

UBND TỈNH CÀ MAU
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 815/STTTT-CNTTBCVT

Cà Mau, ngày 26 tháng 4 năm 2024

V/v rà soát đánh giá tình hình bảo đảm an
toàn thông tin mạng và an toàn hệ thống
thông tin theo cấp độ trên địa bàn tỉnh

Kính gửi: Ủy ban nhân dân tỉnh Cà Mau

Thực hiện ý kiến chỉ đạo của Chủ tịch Ủy ban nhân dân tỉnh tại Công văn số 2919/UBND-KGVX ngày 17/4/2024 về việc tăng cường bảo đảm an toàn thông tin mạng và an toàn hệ thống thông tin theo cấp độ; Công văn số 1337/BTTTT-CATTT ngày 12/4/2024 của Bộ Thông tin và Truyền thông về việc 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.

Sau khi phối hợp với các đơn vị liên quan, tiến hành rà soát kết quả thực hiện việc bảo đảm an toàn thông tin mạng theo hướng dẫn của Bộ Thông tin và Truyền thông tại Công văn số 1337/BTTTT-CATTT ngày 12/4/2024; đồng thời tổng rà soát đánh giá tình hình bảo đảm an toàn thông tin đối với các hệ thống thông tin trên địa bàn tỉnh. Sở Thông tin và Truyền thông tổng hợp hoàn thiện các Phụ lục kèm Công văn số 1337/BTTTT-CATTT ngày 12/4/2024 của Bộ Thông tin và Truyền thông (kèm theo các Phụ lục I, II).

Sở Thông tin và Truyền thông kính trình Ủy ban nhân dân tỉnh xem xét, báo cáo Bộ Thông tin và Truyền thông./.

Nơi nhận:

- Như trên;
- Lưu: VP.

GIÁM ĐỐC



Trần Quốc Chính

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 815/STTTT-CNTTBCVT ngày 26 tháng 4 năm 2024
của Sở 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

Qua rà soát (đến cuối năm 2023) trên địa bàn tỉnh có 10 hệ thống thông tin cụ thể như sau:

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	Cổng thông tin điện tử tỉnh Cà Mau	3	Cổng thông tin điện tử, Văn phòng UBND tỉnh	Đã phê duyệt	
2	Công báo Điện tử tỉnh Cà Mau	3	Cổng thông tin điện tử, Văn phòng UBND tỉnh	Đã phê duyệt	
3	Hệ thống thông tin giải quyết thủ tục hành chính tỉnh Cà Mau	3	Trung tâm giải quyết TTHC, Văn phòng UBND tỉnh	Đã phê duyệt	
4	Phần mềm Quản lý Cán bộ Công chức Viên chức tỉnh Cà Mau	3	Sở Nội vụ	Đã phê duyệt	
5	Phần mềm Quản lý Văn bản và điều hành	3	Sở Thông tin và Truyền thông	Đã phê duyệt	
6	Hệ thống thư điện tử tỉnh Cà Mau	3	Sở Thông tin và Truyền thông	Đã phê duyệt	
7	Cổng thông tin điện tử Sở Giáo dục và Đào tạo	3	Sở Giáo dục và Đào tạo	Đã phê duyệt	
8	Hệ thống Cơ sở dữ liệu hợp đồng, giao dịch đã được công chứng, chứng thực trên địa bàn tỉnh Cà Mau	2	Sở Tư pháp	Đã phê duyệt	

TT	Tên hệ thống thông tin	Cấp độ đề xuất (1-5)	Đơn vị vận hành	Thực trạng phê duyệt (*)	Ghi chú
9	<i>Cổng thông tin điện tử Đảng bộ tỉnh Cà Mau</i>	2	Văn phòng Tỉnh ủy	Đã phê duyệt	
10	<i>Phần mềm Quản lý lao động trên địa bàn tỉnh Cà Mau</i>	2	Sở Lao động Thương binh và Xã hội	Đã phê duyệt	

(*) Đã phê duyệt hoặc chưa phê duyệt

b) Số HTTT thuộc phạm vi quản lý: 10

c) Số lượng HTTT đã được phê duyệt hồ sơ đề xuất cấp độ/tương ứng với tỉ lệ trên tổng số HTTT: 10 hệ thống/đạt tỉ lệ: 100 %.

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: 0 hệ thống/tương ứng tỉ lệ 0 %.

+ Số HTTT đã được phê duyệt cấp độ 2/tương ứng với tỉ lệ phần trăm trên tổng số HTTT được phê duyệt: 03 hệ thống/tương ứng tỉ lệ 30 %.

+ Số HTTT đã được phê duyệt cấp độ 3/tương ứng với tỉ lệ phần trăm trên tổng số HTTT được phê duyệt: 07 hệ thống/tương ứng tỉ lệ 70 %.

+ 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: 10/10 hệ thống/tương ứng tỉ lệ 100 %.

