| ỦY BAN NHÂN DÂN<br>TỈNH ĐỒNG NAI | CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM<br>Độc lập – Tự do – Hạnh phúc |
|---|---|
| Số: 48 /2018/QĐ-UBND | *Đồng Nai, ngày 07 tháng 11 năm 2018* |

# 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 tỉnh Đồng Nai**

## ỦY BAN NHÂN DÂN TỈNH ĐỒNG NAI

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

*Căn cứ Luật Ban hành văn bản quy phạm pháp luật ngày 22 tháng 6 năm 2015;*

*Căn cứ Luật Giao dịch điện tử ngày 29 tháng 11 năm 2005;*

*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 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 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 142/2016/NĐ-CP ngày 14 tháng 10 năm 2016 của Chính phủ về ngăn chặn xung đột thông tin trên mạng;*

*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 03/2017/TT-BTTTT ngày 24 tháng 4 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông về quy định chi tiết và hướng dẫn một số điều của 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;*

*Căn cứ 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;*

*Căn cứ Thông tư số 27/2017/TT-BTTTT ngày 20 tháng 10 năm 2017 của Bộ Thông tin và Truyền thông quy định về việc quản lý vận hành, sử dụng và*

*bảo đảm an toàn thông tin trên mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước;*

*Theo đề nghị của Giám đốc Sở Thông tin và Truyền thông tại Tờ trình số 1843/TTr-STTTT ngày 14 tháng 9 năm 2018.*

**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 tỉnh Đồng Nai.

**Điều 2.** Quyết định này có hiệu lực thi hành kể từ ngày 01 tháng 01 năm 2019 và thay thế Quyết định số 02/2014/QĐ-UBND ngày 14/01/2014 của UBND tỉnh ban hành Quy chế Đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan quản lý hành chính nhà nước trên địa bàn tỉnh Đồng Nai.

**Điều 3.** Chánh Văn phòng UBND tỉnh, Giám đốc Sở Thông tin và Truyền thông, Thủ trưởng các sở, ban, ngành, Chủ tịch UBND các huyện, thị xã Long Khánh, thành phố Biên Hòa có trách nhiệm thi hành Quyết định này./.

***Nơi nhận*:**
- VP. Chính phủ;
- Bộ Thông tin và Truyền thông;
- Cục Kiểm tra văn bản - Bộ Tư pháp;
- Thường trực: TU, HĐND tỉnh;
- Chủ tịch và các PCT. UBND tỉnh;
- Văn phòng: Tỉnh ủy, HĐND tỉnh;
- Như Điều 3;
- Các PCVP.UBND tỉnh;
- Sở Tư pháp;
- Trung tâm Công báo tỉnh;
- Trung tâm HCC;
- Lưu: VT, CNN, TT-TH.

*(Khoa.Cnn/650.QdantoanTTmang)*

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

**Trần Văn Vĩnh**

| ỦY BAN NHÂN DÂN<br>TỈNH ĐỒNG NAI | CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM<br>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 trên địa bàn tỉnh Đồng Nai**

*(Ban hành kèm theo Quyết định số 48 /2018/QĐ-UBND ngày 07 tháng 11 năm 2018 của Ủy ban nhân dân tỉnh Đồng Nai)*

## Chương I
## QUY ĐỊNH CHUNG

**Điều 1. Phạm vi điều chỉnh**

1. Quy chế này quy định bảo đảm an toàn thông tin mạng, bao gồm: Bảo vệ thông tin cá nhân; bảo vệ hệ thống thông tin mạng; giám sát an toàn hệ thống thông tin; ngăn chặn xung đột thông tin trên mạng; đảm bảo an toàn thông tin nội bộ; quy trình ứng cứu, khắc phục sự cố mạng; quản lý và sử dụng thiết bị soạn thảo, lưu trữ văn bản mật của các cơ quan Nhà nước trên địa bàn tỉnh Đồng Nai.

2. Quy định chi tiết và hướng dẫn an toàn thông tin theo cấp độ. Hệ thống thông tin cấp độ 4, 5 không thuộc phạm vi điều chỉnh của Quy chế này.

**Điều 2. Đối tượng áp dụng**

1. Các sở, ban, ngành cấp tỉnh; các đơn vị sự nghiệp công lập trực thuộc UBND tỉnh; UBND các huyện, thị xã Long Khánh, thành phố Biên Hòa; UBND các xã, phường, thị trấn trên địa bàn tỉnh (gọi tắt là các cơ quan, đơn vị).

2. Cán bộ, công chức, viên chức, người lao động (gọi tắt là công chức viên chức) và các tổ chức, cá nhân có liên quan tham gia vận hành, khai thác các hệ thống thông tin tại cơ quan, đơn vị quy định tại Khoản 1 Điều này.

3. Các doanh nghiệp cung cấp dịch vụ viễn thông, công nghệ thông tin (Sau đây viết tắt là CNTT), internet; các doanh nghiệp, tổ chức, cá nhân có tham gia vào các hoạt động ứng dụng CNTT của các cơ quan, đơn vị thuộc Khoản 1 Điều này.

4. Khuyến khích các cơ quan, đơn vị khác hoạt động ứng dụng và phát triển CNTT trên địa bàn tỉnh áp dụng quy chế này.

**Điều 3. Giải thích từ ngữ**

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

1. An toàn thông tin mạng là sự bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái

phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

2. Mạng là môi trường trong đó thông tin được cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông qua mạng viễn thông và mạng máy tính.

3. Hệ thống thông tin là tập hợp phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên mạng.

4. Xâm phạm an toàn thông tin mạng là hành vi truy nhập, sử dụng, tiết lộ, làm gián đoạn, sửa đổi, phá hoại trái phép thông tin, hệ thống thông tin

5. Nguy cơ mất an toàn thông tin là những nhân tố bên trong hoặc bên ngoài có khả năng ảnh hưởng tới trạng thái an toàn thông tin.

