ỦY BAN NHÂN DÂN HUYỆN NINH HẢI	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc
Số:1214 /QĐ-UBND	*Ninh Hải, ngày 29 tháng 10 năm 2024*

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 trên địa bàn huyện Ninh Hải

ỦY BAN NHÂN DÂN HUYỆN NINH HẢI

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 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 12 tháng 6 năm 2018;

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

Căn cứ 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;

Căn cứ Nghị định số 34/2016/NĐ-CP ngày 14 tháng 5 năm 2016 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Ban hành văn bản quy phạm pháp luật;

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 154/2020/NĐ-CP ngày 31 tháng 12 năm 2020 của Chính phủ sửa đổi, bổ sung một số điều của Nghị định số 34/2016/NĐ-CP ngày 14 tháng 5 năm 2016 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Ban hành văn bản quy phạm pháp luật;

Căn cứ Nghị định số 59/2024/NĐ-CP ngày 25 tháng 5 năm 2024 của Chính phủ sửa đổi, bổ sung một số điều của Nghị định số 34/2016/NĐ-CP ngày 14/5/2016 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Ban hành văn bản quy phạm pháp luật đã được sửa đổi, bổ sung một số điều theo Nghị định số 154/2020/NĐ-CP ngày 31/12/2020 của Chính phủ;

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 khan 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 27/2017/ TT-BTTTT ngày 20 tháng 10 năm 2017 của Bộ tnedng Bộ Thông tin và Truyền thông quy định về quản lý, vận hành, kết nổi, sử dụng và bảo đảm an toàn thông tin trên mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước;

Căn cứ Thông tư số 31/2017 TT-BTTTT ngày 15 tháng 11 năm 2017 của Bộ tnedng Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thong thông tin;

Căn cứ Thông tư số 12 2022 TT-BTTTT ngày 12' tháng 8 năm 2022 của Bộ tnedng Bộ Thông tin và Truyền thông quy định chi tiết và hưởng dân một số điều của Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chỉnh phủ về bảo đảm an toàn hệ thong thông tin theo cấp độ;

Căn cứ Quyết định số 76/2024/QĐ-UBND ngày 24/9/2024 của UBND tỉnh về Ban hành Quy chế về bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan Nhà nước trên địa bàn tỉnh Ninh Thuận;

Xét đề nghị của phòng Văn hoá và Thông tin tại Tờ trình số 42/TTr- PVHTT ngày 27 tháng 10 năm 2024,

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 các cơ quan Nhà nước trên địa bàn huyện Ninh Hải; gồm 04 Chương, 23 Điều.

Điều 2. Quyết định này có hiệu lực kể từ ngày ký.

Chánh Văn phòng HĐND và UBND huyện, Trưởng phòng Văn hóa và Thông tin, Thủ trưởng các cơ quan, đơn vị và Chủ tịch Ủy ban nhân dân các xã, thị trấn chịu trách nhiệm thi hành Quyết định này./..

Nơi nhận:
- Như Điều 2;
- UBND tỉnh;
- Sở TT&TT;
- TT. Huyện ủy;
- TT. HĐND huyện;
- Chủ tịch, PCT UBND huyện;
- Trang TTĐT huyện;
- Lưu: VT.

TM ỦY BAN NHÂN DÂN
CHỦ TỊCH

Trần Minh Thái

ỦY BAN NHÂN DÂN HUYỆN NINH HẢI	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc

QUY CHẾ
Bảo đảm an toàn thông tin mạng tronghoạt động ứng dụng công nghệ thông tin của các cơ quan Nhà nước trên địa bàn huyện Ninh Hải
(Ban hành kèm theo Quyết định số1214 /QĐ-UBND ngày29 /10/2024 của UBND huyện Ninh Hải)

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 công tác bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn huyện Ninh Hải.

2. Đối tượng áp dụng: Quy chế này được áp dụng đối với các cơ quan quản lý hành chính nhà nước và các đơn vị sự nghiệp thuộc Ủy ban nhân dân huyện Ninh Hải (sau đây gọi tắt là các cơ quan, đơn vị).

Điều 2. Giải thích từ ngữ

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

1. Mạng ngang hàng là mô hình mạng mà trong đó các máy tính có quyền bình đẳng như nhau, mỗi máy tính có quyền chia sẻ tài nguyên và sử dụng các tài nguyên từ máy tính khác.

2. *Cán bộ chuyên trách về công nghệ thông tin* là cán bộ, công chức được giao nhiệm vụ phụ trách công tác đảm bảo hạ tầng, ứng dụng, cơ sở dữ liệu và an toàn, an ninh thông tin cho việc triển khai, vận hành, khai thác hệ thống Công nghệ thông tin (CNTT) tại huyện.

