

Số: /BTTTT-CATTT

Hà Nội, ngày tháng năm 2024

V/v Hướng dẫn rà soát, đánh giá tình hình
bảo đảm an toàn thông tin mạng đối với các
hệ thống thông tin thuộc phạm vi quản lý

Kính gửi:

- Các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương.

Ngày 07 tháng 4 năm 2024, Thủ tướng Chính phủ ban hành Công điện số 33/CĐ-TTg về tăng cường bảo đảm an toàn thông tin mạng, trong đó giao Bộ Thông tin và Truyền thông hướng dẫn bộ, ngành, địa phương rà soát, đánh giá tình hình bảo đảm an toàn thông tin mạng cho hệ thống thông tin của cơ quan, tổ chức, doanh nghiệp nhà nước trước ngày 11 tháng 4 năm 2024; tổng hợp kết quả, báo cáo Thủ tướng Chính phủ trước ngày 30 tháng 4 năm 2024.

Thực hiện chỉ đạo của Thủ tướng Chính phủ, Bộ Thông tin và Truyền thông trân trọng đề nghị các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ và Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương chỉ đạo và tổ chức rà soát, đánh giá tình hình bảo đảm an toàn thông tin mạng cho hệ thống thông tin của cơ quan, tổ chức, doanh nghiệp nhà nước thuộc phạm vi quản lý như sau:

1. Mục đích

- Rà soát, đánh giá tình hình bảo đảm an toàn thông tin các hệ thống thông tin thuộc phạm vi quản lý để kịp thời khắc phục các tồn tại, lỗ hổng, điểm yếu nhằm phòng ngừa các sự cố tấn công mạng;

- Bảo đảm triển khai đầy đủ quy định pháp luật về bảo đảm an toàn thông tin mạng, trọng tâm là bảo đảm an toàn hệ thống thông tin theo cấp độ;

- Tăng cường kỷ luật, kỷ cương và thực hiện nghiêm, bảo đảm tiến độ các nhiệm vụ trong các văn bản chỉ đạo của Thủ tướng Chính phủ trong công tác bảo đảm an toàn thông tin mạng.

2. Nội dung rà soát, đánh giá công tác phê duyệt hồ sơ đề xuất cấp độ và phương án bảo đảm an toàn thông tin theo cấp độ tương ứng

a) Rà soát, đánh giá công tác phê duyệt hồ sơ đề xuất cấp độ và triển khai phương án bảo đảm an toàn thông tin theo cấp độ tương ứng

- Thống kê, rà soát các hệ thống thông tin thuộc phạm vi quản lý và đánh giá thực trạng phê duyệt hồ sơ đề xuất cấp độ và phương án bảo đảm an toàn thông tin theo cấp độ tương ứng;

- Xây dựng Kế hoạch hoàn thiện và có lộ trình cụ thể đối với các hệ thống thông tin chưa thực hiện phê duyệt hồ sơ đề xuất cấp độ và triển khai đầy đủ phương án bảo đảm an toàn thông tin theo cấp độ được phê duyệt. Bảo đảm đúng thời hạn theo chỉ đạo của Thủ tướng Chính phủ tại Chỉ thị số 09/CT-TTg ngày 23 tháng 2 năm 2024 về tuân thủ quy định pháp luật và tăng cường bảo đảm an toàn hệ thống thông tin theo cấp độ;

- Sử dụng Nền tảng hỗ trợ quản lý bảo đảm an toàn hệ thống thông tin theo cấp độ (gọi tắt là Nền tảng quản lý cấp độ) do Bộ Thông tin và Truyền thông cung cấp để xây dựng, quản lý các hệ thống thông tin thuộc phạm vi quản lý tại đường dẫn: <https://capdo.ais.gov.vn> (thông tin trên nền tảng là cơ sở để Bộ Thông tin và Truyền thông tham khảo, đánh giá).

b) Rà soát, đánh giá tình hình thực hiện kiểm tra, đánh giá an toàn thông tin và quản lý rủi ro an toàn thông tin trong phạm vi quản lý

- Thống kê, rà soát việc tổ chức thực hiện kiểm tra, đánh giá an toàn thông tin và quản lý rủi ro an toàn thông tin đối với các hệ thống thông tin thuộc phạm vi quản lý theo quy định tại khoản 2, Điều 20 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 và Điều 12 Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ Thông tin và Truyền thông;