6. Sự cố an toàn thông tin mạng là việc thông tin, hệ thống thông tin bị gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng.

7. Xung đột thông tin là việc hai hoặc nhiều tổ chức trong nước và nước ngoài sử dụng biện pháp công nghệ, kỹ thuật thông tin gây tổn hại đến thông tin, hệ thống thông tin trên mạng.

8. Phần mềm độc hại là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay toàn bộ hệ thống thông tin hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong hệ thống thông tin.

9. Hệ thống lọc phần mềm độc hại là tập hợp phần cứng, phần mềm được kết nối vào mạng để phát hiện, ngăn chặn, lọc và thống kê phần mềm độc hại

10. Tính toàn vẹn là bảo vệ sự chính xác và đầy đủ của thông tin và các phương pháp xử lý.

11. Tính sẵn sàng là đảm bảo những người được cấp quyền có thể truy nhập thông tin và các tài sản liên quan ngay khi có nhu cầu.

12. Cấu hình chuẩn là cấu hình được các nhà sản xuất thiết bị, phần mềm, khuyến nghị áp dụng, nhằm loại bỏ các xung đột, lỗ hổng có thể xảy ra trong quá trình cấu hình thiết bị.

13. Cổng giao tiếp (Port) là để định danh các ứng dụng gửi và nhận dữ liệu, mỗi ứng dụng sẽ tương ứng với một cổng giao tiếp, những ứng dụng phổ biến được đặt với số hiệu cổng định trước, nhằm định danh duy nhất các ứng dụng đó. Khi máy tính sử dụng dịch vụ nào thì cổng giao tiếp tương ứng với dịch vụ đó sẽ mở.

14. Bản ghi nhật ký hệ thống (Logfile) là một tập tin được tạo ra trên mỗi thiết bị của hệ thống thông tin như: Tường lửa, máy chủ ứng dụng,... có chứa tất cả thông tin về các hoạt động xảy ra trên thiết bị đó. Bản ghi nhật ký hệ thống dùng để phân tích những sự kiện đã xảy ra, nguồn gốc và các kết quả để có các biện pháp xử lý thích hợp.

15. Mạng ngang hàng là 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.

16. Thông tin cá nhân là thông tin gắn với việc xác định danh tính của một người cụ thể.

17. Xử lý thông tin cá nhân là việc thực hiện một hoặc một số thao tác thu thập, biên tập, sử dụng, lưu trữ, cung cấp, chia sẻ, phát tán thông tin cá nhân trên mạng nhằm mục đích thương mại.

**Điều 4. Nguyên tắc bảo đảm an toàn thông tin mạng**

1. Cơ quan, tổ chức, cá nhân có trách nhiệm bảo đảm an toàn thông tin mạng. Hoạt động an toàn thông tin mạng của cơ quan, tổ chức, cá nhân phải đúng quy định của pháp luật, bảo đảm quốc phòng, an ninh quốc gia, bí mật nhà nước, giữ vững ổn định chính trị, trật tự, an toàn xã hội và thúc đẩy phát triển kinh tế - xã hội.

2. Tổ chức, cá nhân không được xâm phạm an toàn thông tin mạng của tổ chức, cá nhân khác.

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.

4. Hoạt động an toàn thông tin mạng phải được thực hiện thường xuyên, liên tục, kịp thời và hiệu quả.

## Chương II
## NỘI DUNG BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

**Điều 5. Bảo vệ thông tin cá nhân**

1. Công chức viên chức có trách nhiệm tự bảo vệ thông tin cá nhân của mình và tuân thủ các quy định tại Khoản 1, Khoản 2 Điều 10; Khoản 1, Khoản 4 Điều 16; Khoản 3 Điều 17; Khoản 1 Điều 18 Luật An toàn thông tin mạng và trong các văn bản pháp luật có liên quan.

Khi sử dụng, khai thác các hệ thống thông tin của cơ quan, đơn vị và các phần mềm ứng dụng dùng chung của tỉnh, có trách nhiệm:

a) Tự quản lý và chịu trách nhiệm về bảo vệ thông tin cá nhân đã được khai báo trong các hệ thống thông tin; không tiết lộ tài khoản đăng nhập, đấu nối, truy cập trái phép vào các phần mềm dùng chung của tỉnh.

b) Phải thực hiện việc đổi mật khẩu ngay sau khi được cấp tài khoản truy cập vào các phần mềm dùng chung của tỉnh, cơ quan, đơn vị.

c) Khi khai thác, sử dụng các phần mềm dùng chung của tỉnh tại các điểm truy cập Internet công cộng, tuyệt đối không đặt chế độ lưu trữ mật khẩu trong quá trình sử dụng.

2. Các cơ quan, đơn vị, cá nhân khi xử lý thông tin cá nhân phải tuân thủ đầy đủ các nội dung theo quy định tại Khoản 2, 3, 4, 5 Điều 16; Khoản 1, 2 Điều 17; Khoản 3 Điều 18; Điều 19 của Luật An toàn thông tin mạng và các quy định sau:

a) Quản lý và phân quyền truy cập trong các phần mềm ứng dụng, hệ thống thông tin, cơ sở dữ liệu phù hợp với chức năng, nhiệm vụ, quyền hạn của người tham gia quản lý, vận hành, khai thác, sử dụng các phần mềm ứng dụng, hệ thống thông tin, cơ sở dữ liệu.

b) Ngay sau khi công chức viên chức đã nghỉ việc hoặc chuyển công tác, các cơ quan, đơn vị phải thực hiện việc thu hồi các thiết bị CNTT liên quan; đồng thời phải thông báo ngay bằng văn bản đến cơ quan quản lý, quản trị phần mềm ứng dụng, hệ thống thông tin, cơ sở dữ liệu để thực hiện các biện pháp kỹ thuật cập nhật lại, khóa hoặc hủy tài khoản người dùng.

