cập, khai thác đối với các hệ thống thông tin thực hiện theo trách nhiệm và phân quyền được quy định; việc khai thác thông tin phải bảo đảm nguyên tắc bảo mật, không được tự ý cung cấp thông tin ra bên ngoài; theo dõi và phát hiện các trường hợp truy cập hệ thống trái phép hoặc thao tác vượt quá giới hạn, báo cáo cho cán bộ quản lý để tiến hành ngăn chặn, thu hồi, khóa quyền truy cập của các tài khoản vi phạm.

3. Trách nhiệm của người sử dụng

a) Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác 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) Có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng được giao sử dụng.

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

d) Tham gia các chương trình đào tạo, hội nghị về an toàn thông tin mạng được cơ quan hoặc đơn vị chuyên môn tổ chức.

Điều 28. Trách nhiệm của các tổ chức, cá nhân liên quan

Các tổ chức, cá nhân liên quan đến sử dụng, khai thác các hệ thống thông tin hoặc liên quan đến hoạt động thực hiện ứng dụng công nghệ thông tin, giao dịch điện tử, chuyển đổi số của các cơ quan nhà nước trên địa bàn tỉnh Ninh Bình phải tuân thủ Quy chế này và các quy định hiện hành của pháp luật về an toàn, an ninh thông tin mạng.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 29. Khen thưởng, kỷ luật

1. Hàng năm, Sở Thông tin và Truyền thông căn cứ kết quả kiểm tra, đánh giá, báo cáo công tác bảo đảm an toàn thông tin mạng của các cơ quan, đơn vị đề xuất UBND tỉnh xem xét khen thưởng cho các cá nhân, đơn vị có nhiều thành tích trong công tác bảo đảm an toàn thông tin mạng theo quy định hiện hành.

2. Tổ chức, cá nhân có hành vi vi phạm quy chế này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý theo quy định hiện hành

Điều 30. Tổ chức thực hiện

1. Thủ trưởng các cơ quan, đơn vị trên địa bàn tỉnh và các đơn vị liên quan có trách nhiệm tổ chức triển khai thực hiện Quy chế này trong phạm vi quản lý của mình.

2. Sở Thông tin và Truyền thông có trách nhiệm theo dõi, đôn đốc, kiểm tra, đánh giá việc thực hiện Quy chế, báo cáo UBND tỉnh theo định kỳ hằng năm hoặc đột xuất theo yêu cầu của cơ quan có thẩm quyền.

Điều 31. Sửa đổi, bổ sung Quy chế

1. Trường hợp các văn bản quy phạm pháp luật được dẫn chiếu tại Quy chế này được bãi bỏ, thay thế, sửa đổi, bổ sung thì thực hiện theo văn bản quy phạm pháp luật mới.

2. Trong quá trình thực hiện Quy chế, nếu có vấn đề vướng mắc, phát sinh, các đơn vị phản ánh kịp thời về Sở Thông tin và Truyền thông để tổng hợp báo cáo UBND tỉnh xem xét sửa đổi, điều chỉnh, cập nhật./.

PHỤ LỤC
DANH MỤC MẪU BIỂU

STT	Mẫu số	Tên Mẫu biểu
1	Mẫu số 01	Báo cáo ban đầu sự cố an toàn thông tin mạng
2	Mẫu số 02	Báo cáo kết thúc ứng phó sự cố

(Mẫu số 01)

TÊN CƠ QUAN CHỦ QUẢN
TÊN CƠ QUAN

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

Số: ….. /BC-

Ninh Bình, ngày ... tháng ... năm ...

BÁO CÁO BAN ĐẦU SỰ CỐ AN TOÀN THÔNG TIN MẠNG

I. 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 (*) .....

II. 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:

.....

III. 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

IV. 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**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: ….. /BC-	*Ninh Bình, ngày ... tháng ... năm ...*

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

I. 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: …/…/.....

II. 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)

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