Điều 3. Nguyên tắc bảo đảm an toàn thông tin

1. Tổ chức, cá nhân có trách nhiệm bảo đảm an toàn, an ninh thông tin trong mọi hoạt động ứng dụng CNTT của đơn vị mình. Bảo đảm an toàn thông tin 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 ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ *(gọi tắt là Nghị định số 85/2016/NĐ-CP).*

2. Các cơ quan, đơn vị có trách nhiệm bảo đảm an toàn thông tin mạng của đơn vị mình; bố trí nhân sự phụ trách chịu trách nhiệm bảo đảm an toàn thông tin mạng; xác định rõ quyền hạn, trách nhiệm của Thủ trưởng cơ quan, đơn vị, từng bộ phận, cá nhân trong đơn vị đối với công tác bảo đảm an toàn thông tin mạng.

3. Việc xử lý sự cố an toàn thông tin mạng phải bảo đảm quyền và lợi ích hợp pháp của tổ chức, cá nhân, không xâm phạm đến đời sống riêng tư, bí mật cá nhân, bí mật gia đình của cá nhân, thông tin riêng của tổ chức.

Điều 4. Các hành vi nghiêm cấm

1. Các hành vi nghiêm cấm 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.

2. Tự ý đấu nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập mạng không dây của cá nhân vào mạng nội bộ; trên cùng một thiết bị thực hiện đồng thời truy cập vào mạng nội bộ và truy cập Internet bằng thiết bị kết nối Internet của cá nhân (3G/4G, điện thoại di động, máy tính bảng, máy tính xách tay) khi cơ quan, đơn vị chủ quản hệ thống thông tin chưa cho phép.

3. Tự ý thay đổi, gỡ bỏ biện pháp an toàn thông tin cài đặt trên thiết bị công nghệ thông tin phục vụ công việc; tự ý thay thế, lắp mới, tráo đổi thành phần của máy tính phục vụ công việc khi cơ quan, đơn vị chủ quản hệ thống thông tin chưa cho phép.

4. Tạo ra, cài đặt, phát tán phần mềm độc hại.

5. Bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã và thông tin của cơ quan, cá nhân khác trên môi trường mạng.

6. Các hành vi khác có tính chất cố tình làm mất an toàn, bí mật thông tin của cơ quan, cá nhân khác được trao đổi, truyền đưa, lưu trữ trên môi trường mạng.

Chương II

QUY ĐỊNH BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Điều 5. Yêu cầu thiết kế, xây dựng hệ thống thông tin

1. Khi thiết kế xây dựng, nâng cấp, mở rộng hệ thống thông tin, chủ quản hệ thống thông tin phải xây dựng phương án bảo đảm an toàn thông tin trong hồ sơ thiết kế và gửi đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin thẩm định (hoặc đơn vị chuyên trách về an toàn thông tin của Ủy ban nhân dân tỉnh) trước khi trình cấp có thẩm quyền phê duyệt dự án.

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 tổ chức đánh giá, phân loại cấp độ an toàn thông tin của hệ thống thông tin theo quy định tại Chương II Nghị định số 85/2016/NĐ-CP để áp dụng phương án bảo đảm an toàn thông tin phù hợp.

b) Hồ sơ đề xuất cấp độ bao gồm các tài liệu được quy định tại Điều 15 Nghị định số 85/2016/NĐ-CP, gửi đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin hoặc đơn vị chuyên trách về an toàn thông tin của Ủy ban nhân dân tỉnh thẩm định, trình cấp có thẩm quyền phê duyệt.

3. Trước khi đưa vào vận hành, khai thác hệ thống thông tin, chủ quản hệ thống thông tin phải thực hiện kiểm thử hoặc vận hành thử trước khi đưa vào sử dụng. Kết quả kiểm thử, vận hành thử phải được lập thành văn bản và tuân thủ theo quy định tại Điều 10 Thông tư số 24/2020/TT-BTTTT ngày 09/9/2020 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về công tác triển khai, giám sát công tác triển khai và nghiệm thu dự án đầu tư ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách Nhà nước.