**Điều 6. Quy định bảo vệ hệ thống thông tin mạng**

1. Đối với các cơ quan nhà nước.

a) Trang bị đầy đủ các kiến thức bảo mật cơ bản cho công chức viên chức trước khi cho phép truy nhập và sử dụng hệ thống thông tin;

b) Phân công công chức viên chức chuyên trách hoặc phụ trách CNTT, để quản lý kỹ thuật nghiệp vụ về an toàn thông tin tại đơn vị;

c) Thủ trưởng cơ quan, đơn vị tạo điều kiện để công chức viên chức chuyên trách hoặc phụ trách CNTT học tập, tiếp thu công nghệ, kiến thức an toàn thông tin;

d) Hàng năm, xác định các nhiệm vụ bảo đảm an toàn thông tin hệ thống (mở rộng, nâng cấp trang thiết bị; đào tạo, bồi dưỡng kiến thức CNTT, ...), để đề xuất kinh phí đến cơ quan có thẩm quyền hoặc phân bổ kinh phí duy trì hoạt động hệ thống thông tin hiệu quả;

đ) Khi xây dựng, nâng cấp, mở rộng hạ tầng kỹ thuật CNTT, các hệ thống thông tin của cơ quan, đơn vị phải có phương án đảm bảo an toàn thông tin mạng, đồng thời phải tuân thủ các điều kiện sau:

- Phòng đặt thiết bị CNTT (đối với các cơ quan, đơn vị đang quản lý, vận hành các hệ thống thông tin, cơ sở dữ liệu của tỉnh) phải đảm bảo các điều kiện đáp ứng các yêu cầu cơ bản (được bố trí ở khu vực có điều kiện an ninh tốt; khô ráo, có điều hòa không khí; nguồn cung cấp điện ổn định và có nguồn điện dự phòng; có bình chữa cháy hoặc hệ thống tự động cảnh báo, chữa cháy khẩn cấp; phòng, chống sét; có nội quy, quy trình làm việc trong khu vực an toàn bảo mật; có hệ thống kiểm soát ra vào). Phải thiết lập cơ chế bảo vệ mạng nội bộ, đảm bảo

an toàn thông tin khi có kết nối với mạng ngoài bằng các công cụ, thiết bị bảo vệ (tường lửa, hệ thống chống xâm nhập trái phép, hệ thống giám sát, cảnh báo sớm).

- Khuyến nghị cơ quan, đơn vị tổ chức có hệ thống mạng nội bộ (mạng LAN) theo hướng sử dụng máy chủ để quản lý các máy trạm trong hệ thống mạng, hạn chế sử dụng mô hình mạng ngang hàng (không có máy chủ quản lý), cài đặt hệ thống tường lửa (Firewall) để bảo vệ hệ thống mạng LAN. Các máy chủ, máy trạm, hệ thống lưu trữ nội bộ, thiết bị mạng, mạng không dây (wifi) phải được bảo vệ bởi mật khẩu an toàn. Tất cả các máy tính tại các cơ quan, đơn vị phải được cài đặt các phần mềm bảo vệ, phòng chống vi-rút.

- Các thiết bị CNTT dùng để soạn thảo, in ấn văn bản, lưu trữ thông tin bí mật nhà nước trong các cơ quan, đơn vị phải được kiểm định và bố trí riêng, tiến hành ở nơi đảm bảo bí mật, an toàn. Trên máy tính này phải thực hiện các chế độ mã hóa, phân quyền và đặt mật khẩu (password) cho người được giao sử dụng để đảm bảo an toàn, bảo mật thông tin.

- Khi thực hiện di chuyển các trang thiết bị CNTT lưu trữ dữ liệu, thông tin thuộc danh mục bí mật nhà nước phải được tổ chức quản lý, giám sát chặt chẽ theo quy định của pháp luật về bảo vệ bí mật nhà nước.

- Cập nhật kịp thời các bản vá lỗ hổng bảo mật từ nhà cung cấp, nhà sản xuất cho các hệ thống thông tin, cơ sở dữ liệu; có cơ chế sao lưu dữ liệu dự phòng, dữ liệu được lưu trữ tại nơi an toàn để sẵn sàng phục hồi cơ sở dữ liệu khi xảy ra sự cố an toàn thông tin mạng.

- Khi thuê dịch vụ CNTT ưu tiên việc đảm bảo an toàn thông tin.

- Tổ chức phân quyền truy cập cho các đối tượng người dùng tham gia vận hành, khai thác các hệ thống thông tin đúng quy trình, chặt chẽ gắn với trách nhiệm của từng tổ chức, cá nhân để đảm bảo an toàn thông tin mạng cho các hệ thống thông tin cơ quan, đơn vị đang quản lý, vận hành.

- Các cơ quan, đơn vị, cá nhân tham gia sử dụng mạng chuyên dùng thực hiện nghiêm túc các nội dung về đảm bảo an toàn thông tin mạng trên mạng truyền số liệu chuyên dùng được quy định tại Thông tư số 27/2017/TT-BTTTT ngày 20/10/2017 của Bộ Thông tin và Truyền thông quy định về việc quản lý vận hành, sử dụng và bảo đảm an toàn thông tin trên mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước;

e) Quản lý các tài khoản của hệ thống thông tin, tài khoản người dùng bao gồm: Tạo mới, sửa đổi, hủy các tài khoản. Thường xuyên kiểm tra các tài khoản của hệ thống thông tin; triển khai các công cụ để hỗ trợ việc quản lý các tài khoản của hệ thống thông tin;

g) Hệ thống thông tin giới hạn tối đa 05 (năm) lần đăng nhập liên tiếp sai tài khoản người dùng, hệ thống tự động khóa tài khoản hoặc cô lập tài khoản trong một khoảng thời gian nhất định, để được đăng nhập hệ thống thông tin lần kế tiếp;

h) Kiểm soát và theo dõi tất cả các phương pháp truy cập từ xa tới hệ thống thông tin, triển khai nhiều cơ chế giám sát, cam kết từ các truy cập từ xa; phát hiện sớm việc truy cập trái phép vào mạng máy tính hay thiết bị lưu trữ dữ liệu;