- Xây dựng kế hoạch, bố trí nguồn lực để tổ chức kiểm tra, đánh giá an toàn thông tin và quản lý rủi ro an toàn thông tin đối với các hệ thống thông tin chưa thực hiện kiểm tra, đánh giá định kỳ (tối thiểu 01 lần/02 năm đối với hệ thống cấp độ 1, cấp độ 2; 01 lần/năm đối với hệ thống thông tin cấp độ 3, cấp độ 4; 01 lần/06 tháng đối với hệ thống thông tin cấp độ 5). Kịp thời khắc phục các tồn tại, lỗ hổng, điểm yếu nhằm phòng ngừa các sự cố tấn công mạng, đặc biệt là các hệ thống cung cấp dịch vụ trực tuyến cho người dân và doanh nghiệp.

c) Rà soát, đánh giá công tác xây dựng kế hoạch ứng phó sự cố an toàn thông tin mạng, tổ chức diễn tập an toàn thông tin mạng

- Thống kê, đánh giá về công tác xây dựng kế hoạch ứng phó sự cố đối với các hệ thống thông tin thuộc phạm vi quản lý. Kịp thời cập nhật phương án xử lý sự cố tương ứng với loại sự cố/hình thức tấn công mạng, đặc biệt là các phương án ứng phó sự cố đối với nguy cơ tấn công mã độc/mã hóa tống tiền (ransomware), tấn công chiếm quyền điều khiển, thay đổi giao diện,...;

- Đánh giá tình hình thực hiện và tổ chức diễn tập thực chiến an toàn thông tin đối với các hệ thống thông tin thuộc phạm vi quản lý theo chỉ đạo tại Chỉ thị số 18/CT-TTg ngày 13 tháng 8 năm 2022 về đẩy mạnh triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng Việt Nam;

- Xây dựng, cập nhật kế hoạch để đảm bảo triển khai tổ chức diễn tập, ứng phó các sự cố có thể xảy ra đối với các hệ thống thông tin thuộc phạm vi quản lý, đặc biệt là các hệ thống thông tin quan trọng, hệ thống thông tin cung cấp dịch vụ

trực tuyến cho người dân và doanh nghiệp.

c) Đánh giá về tình hình bố trí hạng mục về an toàn thông tin khi xây dựng, triển khai kế hoạch ứng dụng công nghệ thông tin hàng năm, giai đoạn 5 năm và các dự án công nghệ thông tin.

3. Về thời hạn báo cáo kết quả rà soát

Báo cáo kết quả rà soát, đánh giá tình hình bảo đảm an toàn thông tin mạng đối với các hệ thống thông tin thuộc phạm vi quản lý gửi về Bộ Thông tin và Truyền thông (qua Cục An toàn thông tin), như sau:

a) Báo cáo lần đầu:

Trước ngày 22 tháng 4 năm 2024 để tổng hợp, báo cáo Thủ tướng Chính phủ trước ngày 30 tháng 4 năm 2024 theo chỉ đạo tại Công điện số 33/CĐ-TTg ngày 07 tháng 4 năm 2024.

b) Báo cáo các lần tiếp theo (hàng Quý):

Trước ngày 20 của tháng cuối Quý (tháng 3, tháng 6, tháng 9, tháng 12 năm báo cáo).

(Chi tiết tại Phụ lục I và Phụ lục II gửi kèm theo).

Trong quá trình triển khai thực hiện nếu có khó khăn, vướng mắc, đề nghị Quý Cơ quan phản ánh về Bộ Thông tin và Truyền thông (Cục An toàn thông tin) để được hướng dẫn giải quyết.

Đầu mối liên hệ: Ông Phùng Quang Minh, Cục An toàn thông tin, Bộ Thông tin và Truyền thông; số điện thoại: 0369596886; thư điện tử: pqminh@mic.gov.vn.

Trân trọng./.

Nơi nhận:

- Như trên;
- Thủ tướng Chính phủ (để b/c);
- Phó Thủ tướng Trần Lưu Quang (để b/c);
- Bộ trưởng (để b/c);
- Thứ trưởng Phạm Đức Long;
- Đơn vị chuyên trách về CNTT/ATTT của: Văn phòng Trung ương Đảng, Văn phòng Quốc hội, Văn phòng Chủ tịch nước, Tòa án nhân dân tối cao, Viện Kiểm sát nhân dân tối cao;
- Đơn vị chuyên trách về CNTT/ATTT của các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Sở TT&TT các tỉnh, TP trực thuộc TW;
- Lưu: VT, CATTT. PQM.