Điều 6. 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) Quản lý thông tin, dữ liệu phát sinh từ dịch vụ đó, không để bên cung cấp dịch vụ truy nhập, sử dụng thông tin, dữ liệu thuộc phạm vi Nhà nước quả lý.

b) 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 và các quy định khác có liên quan.

c) 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. Bảo vệ bí mật Nhà nước trong hoạt động ứng dụng công nghệ thông tin

1. Quy định về soạn thảo, in ấn, phát hành và sao chụp tài liệu mật:

a) Không được sử dụng máy tính hoặc các thiết bị khác đã kết nối hoặc đang kết nối với mạng Internet, mạng máy tính, mạng viễn thông, trừ trường hợp lưu trữ bí mật nhà nước theo quy định của pháp luật về cơ yếu để soạn thảo, chuyển giao,

lưu trữ tài liệu có nội dung bí mật Nhà nước; cung cấp tin, tài liệu có nội dung bí mật Nhà nước trên mạng xã hội (zalo; Telegram; Facebook; ...) và đưa thông tin có nội dung bí mật Nhà nước trên Trang thông tin điện tử huyện.

b) Không được in, sao chụp tài liệu có nội dung bí mật Nhà nước trên các thiết bị có kết nối mạng internet, mạng máy tính, mạng viễn thông, trừ trường hợp theo quy định của pháp luật về cơ yếu.

c) Phải bố trí ít nhất 01 máy tính riêng và phải được kiểm tra an ninh, an toàn thông tin, không kết nối mạng Internet, mạng máy tính, mạng viễn thông, trừ trường hợp theo quy định của pháp luật về cơ yếu dùng để quản lý, lưu trữ, soạn thảo các tài liệu có nội dung bí mật Nhà nước.

2. Khi sửa chữa, khắc phục các sự cố của máy tính dùng soạn thảo, lưu trữ tài liệu có nội dung bí mật nhà nước, các phòng, ban, đơn vị phải báo cáo cho người có thẩm quyền cho ý kiến. Không được thuê, hợp đồng, cho phép các tổ chức, cá nhân không có trách nhiệm trực tiếp sửa chữa, xử lý, khắc phục sự cố.

3. Trước khi thanh lý các máy tính trong các cơ quan Nhà nước, cán bộ chuyên trách về công nghệ thông tin phải tháo ổ cứng (thanh lý không kèm ổ cứng hoặc các thiết bị lưu trữ khác gắn kèm) và dùng các biện pháp kỹ thuật chuyên biệt để xoá bỏ vĩnh viễn dữ liệu lưu trữ trong ổ cứng, các thiết bị lưu trữ khác gắn kèm hoặc phá hủy về mặt vật lý ổ cứng, các thiết bị lưu trữ khác nếu chứa các tài liệu có nội dung bí mật Nhà nước.

Điều 8. Quy định về cấp phát, thu hồi, cập nhật và quản lý các tài khoản truy cập vào hệ thống thông tin dùng chung của tỉnh

1. Mỗi cán bộ, đơn vị được cấp một tài khoản truy cập các ứng dụng dùng chung của tỉnh từ Hệ thống định danh tập trung, tài khoản truy cập với định danh duy nhất gắn với cá nhân đó, đơn vị đó chỉ truy cập vào các Trang/Cổng thông tin điện tử, ứng dụng trực tuyến và các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình. Trường hợp sử dụng tài khoản dùng chung cho một nhóm người hay một đơn vị, phải có cơ chế xác định các cá nhân, đơn vị có trách nhiệm quản lý tài khoản. Người dùng chỉ được truy cập các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình và có trách nhiệm bảo mật tài khoản truy cập được cấp.

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

3. Trường hợp cán bộ thay đổi vị trí công tác, chuyển công tác, thôi việc hoặc nghỉ hưu, trong vòng không quá 05 ngày làm việc sau khi có quyết định của cấp có thẩm quyền thì cơ quan, đơn vị quản lý cá nhân đó phải thông báo Trung tâm Công nghệ thông tin và Truyền thông để điều chỉnh, thu hồi, hủy bỏ các quyền sử dụng đối với hệ thống thông tin.

4. Mật mã đăng nhập, truy cập hệ thống thông tin phải đặt theo quy định tại Điều 7 của Quyết định số 381/QĐ-UBND ngày 01 tháng 7 năm 2022 của Ủy ban nhân dân tỉnh Quy chế thiết lập, quản lý và sử dụng tên tài khoản truy cập các ứng dụng dùng chung của tỉnh Ninh Thuận.

Điều 9. Bảo đảm nguồn nhân lực

1. Cán bộ chuyên trách về công nghệ thông tin được tuyển dụng vào vị trí làm về an toàn thông tin có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, an toàn thông tin, phù hợp với vị trí tuyển dụng.

2. Cán bộ chuyên trách về công nghệ thông tin được bảo đảm các điều kiện học tập, tiếp cận công nghệ, kiến thức an toàn bảo mật thông tin trước khi tiến hành các hoạt động quản lý hay kỹ thuật nghiệp vụ.