i) Thiết lập hệ thống thông tin ghi nhận và lưu vết các sự kiện: Quá trình đăng nhập hệ thống, các thao tác cấu hình hệ thống, quá trình truy xuất hệ thống,...Ghi nhận đầy đủ các thông tin trong các bản ghi nhật ký, thời gian lưu trữ các bản ghi nhật ký hệ thống tối thiểu 01 năm. Thường xuyên kiểm tra bản ghi nhật ký để kịp thời phát hiện dấu hiệu bất thường, có nguy cơ mất an toàn thông tin;

k) Cập nhật và lưu trữ cấu hình chuẩn các thành phần của hệ thống, trước khi tiến hành cài đặt, thiết lập cấu hình lại hệ thống thông tin, đảm bảo duy trì hoạt động của hệ thống thông tin; kiểm soát quá trình cài đặt trên máy chủ;

l) Cấu hình hệ thống thông tin cung cấp những chức năng cơ bản cho người dùng; thiết lập các chế độ phân quyền truy cập theo chỉ đạo của Thủ trưởng đơn vị;

m) Định kỳ hàng tuần sao lưu (backup) thông tin (không lưu đè thông tin, sao lưu dự phòng các thông tin thay đổi), dữ liệu của đơn vị và lưu trữ thông tin sao lưu ở nơi an toàn theo quy định; thường xuyên kiểm tra thông tin, dữ liệu sao lưu để đảm bảo tính sẵn sàng và toàn vẹn;

n) Sử dụng mật khẩu: Đặt cho tài khoản sử dụng ở dạng phức tạp (mật khẩu bao gồm chữ hoa, chữ thường trong bảng chữ cái, số và các ký tự đặc biệt), độ dài tối thiểu 8 ký tự. Không tiết lộ, chia sẻ mật khẩu cho người khác, khi kết thúc công việc hoặc chuyển giao máy tính cho người khác sử dụng phải thoát khỏi tài khoản người dùng.

2. Đối với các đơn vị, doanh nghiệp cung cấp các dịch vụ viễn thông, CNTT, internet cho cơ quan quản lý nhà nước trên địa bàn tỉnh:

Thực hiện các nội dung liên quan đến hoạt động bảo đảm an toàn thông tin mạng theo Điều 22 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; Thông tư số 27/2017/TT-BTTTT ngày 20/10/2017 của Bộ Thông tin và Truyền thông và các quy định sau:

a) Thực hiện các quy định của pháp luật về lưu trữ thông tin, bảo vệ thông tin cá nhân, thông tin riêng của các cơ quan, đơn vị. Áp dụng và tổ chức thực hiện các biện pháp ngăn chặn việc gửi thông tin vi phạm quy định của pháp luật khi nhận được thông báo của cơ quan, đơn vị. Cung cấp các điều kiện kỹ thuật và nghiệp vụ cần thiết để thực hiện nhiệm vụ, bảo đảm an toàn thông tin mạng theo yêu cầu của cơ quan nhà nước có thẩm quyền.

b) Phải có hệ thống lọc phần mềm độc hại trong quá trình thực hiện các dịch vụ gửi, nhận, lưu trữ thông tin trên hệ thống của mình; có biện pháp quản lý, phòng ngừa, phát hiện, ngăn chặn phát tán phần mềm độc hại xử lý theo yêu cầu

của cơ quan nhà nước có thẩm quyền; quản lý, phối hợp ngăn chặn mất an toàn thông tin mạng xuất phát từ tài nguyên internet, từ khách hàng của mình; phối hợp, kết nối định tuyến để đảm bảo hệ thống máy chủ có tên miền quốc gia Việt Nam hoạt động an toàn, ổn định.

3. Nguồn kinh phí thực hiện nhiệm vụ chuyên môn thuộc công tác bảo đảm an toàn thông tin do ngân sách nhà nước bảo đảm, theo quy định của Luật Ngân sách nhà nước và các văn bản pháp luật khác có liên quan.

4. Phòng ngừa, phát hiện, ngăn chặn và xử lý phần mềm độc hại.

a) Tất cả các máy trạm, máy chủ, các thiết bị công nghệ thông tin trong mạng và hệ thống thông tin phải được cài đặt phần mềm phòng chống vi-rút phù hợp. Các phần mềm phòng chống vi-rút phải được thiết lập chế độ tự động cập nhật; chế độ tự động quét mã độc, vi-rút khi sao chép, mở các tập tin.

b) Các công chức viên chức trong cơ quan, đơn vị phải được hướng dẫn về phòng chống phần mềm độc hại, các rủi ro do mã độc gây ra; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm trên máy trạm khi chưa có sự đồng ý của người có thẩm quyền theo quy định của cơ quan.

c) Tất cả các máy tính của cơ quan, đơn vị phải được cấu hình nhằm vô hiệu hóa tính năng tự động thực thi các tập tin trên các thiết bị lưu trữ di động.

d) Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại, vi-rút trên máy chủ, máy trạm, thiết bị công nghệ thông tin như: Máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống vi-rút, mất dữ liệu, những dấu hiệu bất thường khác,... người sử dụng nhanh chóng tắt máy tính (có thể tắt bằng cách ngắt nguồn điện) và báo trực tiếp cho cán bộ hoặc bộ phận có trách nhiệm của cơ quan, đơn vị để xử lý.

đ) Phòng ngừa hư hỏng, sự cố máy tính, hệ thống thông tin qua các sự cố bất khả kháng: Hư hỏng thiết bị đột ngột, chập điện, cháy nổ, lũ lụt, sét đánh, khủng bố, trộm cắp, ....

**Điều 7. Giám sát an toàn hệ thống thông tin mạng**

1. Đối với các cơ quan, đơn vị

Tổ chức thực hiện việc giám sát an toàn hệ thống thông tin của cơ quan, đơn vị trực tiếp quản lý. Nội dung và đối tượng giám sát thực hiện theo quy định tại các Khoản 1, 2 Điều 24 của Luật An toàn thông tin mạng; thực hiện việc lưu trữ nhật ký tình trạng hoạt động của các hệ thống thông tin tại các máy chủ trong thời gian ít nhất là 30 ngày để phục vụ các công tác đảm bảo an toàn thông tin mạng.