**KT. BỘ TRƯỞNG
THỨ TRƯỞNG**

Phạm Đức Long

PHỤ LỤC I
BÁO CÁO TÌNH HÌNH BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG ĐỐI
VỚI CÁC HỆ THỐNG THÔNG TIN THUỘC PHẠM VI QUẢN LÝ
(Kèm theo Công văn số /BTTTT-CATTT ngày tháng năm 2024
của Bộ Thông tin và Truyền thông)

I. VỀ TRIỂN KHAI BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN (HTTT) THEO CẤP ĐỘ

1. Thống kê HTTT thuộc phạm vi quản lý

a) Danh mục hệ thống thông tin

TT	Tên hệ thống thông tin	Cấp độ đề xuất (1-5)	Đơn vị vận hành	Thực trạng phê duyệt (*)	Ghi chú
1	Hệ thống thông tin 1
2	Hệ thống thông tin 2
...
n	Hệ thống thông tin n

(*) Đã phê duyệt hoặc chưa phê duyệt

b) Số HTTT thuộc phạm vi quản lý:.....

c) Số lượng HTTT đã được phê duyệt hồ sơ đề xuất cấp độ/tương ứng với tỉ lệ trên tổng số HTTT:.....hệ thống/đạt tỉ lệ.....%.

Trong đó:

+ Số HTTT đã được phê duyệt cấp độ 1/tương ứng với tỉ lệ phần trăm trên tổng số HTTT được phê duyệt:hệ thống/tương ứng tỉ lệ.....%.

+ Số HTTT đã được phê duyệt cấp độ 2/tương ứng với tỉ lệ phần trăm trên tổng số HTTT được phê duyệt:hệ thống/tương ứng tỉ lệ.....%.

+ Số HTTT đã được phê duyệt cấp độ 3/tương ứng với tỉ lệ phần trăm trên tổng số HTTT được phê duyệt:hệ thống/tương ứng tỉ lệ.....%.

+ Số HTTT đã được phê duyệt cấp độ 4/tương ứng với tỉ lệ phần trăm trên tổng số HTTT được phê duyệt:hệ thống/tương ứng tỉ lệ.....%.

+ Số HTTT đã được phê duyệt cấp độ 5/tương ứng với tỉ lệ phần trăm trên tổng số HTTT được phê duyệt:hệ thống/tương ứng tỉ lệ.....%.

2. Tỉ lệ HTTT triển khai đầy đủ phương án bảo vệ theo Hồ sơ đề xuất cấp độ đã được phê duyệt

Số lượng HTTT đã triển khai đầy đủ phương án bảo vệ theo Hồ sơ đề xuất cấp độ đã được phê duyệt/tương ứng với tỉ lệ phần trăm trên tổng số HTTT được phê duyệt: hệ thống/tương ứng tỉ lệ.....%.

3. Kế hoạch hoàn thành phê duyệt và triển khai đầy đủ phương án bảo vệ theo Hồ sơ đề xuất cấp độ đã được phê duyệt năm 20...

(Đối với các Hệ thống thông tin chưa phê duyệt HSDXCD và triển khai đầy đủ phương án bảo đảm an toàn hệ thống thông tin theo cấp độ được phê duyệt)

TT	Tên hệ thống thông tin	Cấp độ đề xuất (1-5)	Thời hạn hoàn phê duyệt (Tháng/Năm)	Thời hạn triển khai đầy đủ (Tháng/năm)	Ghi chú
1	Hệ thống thông tin 1
2	Hệ thống thông tin 2
...
n	Hệ thống thông tin n

Lưu ý:

Việc đánh giá thực trạng phê duyệt và triển khai đầy đủ phương án bảo đảm an toàn thông tin mạng đối với các hệ thống thông tin, Bộ Thông tin và Truyền thông (Cục An toàn thông tin) sẽ đánh giá, đối chiếu với thực trạng quản lý thông tin trên Nền tảng quản lý cấp độ theo chỉ đạo của Thủ tướng Chính phủ tại Chỉ thị số 09/CT-TTg.