3. Cán bộ 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.

Điều 10. Bảo đảm an toàn hạ tầng mạng

1. Quản lý hạ tầng mạng nội bộ:

a) Tuân thủ các quy định kiến trúc hệ thống, tiêu chuẩn, quy chuẩn kỹ thuật; cài đặt, cấu hình, tổ chức hệ thống mạng phù hợp với các tiêu chuẩn ứng dụng công nghệ thông tin của các cơ quan Nhà nước, bảo đảm an toàn thông tin; hạn chế sử dụng mô hình mạng có nguy cơ mất an toàn thông tin cao.

b) Tổ chức mô hình mạng: Cài đặt, cấu hình, tổ chức hệ thống mạng theo mô hình Máy khách/Máy chủ (Client/Server), hạn chế sử dụng mô hình mạng ngang hàng. Trang bị thiết bị tường lửa hoặc phần mềm tường lửa để ngăn chặn và phát hiện xâm nhập trái phép vào mạng nội bộ của cơ quan, đơn vị khi kết nối với hệ thống bên ngoài; ưu tiên sử dụng các sản phẩm, giải pháp, dịch vụ an toàn thông tin mạng do doanh nghiệp Việt Nam sản xuất hoặc làm chủ công nghệ.

c) Đối với các phòng, ban, đơn vị trực thuộc không nằm cùng một khu vực thì cần thiết lập mạng riêng ảo (VPN) để tăng cường an ninh cho hạ tầng mạng nội bộ. Khi thiết lập các dịch vụ trên môi trường mạng Internet, chỉ cung cấp những chức năng thiết yếu nhất bảo đảm duy trì hoạt động của hệ thống thông tin; hạn chế sử dụng/mở cổng giao tiếp mạng, giao thức và các dịch vụ không cần thiết.

d) Khi thực hiện truy cập từ xa vào mạng nội bộ để thực hiện chức năng quản trị, phải sử dụng giao thức mạng có mã hóa thông tin (như: SSL/TLS, VPN...) và thiết lập mật khẩu có độ phức tạp cao.

đ) Xây dựng quy trình kết nối thiết bị đầu cuối của người sử dụng vào hệ thống mạng; truy cập và quản lý cấu hình hệ thống; cấu hình tối ưu, tăng cường bảo mật cho thiết bị mạng, bảo mật trong hệ thống và thực hiện quy trình trước khi đưa hệ thống vào vận hành khai thác.

e) Cá nhân, tổ chức phải có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng.

2. Quản lý hệ thống mạng không dây:

a) Khi thiết lập mạng không dây để kết nối với mạng cục bộ thông qua các điểm truy nhập (Access Point - AP), cơ quan, đơn vị vận hành phải thiết lập các tham số: Tên, nhận dạng dịch vụ (Service Set Identifier - SSID), mật khẩu phải đặt theo quy định tại Điều 7 của Quyết định số 381/QĐ-UBND ngày 01 tháng 7 năm 2022, cấp phép truy nhập đối với địa chỉ vật lý (MAC Address), mã hóa dữ liệu theo cơ chế bảo mật WPA2 hoặc WPA3.

b) Mật khẩu đăng nhập phải được thiết lập có độ phức tạp cao, định kỳ 6 tháng thay đổi mật khẩu nhằm tăng cường công tác bảo mật.

c) Khi cung cấp truy cập Internet qua mạng không dây cho Camera hoặc người ngoài, cơ quan, đơn vị sử dụng phải phân VLAN riêng với một SSID riêng và giới hạn băng thông truy cập phù hợp đối với đối tượng.

Điều 11. Bảo đảm an toàn máy chủ và ứng dụng

1. Trên hệ thống máy chủ:

a) Hệ điều hành được cài đặt là phần mềm có bản quyền (bao gồm bản quyền thương mại hoặc mã nguồn mở có nguồn gốc rõ ràng), các dịch vụ cài đặt trên máy chủ là các dịch vụ được sử dụng dùng chung cho cơ quan, đơn vị, không cài đặt các dịch vụ không sử dụng.

b) Thiết lập chế độ tự động cập nhật phiên bản và 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 cập chế độ tự động bảo vệ màn hình sau 10 phút không sử dụng đối với tất cả máy chủ.

c) Các máy chủ cần được cài đặt mật khẩu ở phần cấu hình (setup) của BIOS (Basic Input/Output System), trong đó lưu ý việc vô hiệu hóa các cổng USB trên máy chủ.