2. Đối với các doanh nghiệp cung cấp các dịch vụ viễn thông, CNTT, internet có trách nhiệm thực hiện theo quy định tại Khoản 3 Điều 24 của Luật An toàn thông tin mạng.

**Điều 8. Ngăn chặn xung đột thông tin trên mạng**

1. Cá nhân, tổ chức ngăn chặn thông tin phá hoại xuất phát từ hệ thống thông tin của mình; hợp tác xác định nguồn, đẩy lùi, khắc phục hậu quả tấn công mạng được thực hiện thông qua hệ thống thông tin của tổ chức, cá nhân trong nước và nước ngoài;

2. Cá nhân, tổ chức ngăn chặn hành động của tổ chức, cá nhân trong nước và nước ngoài có mục đích phá hoại tính nguyên vẹn của mạng;

3. Cá nhân, tổ chức loại trừ việc tổ chức thực hiện hoạt động trái pháp luật trên mạng có ảnh hưởng nghiêm trọng đến quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội của tổ chức, cá nhân trong nước và nước ngoài.

4. Cá nhân, tổ chức thực hiện quy định tại Điều 27 Nghị định số 142/2016/NĐ-CP ngày 14 tháng 10 năm 2016 của Chính phủ về ngăn chặn xung đột thông tin trên mạng.

5. Các cơ quan, đơn vị chức năng trên địa bàn tỉnh thực hiện quy định, trách nhiệm được Chính phủ phân công tại Nghị định số 142/2016/NĐ-CP ngày 14 tháng 10 năm 2016 của Chính phủ về ngăn chặn xung đột thông tin trên mạng.

**Điều 9. Xây dựng quy chế bảo đảm an toàn thông tin nội bộ**

Trên cơ sở Quy chế này và hướng dẫn của bộ, ngành Trung ương, các sở, ban, ngành cấp tỉnh, UBND các huyện, thị xã Long Khánh, thành phố Biên Hòa ban hành quy chế bảo đảm an toàn thông tin nội bộ tại cơ quan, địa phương quy định rõ các vấn đề cơ bản sau:

1. Phân công cụ thể công chức viên chức chuyên trách CNTT, số điện thoại liên hệ khi có sự cố về an toàn thông tin;

2. Phân công công chức viên chức chịu trách nhiệm quản lý máy tính để dự thảo các văn bản, tài liệu có tính mật; việc sử dụng và vận hành máy tính này, đảm bảo tuân thủ các quy định của pháp luật về bảo mật và an toàn thông tin;

3. Thiết lập quy tắc vào ra, quản lý phòng máy chủ; quy tắc cài đặt phần mềm lên máy chủ, máy tính trạm;

4. Quy tắc phân loại và quản lý mức độ ưu tiên đối với các tài nguyên của hệ thống thông tin (phần mềm, dữ liệu, trang thiết bị...);

5. Kiểm tra, rà soát và khắc phục sự cố an toàn của hệ thống thông tin sử dụng các biện pháp được quy định tại Điều 5 của Quy chế này;

6. Quy tắc quản lý bảo đảm an toàn hệ thống thông tin tại đơn vị; đảm bảo tính toàn vẹn, tính tin cậy, tính thống nhất và tính sẵn sàng của dữ liệu trong quản lý và vận hành trao đổi thông tin;

7. Quy trình xử lý các sự cố ảnh hưởng đến an toàn hệ thống tại đơn vị;

8. Chế độ báo cáo tổng hợp tình hình an toàn của hệ thống thông tin.

**Điều 10. Quy trình phối hợp ứng cứu sự cố mạng bảo đảm an toàn thông tin số trên địa bàn tỉnh**

1. Quy trình xử lý khẩn cấp.

Khi phát hiện hệ thống có nguy cơ mất an toàn thông tin như: Hệ thống hoạt động chậm bất thường, không truy cập được hệ thống ứng dụng, nội dung cổng (trang) thông tin điện tử hoặc giao diện ứng dụng bị thay đổi, các sự cố khác có liên quan,... thực hiện các bước cơ bản:

a) Bước 1: Ngắt kết nối hệ thống máy chủ ra khỏi hệ thống mạng, báo cáo sự cố đến Thủ trưởng cơ quan, đơn vị;

b) Bước 2: Sao chép nhật ký truy cập của người dùng (logfile) và toàn bộ dữ liệu của hệ thống ra thiết bị lưu trữ (phục vụ cho công tác phân tích);

c) Bước 3: Khắc phục hệ thống, hoặc sử dụng hệ thống dự phòng hoặc chuyển dữ liệu sao lưu dự phòng (backup) mới nhất để hệ thống hoạt động;

d) Bước 4: Tổng hợp, báo cáo sự cố và nội dung khắc phục gửi về Đội ứng cứu để tổng hợp.

2. Nguyên tắc phối hợp trong ứng cứu sự cố:

a) Đơn vị vận hành hệ thống thông tin:

- Thực hiện các bước khắc phục sự cố theo Khoản 1 Điều này.

- Các sự cố vượt quá khả năng xử lý, đơn vị thông báo đến Đội ứng cứu để hỗ trợ khắc phục và thực hiện báo cáo sự cố mạng theo mẫu quy định tại (*Phụ lục đính kèm*).

- Tổng hợp, báo cáo Đơn vị chuyên trách CNTT (Sở Thông tin và Truyền thông) theo định kỳ 06 tháng một lần và báo cáo đột xuất khi có yêu cầu.

b) Đội ứng cứu:

- Tiếp nhận thông tin, báo cáo sự cố mất an toàn thông tin của đơn vị.