II. VỀ KIỂM TRA, ĐÁNH GIÁ ĐỊNH KÌ HỆ THỐNG THÔNG TIN

1. Kết quả năm 2023 (hoặc trước năm kỳ báo cáo)

a) Số lượng HTTT được kiểm tra, đánh giá đầy đủ các nội dung theo quy định tại Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022

- Số lượng HTTT của Bộ/địa phương đã được kiểm tra, đánh giá/tương ứng với tỉ lệ phần trăm trên tổng số HTTT:.....hệ thống/ tương ứng tỉ lệ.....%.

Trong đó:

+ Số HTTT được đánh giá lỗ hổng, bảo mật:.....hệ thống.

+ Số HTTT được đánh giá mã nguồn ứng dụng:.....hệ thống.

b) Danh sách hệ thống thông tin được kiểm tra, đánh giá đến hiện tại:

TT	Tên hệ thống thông tin	Cấp độ đề xuất (1-5)	Thời gian tổ chức kiểm tra, đánh giá (Tháng/Năm)	Hình thức thực hiện (Thuê ngoài/Tự thực hiện)	Ghi chú
1	Hệ thống thông tin 1
2	Hệ thống thông tin 2
...

TT	Tên hệ thống thông tin	Cấp độ đề xuất (1-5)	Thời gian tổ chức kiểm tra, đánh giá (Tháng/Năm)	Hình thức thực hiện (Thuê ngoài/Tự thực hiện)	Ghi chú
<i>n</i>	<i>Hệ thống thông tin n</i>

2. Kế hoạch kiểm tra, đánh giá năm 2024 (hoặc năm kỳ báo cáo)

TT	Tên hệ thống thông tin	Cấp độ đề xuất (1-5)	Thời gian tổ chức kiểm tra, đánh giá (Tháng/Năm)	Hình thức thực hiện (Thuê ngoài/Tự thực hiện)	Ghi chú
<i>1</i>	<i>Hệ thống thông tin 1</i>
<i>2</i>	<i>Hệ thống thông tin 2</i>
...
<i>n</i>	<i>Hệ thống thông tin n</i>

III. VỀ TỔ CHỨC DIỄN TẬP THỰC CHIẾN

1. Kết quả năm 2023 (hoặc trước năm kỳ báo cáo)

a) Tổ chức diễn tập thực chiến an toàn thông tin mạng

- Số lượng cuộc diễn tập theo hình thức thông thường được tổ chức:
- Số lượng cuộc diễn tập thực chiến được tổ chức:
- Số lượng HTTT được lựa chọn để tổ chức diễn tập thực chiến:
- Chi tiết kết quả hoạt động diễn tập thực chiến an toàn thông tin mạng:

STT	Tên cuộc Diễn tập thực chiến	Ngày tổ chức	Đơn vị tổ chức	Phạm vi, quy mô	Số lượng sự cố đã phát hiện	Số lượng sự cố đã được xử lý
<i>1</i>	...	<i>.../.../20...</i>	<i>(Phối hợp hoặc tự tổ chức)</i>	<i>(Tên Hệ thống thông tin thuộc phạm vi quản lý được lựa chọn để tổ chức, cấp độ an toàn của hệ thống)</i>
<i>2</i>	...	<i>.../.../20...</i>

STT	Tên cuộc Diễn tập thực chiến	Ngày tổ chức	Đơn vị tổ chức	Phạm vi, quy mô	Số lượng sự cố đã phát hiện	Số lượng sự cố đã được xử lý
.../.../20...

b) Phát hiện và xử lý sự cố an toàn thông tin mạng

- Số lượng sự cố đã phát hiện tại các HTTT thuộc phạm vi quản lý:

Ghi chú: Số lượng sự cố, đánh giá năng lực phát hiện sự cố gồm cả sự cố tự phát hiện và sự cố từ các cảnh báo của các đơn vị chuyên trách.

- Số lượng sự cố đã được xử lý tại các Bộ/địa phương/tương ứng với tỉ lệ trên số lượng sự cố được phát hiện:

Chi tiết kết quả phát hiện, xử lý sự cố an toàn thông tin mạng:

2. Kế hoạch năm 2024 (hoặc năm kỳ báo cáo)

a) Số lượng và thời gian diễn tập:

b) Danh sách các thông dự kiến sẽ triển khai diễn tập thực chiến

TT	Tên hệ thống thông tin	Cấp độ đề xuất (1-5)	Thời gian tổ chức diễn tập thực chiến	Ghi chú
1	Hệ thống thông tin 1
2	Hệ thống thông tin 2
...
N	Hệ thống thông tin n