2. Cơ quan chủ quản có trách nhiệm trang bị phần mềm phòng, chống mã độc (Antivirus) có bản quyền cho hệ thống máy chủ; cơ quan, đơn vị vận hành thiết lập chế độ tự động cập nhật phiên bản mới, các bản vá lỗi; chế độ tự động quét mã độc khi sao chép, mở các tập tin; chế độ quét toàn bộ máy tính định kỳ hằng tuần.

3. Định kỳ hằng tuần, cơ quan, đơn vị vận hành phải kiểm tra các tiến trình trên máy chủ nhằm sớm phát hiện nguy cơ cài cắm phần mềm độc hại trên máy chủ.

Điều 12. Bảo đảm an toàn dữ liệu

1. Quản lý tài khoản:

Chủ tài khoản không chia sẻ, giao quyền tài khoản và mật khẩu truy nhập cho người khác. Không sử dụng tài khoản của người khác để đăng nhập vào hệ thống thông tin, cơ sở dữ liệu.

a) Tài khoản thư điện tử công vụ tỉnh (xxx@ninhthuan.gov.vn) để phục vụ cho các hoạt động mang tính công vụ, không sử dụng để giao dịch, đăng ký trên mạng xã hội, các trang thông tin điện tử công cộng khác; định kỳ 01 năm kiểm tra việc lưu trữ của hệ thống thư điện tử, tiến hành xóa các email quá cũ, không cần thiết để bảo đảm hệ thống hoạt động ổn định thông suốt.

b) Tài khoản quản trị hệ thống được giao cho cán bộ chuyên trách về công nghệ thông tin phục vụ cho công tác quản trị, phân quyền, cấu hình hệ thống đó. Cán bộ quản trị hệ thống không sử dụng cùng một mật khẩu cho nhiều tài khoản khác nhau;

c) Khi cá nhân thay đổi vị trí công tác, chuyển công tác, thôi việc, nghỉ hưu thì cơ quan, đơn vị vận hành thực hiện khoản 4 Điều 8 Quy chế này về điều chỉnh, thu hồi, hủy bỏ tài khoản.

d) Thông tin, dữ liệu thuộc phạm vi bí mật Nhà nước phải được quản lý theo Điều 7 của Quy chế này.

Điều 13. Bảo đảm an toàn thiết bị 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 cập 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. Khuyến khích các cơ quan, đơn vị đầu tư, mua sắm thiết bị công nghệ thông tin sản xuất trong nước.

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, đơn vị;

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 của cơ quan, đơn vị. Các máy tính truy cập mạng Internet phải cài đặt phần mềm giám sát mã độc tập trung của Sở Thông tin và Truyền thông triển khai.

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 cán bộ 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.

Điều 14. Quản lý giám sát an toàn hệ thống thông tin

1. Chủ quản hệ thống thông tin phải triển khai hệ thống giám sát an toàn thông tin đáp ứng các yêu cầu tại Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin.

2. Định kỳ hàng năm tổ chức đánh giá, kiểm tra đối với hệ thống thông tin nội bộ tại cơ quan, đơn vị. Thực hiện các biện pháp bảo trì cần thiết để bảo đảm khả năng xử lý và tính sẵn sàng của hệ thống thông tin.

Điều 15. Ứng cứu sự cố an toàn thông tin

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.

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

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

2. Phân nhóm sự cố an toàn thông tin:

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

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

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

d) Sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn. Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin: Hoạt động ứng cứu sự cố an toàn thông tin mạng huy động các nguồn lực nằm ngoài phạm vi của đơn vị vận hành hệ thống thông tin để đối phó với các sự cố quy định tại khoản 1 điều này.

3. Phân loại mức độ nghiêm trọng 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, đơn vị.

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, đơn vị.

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, đơn

vị 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, đơn vị và 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, đơn vị và người dân, doanh nghiệp, đe dọa trật tự an toàn xã hội.

4. Quy trình phối hợp ứng cứu xử lý sự cố:

a) Bước 1: Nếu hệ thống có nguy cơ mất an toàn thông tin mạng thuộc thẩm quyền cơ quan, đơn vị trực tiếp quản lý thì thực hiện tiếp Bước 2. Nếu hệ thống có nguy cơ mất an toàn thông tin mạng thuộc Trung tâm Công nghệ thông tin và Truyền thông trực thuộc Sở Thông tin và Truyền thông quản lý (các hệ thống được triển khai tập trung tại Trung tâm tích hợp Dữ liệu tỉnh) thì thực hiện tiếp Bước 3.

b) Bước 2: Tiến hành xử lý sự cố theo quy chế nội bộ của cơ quan, đơn vị. Nếu sự cố được khắc phục thì lập biên bản ghi nhận và kết thúc quy trình phối hợp xử lý sự cố. Khi sự cố vượt quá khả năng xử lý của cơ quan, đơn vị, lập biên bản ghi nhận và thực hiện tiếp Bước 3.

c) Bước 3: Báo sự cố về UBND huyện (qua Phòng Văn hóa và Thông tin) theo mẫu số 01 kèm theo Quy chế.

d) Bước 4: Phối hợp với Phòng Văn hóa và Thông tin và các cơ quan, đơn vị, tổ chức có liên quan để tiến hành khắc phục sự cố và thực hiện tiếp Bước 5.