- Phản hồi cho đơn vị, cá nhân gửi thông báo, báo cáo ban đầu ngay sau khi nhận được để xác nhận về việc đã nhận được thông báo, báo cáo sự cố; tối đa trong vòng 24 giờ kể từ thời điểm nhận được thông tin báo cáo sự cố của đơn vị.

- Thẩm tra, xác minh và phân loại sự cố an toàn thông tin mạng để lựa chọn phương án ứng cứu phù hợp hoặc đề xuất với Ban chỉ đạo CNTT hướng giải quyết trong trường hợp vượt thẩm quyền; tối đa 48 giờ kể từ thời điểm phát sinh sự cố và nhận được thông báo của đơn vị có sự cố.

- Chủ động hỗ trợ ngay đơn vị cần ứng cứu, xử lý sự cố trong khả năng và trách nhiệm của mình, tối đa 48 giờ phải cử cán bộ kỹ thuật của Đội có mặt tại đơn vị báo sự cố để phối hợp, hướng dẫn, ghi nhận giải quyết sự cố, trong trường hợp sự cố phức tạp, nguy cơ cao về an toàn thông tin mà không thể hướng dẫn, trao đổi qua điện thoại, email với đơn vị bị sự cố.

- Giám sát diễn biến tình hình ứng cứu sự cố và báo cáo Ban Chỉ đạo CNTT tỉnh; đề xuất, xin ý kiến chỉ đạo trong trường hợp không thuộc thẩm quyền, phạm vi trách nhiệm hoặc vượt khả năng xử lý của mình.

- Tổng hợp, báo cáo Cơ quan điều phối quốc gia theo quy định và báo cáo đột xuất khi có yêu cầu.

c) Sở Thông tin và Truyền thông báo cáo về Ủy ban nhân dân tỉnh đồng thời thông báo đến Bộ Thông tin và Truyền thông thông qua Trung tâm Ứng cứu khẩn cấp Máy tính Việt Nam, để được hỗ trợ khắc phục các sự cố vượt quá khả năng xử lý của địa phương.

**Điều 11. Mua sắm, trang bị máy tính, thiết bị công nghệ thông tin có liên quan đến an toàn thông tin mạng**

1. Trong quá trình mua sắm trang thiết bị cho hệ thống, các cơ quan, đơn vị cần tuân thủ quy định tại Thông tư số 47/2016/TT-BTTTT ngày 26/12/2016 của Bộ trưởng Bộ Thông tin và Truyền thông Quy định chi tiết về ưu tiên đầu tư mua sắm sản phẩm, dịch vụ CNTT sản xuất trong nước sử dụng nguồn vốn ngân sách nhà nước.

2. Việc đầu tư mua sắm các thiết bị, máy tính với mục đích soạn thảo, lưu trữ văn bản mật phải được kiểm định của Công an tỉnh trước khi đưa vào sử dụng.

**Điều 12. Tiếp nhận thông tin báo cáo sự cố mất an toàn thông tin mạng, sự cố mạng truyền số liệu chuyên dùng**

Địa chỉ tiếp nhận thông tin, báo cáo sự cố mất an toàn thông tin mạng; sự cố tắc, nghẽn, đứt, rớt, không truy cập được của mạng truyền số liệu chuyên dùng, cơ quan, đơn vị thông báo ngay đến địa chỉ: Phòng CNTT thuộc Sở Thông tin và Truyền thông là bộ phận làm đầu mối liên lạc ứng cứu an toàn thông tin máy tính trên địa bàn tỉnh và trong mạng lưới ứng cứu trên toàn quốc, qua các thông tin liên hệ: Điện thoại: (0251).3810269, Fax: (0251).3827071, Email: attt@dongnai.gov.vn.

## Chương III
## TRÁCH NHIỆM ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG

**Điều 13. Tổ chức, cá nhân bên ngoài khi tham gia sử dụng hệ thống thông tin của cơ quan nhà nước, để giao tiếp, cung cấp và trao đổi thông tin số với cơ quan nhà nước**

1. Nghiêm chỉnh thi hành Quy chế này và các quy định khác của pháp luật về bảo đảm an toàn thông tin mạng.

2. Khi phát hiện sự cố ảnh hưởng đến an toàn hệ thống thông tin, phải thông báo ngay với cơ quan nhà nước, nơi tổ chức, cá nhân đang thực hiện giao tiếp.

3. Các tổ chức, cá nhân tham gia vào quá trình ứng dụng CNTT trên địa bàn tỉnh, chịu sự thanh tra, kiểm tra của các cơ quan nhà nước có thẩm quyền về lĩnh vực an toàn thông tin.

**Điều 14. Công chức viên chức trong cơ quan nhà nước**

1. Nghiêm chỉnh thi hành Quy chế này và các quy định khác của pháp luật về bảo đảm an toàn thông tin.

2. Khi phát hiện sự cố ảnh hưởng đến an toàn hệ thống thông tin, phải thông báo ngay đến công chức viên chức chuyên trách CNTT của đơn vị.

3. Các thông tin, tài liệu, văn bản có tính mật theo quy định, phải dự thảo, lưu trữ đúng theo quy định về bảo mật và an toàn thông tin.

4. công chức viên chức chuyên trách CNTT:

a) Triển khai hoặc tham mưu để triển khai thực hiện các nội dung tại Khoản 1 Điều 5 và Khoản 1, 2 Điều 9 Quy chế này;

b) Theo nhiệm vụ được Thủ trưởng cơ quan, đơn vị phân công, chịu trách nhiệm tham mưu chuyên môn và vận hành đảm bảo an toàn hệ thống thông tin tại cơ quan, đơn vị;

c) Hướng dẫn, hỗ trợ người dùng tại cơ quan, đơn vị giải pháp phòng, chống vi rút máy tính. Thực hiện việc đánh giá, báo cáo các rủi ro và mức độ các rủi ro ảnh hưởng đến hoạt động hệ thống thông tin của đơn vị, các giải pháp cơ bản khắc phục các rủi ro;

d) Phối hợp với các cá nhân, tổ chức có liên quan trong việc kiểm tra, phát hiện, phòng ngừa, đấu tranh, ngăn chặn xâm phạm an toàn thông tin; tham gia khắc phục các sự cố mất an toàn thông tin.