IV. VỀ KINH PHÍ ĐẦU TƯ HẠNG MỤC AN TOÀN THÔNG TIN (năm 2023, 2024,...)

1. Kết quả năm 2023 (trước năm kỳ báo cáo)

- Kinh phí đầu tư từ NSNN chi cho an toàn thông tin:

- Kinh phí thường xuyên từ NSNN chi cho an toàn thông tin:

- Tỉ lệ kinh phí bảo đảm an toàn thông tin so với kinh phí chi cho khoa học công nghệ, chuyển đổi số, ứng dụng công nghệ thông tin:

Trong đó gồm:

- Kinh phí giám sát an toàn thông tin:

- Kinh phí kiểm tra, đánh giá an toàn thông tin:

- Kinh phí diễn tập, ứng cứu sự cố an toàn thông tin:

- Kinh phí đào tạo, tập huấn và tuyên truyền, nâng cao nhận thức về an toàn thông tin:

- Kinh phí chi dành cho an toàn thông tin của cơ quan Bộ/Tỉnh sử dụng các giải pháp an toàn thông tin nội địa:

- Kinh phí khác (nếu có):

Chi tiết:

STT	Năm	Kinh phí đầu tư từ ngân sách nhà nước chỉ cho an toàn thông tin	Kinh phí thường xuyên từ ngân sách nhà nước chỉ cho an toàn thông tin	Kinh phí chi thuê dịch vụ các hạng mục về an toàn thông tin	Kinh phí đầu tư hạ tầng các hạng mục về an toàn thông tin	Tỷ lệ kinh phí chi cho các sản phẩm, dịch vụ an toàn thông tin mạng trong tổng kinh phí triển khai kế hoạch ứng dụng công nghệ thông tin (%)
1	2022
2	2023
3	2024
..

2. Kế hoạch năm 2024 (hoặc năm báo cáo)

- Kinh phí đầu tư từ NSNN chỉ cho an toàn thông tin:

- Kinh phí thường xuyên từ NSNN chỉ cho an toàn thông tin:

- Tỷ lệ kinh phí bảo đảm an toàn thông tin so với kinh phí chi cho chuyển đổi số, ứng dụng công nghệ thông tin:

Trong đó gồm:

- Kinh phí giám sát an toàn thông tin:

- Kinh phí kiểm tra, đánh giá an toàn thông tin:

- Kinh phí diễn tập, ứng cứu sự cố an toàn thông tin:

- Kinh phí đào tạo, tập huấn và tuyên truyền, nâng cao nhận thức về an toàn thông tin:

- Kinh phí chi dành cho an toàn thông tin của cơ quan Bộ/Tỉnh sử dụng các giải pháp an toàn thông tin nội địa:

- Kinh phí khác (nếu có):

PHỤ LỤC II
RÀ SOÁT, ĐÁNH GIÁ TÌNH HÌNH BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG ĐỐI VỚI CÁC HỆ THỐNG THÔNG TIN THUỘC PHẠM VI QUẢN LÝ

(Kèm theo Công văn số /BTTTT-CATT ngày tháng năm 2024
của Bộ Thông tin và Truyền thông)

1. Đối với Hệ thống thông tin cấp độ 1, 2

STT	Tên hệ thống thông tin	Cấp độ đề xuất	Tình trạng phê duyệt	Cung cấp dịch vụ trực tuyến	Các phương án kỹ thuật tương ứng với cấp độ đề xuất					
					Quản lý truy cập từ xa	Quản lý các vùng mạng	Phòng chống mã độc	Phòng chống tấn công web	An toàn thư điện tử	Dự phòng thiết bị chính
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
Chú thích (- Từ tiêu chí số 1 đến tiêu chí số 3 đối với Hệ thống thông tin cấp độ 1; - Từ tiêu chí số 1 đến tiêu chí số 6 đối với Hệ thống thông tin cấp độ 2; - Đánh dấu "x" trong trường hợp Hệ thống đã đáp ứng tiêu chí.)										
1	Hệ thống thông tin 1
2	Hệ thống thông tin 2
...
n	Hệ thống thông tin n									

Ghi chú:

- (1) Số thứ tự
- (2) Tên Hệ thống thông tin thuộc phạm vi quản lý
- (3) Cấp độ đề xuất tương ứng (Ví dụ: cấp độ 1)
- (4) Tình trạng phê duyệt hồ sơ đề xuất cấp độ của Hệ thống (Ví dụ: Đã phê duyệt)