đ) Bước 5: Lập biên bản ghi nhận và kết thúc quy trình phối hợp xử lý sự cố theo mẫu số 02 kèm theo Quy chế này. Lãnh đạo cơ quan, đơn vị phải chỉ đạo kịp thời để khắc phục và hạn chế thiệt hại, báo cáo bằng văn bản cho UBND huyện (qua Phòng Văn hóa và Thông tin).

5. Trường hợp có sự cố nghiêm trọng ở mức độ cao, khẩn cấp hoặc vượt quá khả năng khắc phục của Phòng Văn hóa và Thông tin tham mưu UBND huyện báo cáo ngay Sở Thông tin và Truyền thông để được hướng dẫn, hỗ trợ.

6. Phòng Văn hóa và Thông tin là cơ quan chuyên trách về an toàn thông tin có trách nhiệm:

a) 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) Thực hiện 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, hỗ trợ cung cấp quy trình xử lý sự cố cho các dịch vụ do bên cung cấp, hỗ trợ cung cấp liên quan đến hệ thống.

d) Tham gia diễn tập phương án xử lý sự cố an toàn thông tin theo chỉ đạo của ngành cấp trên.

Chương III
KIỂM TRA ĐÁNH GIA CÔNG TÁC ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG

Điều 16. Kế hoạch kiểm tra hàng năm

1. Phòng Văn hóa và Thông tin chủ trì, phối hợp với Văn phòng HĐND và UBND huyện, Công an huyện và các đơn vị liên quan tiến hành kiểm tra công tác đảm bảo an toàn thông tin đối với các cơ quan, đơn vị trên địa bàn huyện theo Kế hoạch công tác hằng năm.

2. Tiến hành kiểm tra đột xuất các cơ quan, đơn vị khi có dấu hiệu vi phạm an toàn đối với các hệ thống thông tin trên địa bàn huyện.

Điều 17. Nội dung hình thức kiểm tra đánh giá hệ thống thông tin:

1. Nội dung kiểm tra, đánh giá:

a) Kiểm tra việc thực theo các nội dung theo Quy chế này; việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin; kiểm tra hiệu quả của các biện pháp bảo đảm an toàn thông tin.

b) Đánh giá hiệu quả của biện pháp bảo đảm an thông tin tại đơn vị; phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống.

c) Kiểm tra, đánh giá các nội dung khác theo quy định hệ thống an toàn thông tin.

2. Hình thức kiểm tra, đánh giá:

a) Kiểm tra, đánh giá định kỳ theo kế hoạch của UBND huyện và đơn vị chuyên trách về an toàn thông tin của tỉnh.

b) Kiểm tra, đánh giá đột xuất theo yêu cầu của cấp có thẩm quyền.

3. Cấp có thẩm quyền yêu cầu kiểm tra, đánh giá:

a) Đơn vị chuyên trách ATTT tại Trung ương.

b) Ủy ban nhân dân tỉnh hoặc Sở Thông tin và Truyền thông (đơn vị chuyên trách về an toàn thông tin trên địa bàn tỉnh).

c) UBND huyện giao nhiệm vụ kiểm tra về an toàn thông tin trên địa bàn huyện cho Phòng Văn hóa và Thông tin.

4. Đơn vị chủ trì kiểm tra, đánh giá là đơn vị được cấp có thẩm quyền giao nhiệm vụ hoặc được lựa chọn để thực hiện nhiệm vụ kiểm tra, đánh giá.

5. Đối tượng kiểm tra, đánh giá là các ban, ngành, đơn vị hoạt động sự nghiệp thuộc UBND huyện.

Chương IV

TRÁCH NHIỆM BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG VÀ TỔ CHỨC THỰC HIỆN

Điều 18. Trách nhiệm của Phòng Văn hóa và Thông tin

1. Tham mưu Ủy ban nhân dân huyện về công tác bảo đảm an toàn thông tin trên địa bàn huyện và chịu trách nhiệm trước Ủy ban nhân dân huyện trong việc bảo đảm an toàn thông tin.