**Điều 15. Các cơ quan nhà nước trên địa bàn tỉnh**

1. Cơ quan nhà nước có bị sự cố về an toàn thông tin, thực hiện theo nội dung quy định tại Khoản 1 Điều 42 Nghị định số 64/2007/NĐ-CP.

2. Báo cáo định kỳ vào ngày 15/10 hàng năm hoặc đột xuất theo yêu cầu về Sở Thông tin và Truyền thông để tổng hợp, báo cáo UBND tỉnh, Bộ Thông tin và Truyền thông.

3. Tuân thủ và bảo đảm an toàn thông tin trong ứng dụng CNTT, đảm bảo an toàn thông tin mạng nội bộ của cơ quan, đơn vị theo hướng dẫn của Sở Thông tin và Truyền thông theo quy định của Quy chế này và các quy định khác của pháp luật có liên quan.

4. Tuyên truyền, phổ biến quy chế này và các quy định khác của pháp luật có liên quan về an toàn thông tin trong phạm vi trách nhiệm và quyền hạn của từng cơ quan.

5. Xác định và trình cấp có thẩm quyền phê duyệt cấp độ hệ thống thông tin của cơ quan, đơn vị.

6. Khi được kiểm tra công tác đảm bảo an toàn thông tin mạng tại cơ quan, đơn vị cử cán bộ có chuyên môn về CNTT tham gia đoàn kiểm tra; phối hợp với đoàn kiểm tra xây dựng các tiêu chí và quy trình kỹ thuật kiểm tra công tác đảm bảo an toàn thông tin.

**Điều 16. Sở Thông tin và Truyền thông**

1. Tham mưu UBND tỉnh về công tác đảm bảo an toàn thông tin trên địa bàn tỉnh và chịu trách nhiệm trước Ủy ban nhân dân tỉnh trong việc đảm bảo an toàn cho các hệ thống thông tin cấp tỉnh.

2. Tham mưu UBND tỉnh thiết lập kênh thông tin trực tuyến để tiếp nhận kiến nghị, phản ánh của tổ chức, cá nhân liên quan đến bảo đảm an toàn thông tin cá nhân trên mạng. Thực hiện tổ chức thanh tra, kiểm tra đối với tổ chức, cá nhân xử lý thông tin cá nhân; tổ chức thanh tra, kiểm tra đột xuất trong trường hợp cần thiết.

3. Xây dựng và triển khai các kế hoạch, chương trình, dự án đầu tư, đào tạo về an toàn thông tin trong ứng dụng CNTT trên địa bàn tỉnh.

4. Tùy theo mức độ sự cố, phối hợp Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) và các đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố an toàn thông tin trên địa bàn tỉnh; cảnh báo các vấn đề về an toàn thông tin trong các cơ quan nhà nước trên địa bàn tỉnh.

5. Quản lý vận hành, hướng dẫn kết nối mạng truyền số liệu chuyên dùng của các cơ quan Đảng và nhà nước trên địa bàn tỉnh; xử lý các vấn đề liên quan sự cố mạng truyền số liệu chuyên dùng.

6. Hướng dẫn, hỗ trợ sao lưu dự phòng các thông tin, cơ sở dữ liệu của các cơ quan nhà nước một cách an toàn.

7. Hướng dẫn, giám sát các đơn vị xây dựng quy chế và thực hiện việc đảm bảo an toàn cho hệ thống thông tin theo quy định; hướng dẫn các cơ quan về khung báo cáo; định kỳ tổng hợp báo cáo Ủy ban nhân dân tỉnh và Bộ Thông tin và Truyền thông về công tác an toàn thông tin số trên địa bàn tỉnh.

8. Tuyên truyền và định hướng tuyên truyền, phối hợp tuyên truyền đến các phương tiện truyền thông đại chúng trên địa bàn tỉnh về công tác bảo đảm an toàn thông tin.

9. Hàng năm, tổ chức đào tạo chuyên sâu về an toàn thông tin mạng cho công chức viên chức chuyên trách CNTT đảm bảo an toàn thông tin mạng của các cơ quan, đơn vị.

10. Cung cấp, hỗ trợ các cơ quan đơn vị thiết bị CNTT soạn thảo và lưu trữ văn bản mật. Chủ trì phối hợp với Công an tỉnh thẩm định, bảo hành-bảo trì đảm bảo an toàn thông tin của thiết bị CNTT soạn thảo và lưu trữ văn bản mật của các cơ quan, đơn vị.

11. Khảo sát, triển khai, xây dựng mô hình kết nối mạng nội bộ (LAN) đảm bảo an toàn thông tin chung cho các cơ quan, đơn vị triển khai thực hiện.

12. Tham mưu xây dựng kế hoạch hàng năm, phối hợp với Công an tỉnh và các đơn vị có liên quan tổ chức kiểm tra định kỳ đảm bảo an toàn thông tin mạng, hệ thống thông tin theo cấp độ được đề xuất của các cơ quan, đơn vị.

**Điều 17. 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 và chịu trách nhiệm quản lý, kiểm soát, phòng ngừa, đấu tranh, ngăn chặn các loại tội phạm lợi dụng hệ thống thông tin gây phương hại đến an ninh mạng trong cơ quan nhà nước.

2. Chủ trì, phối hợp với Sở Thông tin và Truyền thông và các cơ quan, đơn vị có liên quan tổ chức đoàn kiểm tra về an ninh mạng để kịp thời phát hiện, xử lý các hành vi vi phạm theo quy định của pháp luật.

3. Kiểm định thiết bị CNTT soạn thảo và lưu trữ văn bản mật của các cơ quan, đơn vị; chủ trì, phối hợp với các đơn vị liên quan định kỳ kiểm tra thiết bị CNTT soạn thảo, lưu trữ văn bản mật.