(5) Đánh dấu “x” trong trường hợp là Hệ thống cung cấp dịch vụ trực tuyến phục vụ người dân, doanh nghiệp

(6) Các phương án kỹ thuật tương ứng với cấp độ đề xuất theo quy định tại Thông tư số 12/2022/TT-BTTTT, cụ thể:

- Tiêu chí 1: Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn
- Tiêu chí 2: Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập
- Tiêu chí 3: Có phương án phòng chống mã độc cho máy chủ và máy trạm
- Tiêu chí 4: Có phương án phòng chống tấn công mạng cho ứng dụng web
- Tiêu chí 5: Có phương án bảo đảm an toàn thông tin cho hệ thống thư điện tử (nếu có)
- Tiêu chí 6: Có phương án dự phòng cho các thiết bị mạng chính, bao gồm thiết bị chuyển mạch trung tâm hoặc tương đương, thiết bị tường lửa trung tâm

2. Đối với Hệ thống thông tin cấp độ 3, 4, 5

2.1. Hệ thống thông tin 1

2.1.1. Tên hệ thống thông tin:

2.1.2. Hiện trạng phê duyệt Hồ sơ đề xuất cấp độ:

- Đã phê duyệt : Quyết định số: Ngày phê duyệt: .../.../20....
- Chưa phê duyệt :

2.1.3. Kết quả rà soát các tiêu chí theo cấp độ đề xuất

STT	Yêu cầu	Giải pháp/thiết bị/phương án đang triển khai	Ghi chú
Tiêu chí theo Công văn số 708/BTTTT-CATT			
(- Từ tiêu chí số 1 đến tiêu chí số 16 đối với Hệ thống thông tin cấp độ 3; - Từ tiêu chí số 1 đến tiêu chí số 17 đối với Hệ thống thông tin cấp độ 4; - Từ tiêu chí số 1 đến tiêu chí số 19 đối với Hệ thống thông tin cấp độ 5)			

STT	Yêu cầu	Giải pháp/thiết bị/phương án đang triển khai	Ghi chú
1	Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn		
2	Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập		
3	Có phương án phòng chống tấn công mạng cho ứng dụng web		
4	Có phương án cân bằng tải, dự phòng nóng cho các thiết bị mạng chính (Đối với HTTT cấp độ 5 yêu cầu có dự phòng nóng cho các thiết bị mạng)		
5	Có phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu		
6	Có phương án chặn lọc phần mềm độc hại trên môi trường mạng		
7	Có phương án phòng chống tấn công từ chối dịch vụ		
8	Có phương án bảo đảm an toàn thông tin cho hệ thống thư điện tử (nếu có)		
9	Có phương án quản lý truy cập lớp mạng		
10	Có phương án giám sát hệ thống thông tin tập trung		
11	Có phương án giám sát an toàn hệ thống thông tin tập trung		
12	Có phương án quản lý sao lưu dự phòng tập trung		
13	Có phương án quản lý phần mềm phòng chống mã độc trên máy chủ/máy tính người dùng		
14	Có phương án phòng, chống thất thoát dữ liệu		
15	Có phương án dự phòng kết nối mạng Internet cho các máy chủ dịch vụ		
16	Có phương án bảo đảm an toàn cho mạng không dây (nếu có)		

STT	Yêu cầu	Giải pháp/thiết bị/phương án đang triển khai	Ghi chú
17	Có phương án quản lý tài khoản đặc quyền, sử dụng Sản phẩm Quản lý tài khoản đặc quyền (HTTT cấp độ 4, 5)		
18	Có phương án dự phòng hệ thống ở vị trí địa lý khác nhau, cách nhau tối thiểu 30 km (HTTT cấp độ 5)		
19	Có phương án dự phòng cho kết nối mạng giữa các hệ thống chính và dự phòng (HTTT tin cấp độ 5)		

2.2 Hệ thống thông tin 2

2.2.1. Tên hệ thống thông tin:

2.2.2. Hiện trạng phê duyệt Hồ sơ đề xuất cấp độ:

- Đã phê duyệt : Quyết định số: Ngày phê duyệt:.../.../20....

- Chưa phê duyệt :

2.2.3. Kết quả rà soát các tiêu chí theo cấp độ đề xuất
(*Tương tự mục 2.1.3 ở trên*)

.....

n. Hệ thống thông tin n

(*Nội dung báo cáo tương tự hệ thống thông tin 1*).