2. Tham mưu Ủy ban nhân dân huyện xây dựng hồ sơ đề xuất cấp độ an toàn thông tin và 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 các cơ quan, đơn vị có liên quan tiến hành kiểm tra công tác bảo đảm an toàn thông tin mạng định kỳ hàng năm hoặc theo chỉ đạo của Ủy ban nhân dân huyện đối với các cơ quan nhà nước đóng trên địa bàn huyện.

4. Hàng năm, cử cán bộ tham gia các lớp đào tạo, tập huấn về công tác bảo đảm an toàn thông tin mạng cho cán bộ phụ trách an toàn thông tin mạng. Tổ chức tuyên truyền về an toàn thông tin mạng trong công tác quản lý nhà nước trên địa bàn huyện.

5. Phối hợp với Công an huyện có các biện pháp phòng, chống các thông tin vi phạm pháp luật, ảnh hưởng đến an ninh quốc gia, trật tự, an toàn xã hội trên môi trường mạng, nhất là trên các cổng/trang thông tin điện tử, mạng xã hội.

6. Là cơ quan đầu mối thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin mạng trên địa bàn huyện.

Điều 19. Trách nhiệm của Văn phòng HĐND và UBND huyện

1. Tham mưu UBND huyện 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 cán 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.

3. Phối hợp với Công an huyện và Phòng Văn hóa và Thông tin thực hiện biện pháp phòng, chống các thông tin vi phạm pháp luật, ảnh hưởng đến an ninh quốc gia, trật tự, an toàn xã hội trên môi trường mạng, nhất là trên các cổng/trang thông tin điện tử, mạng xã hội.

4. Cử cán bộ tham gia các lớp đào tạo, tập huấn về công tác bảo đảm an toàn thông tin mạng.

Điều 20. Trách nhiệm của các cơ quan, đơn vị và UBND các xã, thị trấn

1. Thủ trưởng các cơ quan, đơn vị; Chủ tịch UBND các xã, thị trấn có trách nhiệm tổ chức thực hiện các quy định tại Quy chế này và chịu trách nhiệm trong

công tác bảo đảm an toàn thông tin mạng của cơ quan, đơn vị mình; 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.

2. Phân công cán bộ thực hiện việc 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; thường xuyên tổ chức quán triệt các quy định về an toàn thông tin trong cơ quan, đơn vị.

3. Thực hiện bảo đảm an toàn thông tin 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.

4. 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.

5. Phối hợp chặt chẽ với Công an huyện, Phòng Văn hóa và Thông tin 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.

6. 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 mua phần mềm chống virus có bản quyền phần mềm... nhằm thực hiện tốt công tác bảo mật, bảo đảm an toàn thông tin mạng đưa vào dự toán chi để triển khai thực hiện.

7. Phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin.

8. Thực hiện các báo cáo về an toàn thông tin mạng khi UBND huyện có yêu cầu.

Điều 21. 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 phụ trách về an toàn thông tin/công nghệ thông tin tại cơ quan, đơn vị:

a) Chịu trách nhiệm bảo đảm an toàn thông tin mạng của cơ quan, đơn vị;

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.

đ) 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. 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 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 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 đơn vị chuyên môn tổ chức.

Điều 22. Trách nhiệm của các tổ chức, cá nhân liên quan

Các tổ chức, cá nhân khác có sử dụng các hệ thống thông tin do Ủy ban nhân dân huyện triển khai hoặc liên quan đến hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước của huyện phải tuân thủ Quy chế này và các quy định hiện hành của pháp luật có liên quan.

Điều 23. Tổ chức thực hiện

1. Căn cứ Quy chế này, thủ trưởng các cơ quan, đơn vị trên địa bàn huyện 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. Phòng Văn hóa và Thông tin có trách nhiệm theo dõi, đôn đốc, kiểm tra, đánh giá việc thực hiện Quy chế, báo cáo Ủy ban nhân dân huyện theo định kỳ hằng năm hoặc đột xuất theo yêu cầu của UBND huyện và cơ quan có thẩm quyền của tỉnh.

3. Trong quá trình thực hiện quy chế, nếu có vấn đề vướng mắc, phát sinh, các đơn vị phản ánh kịp thời về Phòng Văn hóa và Thông tin để tổng hợp báo cáo Ủy ban nhân dân huyện xem xét điều chỉnh, bổ sung./.