4. Cử cán bộ phối hợp, tham gia đoàn kiểm tra, đánh giá công tác đảm bảo an toàn thông tin trong hoạt động ứng dụng CNTT của các cơ quan, đơn vị; điều tra và xử lý các trường hợp vi phạm các quy định về an toàn thông tin mạng theo thẩm quyền.

5. Kiểm tra đột xuất các cơ quan, đơn vị khi phát hiện có dấu hiệu vi phạm pháp luật về an toàn thông tin và an ninh mạng theo đúng quy định của pháp luật.

**Điều 18. Các doanh nghiệp cung cấp dịch vụ viễn thông, CNTT và internet cho các cơ quan quản lý nhà nước trên địa bàn tỉnh**

1. Đầu tư xây dựng, trang bị hạ tầng kỹ thuật đáp ứng đầy đủ các yêu cầu, tiêu chuẩn kỹ thuật theo quy định của Bộ Thông tin và Truyền thông về an toàn thông tin và các nội dung quy định tại Quy chế này.

2. Phối hợp với Sở Thông tin và Truyền thông để tham gia các hoạt động điều phối, ứng cứu, khắc phục sự cố thông tin đảm bảo an toàn thông tin mạng cho các cơ quan, đơn vị trong quá trình sử dụng, khai thác sử dụng dịch vụ.

3. Viễn thông Đồng Nai

a) Đảm bảo đúng trách nhiệm hợp đồng với Sở Thông tin và Truyền thông, bảo đảm mạng truyền số liệu chuyên dùng cung cấp cho các cơ quan, đơn vị được thông suốt, ổn định.

b) Chịu hoàn toàn trách nhiệm nếu có sự cố xảy ra mà thời gian xử lý vượt quá 4 giờ kể từ thời điểm nhận được thông tin sự cố.

c) Chịu hoàn toàn trách nhiệm trước UBND tỉnh về chất lượng dịch vụ nếu để số sự cố xảy ra quá 3 lần/tháng/01 đơn vị.

**Điều 19. Sở Tài chính**

Hàng năm, căn cứ khả năng cân đối ngân sách và chế độ, tiêu chuẩn, định mức do nhà nước ban hành, tham mưu UBND tỉnh bố trí kinh phí triển khai thực hiện nhiệm vụ chuyên môn về bảo đảm an toàn thông tin theo phân cấp hiện hành của Luật Ngân sách Nhà nước.

**Điều 20. Sở Kế hoạch và Đầu tư**

Chủ trì, phối hợp các đơn vị liên quan tham mưu UBND tỉnh trình Hội đồng nhân dân thông qua vốn phân bổ kế hoạch vốn trung hạn và hàng năm thực hiện các dự án về bảo đảm an toàn thông tin.

**Điều 21. Trách nhiệm thi hành**

1. Sở Thông tin và Truyền thông chủ trì, phối hợp với các sở, ban ngành, UBND các huyện, thị xã Long Khánh, thành phố Biên Hòa và các đơn vị có liên quan triển khai thực hiện Quy chế này.

2. Trong quá trình thực hiện nếu có phát sinh khó khăn, vướng mắc cần sửa đổi, bổ sung các cơ quan, đơn vị kịp thời báo cáo về Sở Thông tin và Truyền thông tổng hợp trình UBND tỉnh xem xét, quyết định./.

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

**Trần Văn Vĩnh**

| ỦY BAN NHÂN DÂN<br>TỈNH ĐỒNG NAI | CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM<br>Độc lập – Tự do – Hạnh phúc |
|---|---|

**Phụ lục**

**MẪU BÁO CÁO BAN ĐẦU/THÔNG BÁO SỰ CỐ MẠNG**

*(Ban hành kèm theo Quyết định số 48 /2018/QĐ-UBND ngày 07 tháng 11 năm 2018 của UBND tỉnh Đồng Nai)*

**THÔNG TIN VỀ TỔ CHỨC/CÁ NHÂN THÔNG BÁO SỰ CỐ**

- Tên tổ chức/cá nhân thông báo 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* | | | | |
| 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 (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 nguy cơ 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:* .....<br>.....<br>.....<br>.....<br>..... |

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

**HIỆN TRẠNG SỰ CỐ (*)**

☐ Đã được xử lý ☐ Chưa được xử lý

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

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

☐ Nhận được thông báo từ: .....

☐ Khác, đó là .....

**ĐÃ GỬI THÔNG BÁO SỰ CỐ CHO ***

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

☐ ISP đang trực tiếp cung cấp dịch vụ

☐ Cơ quan điều phối

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

- Hệ điều hành ..... Version .....
- Các dịch vụ có trên hệ thống *(Đánh dấu những dịch vụ được sử dụng trên hệ thống)*

☐ Web server ☐ Mail server ☐ Database server

☐ Dịch vụ khác, đó là .....

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

☐ Antivirus ☐ Firewall ☐ Hệ thống phát hiện xâm nhập

☐ Khác: .....

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

.....

- Các tên miền của hệ thống

.....

- Mục đích chính sử dụng hệ thống .....

.....

- Thông tin gửi kèm

☐ Nhật ký hệ thống ☐ Mẫu virus / mã độc ☐ Khác:.....

- Các thông tin cung cấp trong thông báo sự cố này đều phải được giữ bí mật: ☐ Có ☐ Không
- Sự cố đã được khắc phục: ☐ Đã khắc phục ☐ Chưa khắc phục (đề nghị ứng cứu)
- Kiến nghị .....

**THỜI GIAN THỰC HIỆN BÁO CÁO SỰ CỐ *:** .../... /...../.../...
(ngày/tháng/năm/giờ/phút)

**Cá nhân / Tổ chức báo cáo**
*(Ký tên, đóng dấu)*

*Chú thích:*

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

*2. Sử dụng tiêu đề (subject) bắt đầu bằng "[TBSC]" khi gửi thông báo qua email*

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


**Trần Văn Vĩnh**