PHỤ LỤC

Danh mục mẫu quy định ứng cứu sự cố an toàn thông tin mạng trên địa bàn huyện

(Ban hành kèm theo Quyết định ……../QĐ-UBND ngày tháng năm 2024 của Ủy ban nhân dân huyện Ninh Hải)

STT	Mẫu số	Tên Mẫu biểu
1	Mẫu số 01	Báo cáo 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, TỔ CHỨC CHỦ QUẢN CẤP TRÊN TRỰC TIẾP
TÊN CƠ QUAN, TỔ CHỨC

Số:…….

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

……, ngày……tháng…..năm…..

BÁO CÁO 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 chủ quản:	*Điền tên cơ quan chủ quản*				
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 1	☐ Cấp 2	☐ Cấp 3	☐ Cấp 4	☐ Cấp 5
Tổ chức cung cấp dịch vụ an toàn thông tin (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 dân đến khả năng phá hoại hoặc gián đoạn dịch vụ. Cũng vui lòng xác định mức độ nhạy cảm của thông tin liên quan hoặc những đối tượng bị ảnh hưởng bởi sự cố: …… …… …… …… ……	
Ngày phát hiện sự cố (*) (dd/mm/yyyy) …../…../…..	Thời gian phát hiện (*):…..giờ…..phút

HIỆN TRẠNG SỰ CỐ (*)

☐ Đã được xử lý ☐ Chưa được xử lý

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

☐ Qua hệ thống phát hiện xâm nhập ☐ Kiểm tra dữ liệu lưu lại (Log File)

☐ Nhận được thông báo từ: .....

☐ Khác, đó là .....

ĐÃ GỬI THÔNG BÁO SỰ CỐ CHO *

☐ Thành viên mạng lưới chịu trách nhiệm ứng cứu sự cố cho tổ chức, cá nhân

☐ ISP đang trực tiếp cung cấp dịch vụ

☐ Cơ quan điều phối

THÔNG TIN BỔ SUNG VỀ HỆ THỐNG XẢY RA SỰ CỐ

Hệ điều hành Version ……

Các dịch vụ có trên hệ thống *(Đánh dấu những dịch vụ được sử dụng trên hệ thống)*

☐ Web Server ☐ Mail Server ☐ Database Server

☐ Dịch vụ khác, đó là .....

Các biện pháp an toàn thông tin đã triển khai (*Đánh dấu những biện pháp đã triển khai*)

☐ Antivirus ☐ Firewall ☐ Hệ thống phát hiện xâm nhập

☐ Khác:……..

Các địa chỉ IP của hệ thống

(Liệt kê địa chỉ IP sử dụng trên Internet, không liệt kê địa chỉ IP nội bộ)
Các tên miền của hệ thống

Mục đích chính sử dụng hệ thống :……..

Thông tin gửi kèm:……

☐ Nhật ký hệ thống ☐ Mẫu virus/mã độc

☐ Khác: .....

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

☐ Có ☐ Không

KIẾN NGHỊ, ĐỀ XUẤT HỖ TRỢ

Mô tả về đề xuất, kiến nghị
Đề nghị cung cấp tóm lược về các kiến nghị và đề xuất hỗ trợ ứng cứu (nếu có) …….. …….. …….. …….. …….. ……..

THỜI GIAN THỰC HIỆN BÁO CÁO SỰ CỐ

(ngày/tháng/năm/giờ/phút):

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

MẪU SỐ 02

TÊN CƠ QUAN, TỔ CHỨC CHỦ QUẢN CẤP TRÊN TRỰC TIẾP
TÊN CƠ QUAN, TỔ CHỨC

Số:…….

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

……, ngày……tháng…..năm…..

BÁO CÁO KẾT THÚC ỨNG PHÓ SỰ CỐ

THÔNG TIN VỀ TỔ CHỨC/CÁ NHÂN BÁO CÁO

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

Địa chỉ: (*) ……

Điện thoại (*) …… ……...Email (*) ……

KÝ HIỆU BÁO CÁO BAN ĐẦU SỰ CỐ

Số ký hiệu.....Ngày báo cáo: / / 20….

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 chủ quản:	*Điền tên cơ quan chủ quản*				
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					
Ngày phát hiện sự cố / / (dd/mm/yy)		Thời gian phát hiện (*):		.... giờ.... phút	
Kết quả xử lý sự cố					
Cung cấp, tóm tắt tổng quát về những gì đã xảy ra và cách thức giải quyết, đề xuất giải pháp ứng cứu ứng sự cố nhằm xử lý nhanh sự cố, giảm nhẹ rủi ro và thiệt hại đối với sự cố tương tự trong tương lai...					
Các tài liệu đính kèm Liệt kê các tài liệu liên quan (báo cáo diễn biến sự cố; phương án xử lý, log file….)					

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