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 2024

(Đối với các Hệ thống thông tin chưa phê duyệt HSĐXCD 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	Phần mềm Phản ánh Hiện trường	2	30/5/2024	15/11/2024	
2	Hệ thống truy xuất nguồn gốc sản phẩm (Blockchain)	2	30/5/2024	15/11/2024	
3	Trục liên thông nội tỉnh (LGSP), SSO	3	30/5/2024	15/11/2024	
4	Hệ thống thông tin nguồn	2	30/5/2024	15/11/2024	
5	Phần mềm quản lý cơ sở dữ liệu ngành Công thương	2	30/5/2024	15/11/2024	

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: 10 hệ thống/ tương ứng tỉ lệ 100 %.

Trong đó:

+ Số HTTT được đánh giá lỗ hổng, bảo mật: 01 hệ thống.

+ Số HTTT được đánh giá mã nguồn ứng dụng: 09 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	Trục LGSP, Trục Liên thông văn bản quốc gia	3	16/10/2023	Thuê ngoài	
3	Website ứng dụng Dịch vụ công trực tuyến	3	16/10/2023	Thuê ngoài	

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
4	Cổng Thông tin điện tử tỉnh	3	16/10/2023	Thuê ngoài	
5	Hệ thống Mail tỉnh và Hệ thống SSO	3	16/10/2023	Thuê ngoài	

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
1	Cổng thông tin điện tử tỉnh Cà Mau	3	10/2024	Thuê ngoài	
2	Công báo điện tử tỉnh Cà Mau	3	10/2024	Tự thực hiện	
3	Hệ thống thông tin giải quyết thủ tục hành chính tỉnh Cà Mau		10/2024	Thuê ngoài	
4	Phần mềm Quản lý CBCCVC tỉnh	3	10/2024	Tự thực hiện	
5	Phần mềm Quản lý Văn bản và điều hành	3	10/2024	Tự thực hiện	
6	Hệ thống thư điện tử tỉnh Cà Mau và Hệ thống SSO	3	10/2024	Thuê ngoài	
7	Cổng thông tin điện tử Sở Giáo dục và Đào tạo	3	10/2024	Tự thực hiện	
8	Hệ thống cơ sở dữ liệu hợp đồng, giao dịch đã được công chứng, chứng thực trên địa bàn tỉnh Cà Mau	2	10/2024	Tự thực hiện	
9	Cổng thông tin điện tử Đảng bộ tỉnh Cà Mau	2	10/2024	Thuê ngoài	
10	Phần mềm Quản lý lao động trên địa bàn tỉnh Cà Mau	2	10/2024	Tự thực hiện	
11	Phần mềm Phản ánh Hiện trường	2	10/2024	Tự thực hiện	
12	Hệ thống truy xuất nguồn gốc sản phẩm (Blockchain)	2	10/2024	Tự thực hiện	

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
13	Trục liên thông nội tỉnh (LGSP), Trục Liên thông văn bản quốc gia	3	10/2024	Thuê ngoài	
14	Hệ thống thông tin nguồn	2	10/2024	Tự thực hiện	
15	Phần mềm quản lý cơ sở dữ liệu ngành Công thương	2	10/2024	Tự thực hiện	

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: 01 cuộc
- Số lượng cuộc diễn tập thực chiến được tổ chức: 01 cuộc
- Số lượng HTTT được lựa chọn để tổ chức diễn tập thực chiến: 01 hệ thống (Cấp độ 3)

- 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
1	Diễn tập thực chiến Ứng cứu sự cố an toàn thông tin mạng	21-22/12/2023	Sở Thông tin và Truyền thông	Trong tỉnh Cà Mau	8	8

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: 10 sự cố

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: 10/10 sự cố

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

- Tấn công sử dụng mã độc: 01 sự cố.

- Lộ lọt thông tin tài khoản, mật khẩu: 07 sự cố.
- Lỗ hổng bảo mật (CVE) CVE-2021-27748 Trang thông tin điện tử tỉnh: 01 sự cố.
- Lỗ hổng an toàn thông tin Zero-day trong hệ thống mail Zimbra: 01 sự cố

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 Phần mềm Công báo tỉnh Cà Mau	3	Dự kiến: 24-25/10/2024	

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: 0 đồng
- Kinh phí thường xuyên từ NSNN chi cho an toàn thông tin: 3.488 triệu đồng.
- Tỷ 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: 3.488 triệu đồng /50.000 triệu đồng (tỷ lệ 0,06 %)

Trong đó gồm:

- Kinh phí giám sát an toàn thông tin: 2.000 triệu đồng
- Kinh phí kiểm tra, đánh giá an toàn thông tin: 1.000 triệu đồng
- Kinh phí diễn tập, ứng cứu sự cố an toàn thông tin: 190 triệu đồng
- Kinh phí đào tạo, tập huấn và tuyên truyền, nâng cao nhận thức về an toàn thông tin: 298 triệu đồng
- 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 chi cho an toàn thông tin	Kinh phí thường xuyên từ ngân sách nhà nước chi 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	0	3.000 triệu đồng	3.000 triệu đồng	0	3.000 triệu đồng /50.000 triệu đồng (tỷ lệ 0, 06%)
2	2023	0	3.488 triệu đồng	3.488 triệu đồng	0	3.488 triệu đồng /50.00 triệu đồng (tỷ lệ 0, 06%)
3	2024	0	3.000 triệu đồng	3.000 triệu đồng	0	3.000 triệu đồng /50.000 triệu đồng (tỷ lệ 0, 06%)

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

- Kinh phí đầu tư từ NSNN chi cho an toàn thông tin: 0 đồng

- Kinh phí thường xuyên từ NSNN chi cho an toàn thông tin: 3.000 triệu đồng - 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: 3.000 triệu đồng / 50.000 triệu đồng (tỷ lệ 0,06%)

Trong đó gồm:

- Kinh phí giám sát an toàn thông tin: 2.000 triệu đồng

- Kinh phí kiểm tra, đánh giá an toàn thông tin: 1.000 triệu đồng

- Kinh phí diễn tập, ứng cứu sự cố an toàn thông tin: 0 đồng

- Kinh phí đào tạo, tập huấn và tuyên truyền, nâng cao nhận thức về an toàn thông tin: 0 đồng

- 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 /STTTT-CNTTBCVT ngày 26 tháng 4 năm 2024
của Sở 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 cơ sở dữ liệu hợp đồng, giao dịch đã được công chứng, chứng thực trên địa bàn tỉnh Cà Mau	2	Đã phê duyệt		x	x	x	x	x	x
2	Cổng thông tin điện tử Đảng bộ tỉnh Cà Mau	2	Đã phê duyệt		x	x	x	x	x	x
3	Phần mềm Quản lý lao động trên địa bàn tỉnh Cà Mau	2	Đã phê duyệt		x	x	x	x	x	x

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: **Cổng thông tin điện tử tỉnh Cà Mau**

2.1.2. Hiện trạng phê duyệt Hồ sơ đề xuất cấp độ: 3

- Đã phê duyệt : ☒ Quyết định số: 05/QĐ-UBND Ngày phê duyệt: 04/1/2022

- 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)			
1	Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn	Sử dụng giải pháp VPN trên thiết bị Sophos Firewall XG650. Đối với các đơn vị thứ 3 khi hỗ trợ, phối hợp khắc phục lỗi phần mềm khi kết nối vào hệ thống, Trung tâm đã áp dụng các chính sách bảo mật như: giải pháp truy cập bằng key và mật khẩu, giới hạn, chỉ cho phép truy cập theo địa chỉ IP Public của đơn vị đó đã đăng ký. Sau khi khắc phục sự cố xong thực hiện đóng cổng.	
2	Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập	Giữa các vùng mạng trong hệ thống được trang bị thiết bị tường lửa IDS/IPS Sophos Firewall XG650; Tường lửa Fortinet 1000C; Tường lửa Web Barracuda Web Application Firewall 660; tường lửa mềm trên các máy chủ Ubuntu Server 20.04.	
3	Có phương án phòng chống tấn công mạng cho ứng dụng web	Hệ thống được trang bị: - 02 thiết bị tường lửa Sophos XG650. - 02 thiết bị tường lửa Fortinet 1000C. - 02 thiết bị tường lửa ứng dụng Barracuda WAF 660 có tích hợp tính năng chống ATP, Bot Protection. - 01 thiết bị phòng chống DDoS Arbor (lớp ngoài).	

STT	Yêu cầu	Giải pháp/thiết bị/phương án đang triển khai	Ghi chú
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)	Hệ thống được trang bị: - 02 thiết bị Peplink Balance 710. - 02 thiết bị Core Switch Aruba 5412R.	
5	Có phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu	Giải pháp: các máy chủ dữ liệu được đặt nằm trong vùng an toàn (vùng không kết nối mạng internet), Vùng mạng này được bảo vệ bằng thiết bị tường lửa Sophos Firewall XG650; Tường lửa Fortinet 1000C (trên thiết bị thiết lập các chính sách mở cổng kết nối về dữ liệu), các máy chủ được cài đặt phần mềm phòng chống mã độc Kaspersky Endpoint Security. Giải pháp bảo vệ cơ sở dữ liệu Imperva.	
6	Có phương án chặn lọc phần mềm độc hại trên môi trường mạng	Hệ thống Trung tâm lưu trữ dữ liệu được trang bị các thiết bị tường lửa (Sophos Firewall XG650; Tường lửa Fortinet 1000C; Barracuda Web Application Firewall 660); phần mềm phòng chống mã độc Kaspersky Endpoint Security.	
7	Có phương án phòng chống tấn công từ chối dịch vụ	Hệ thống có 01 thiết bị phòng chống tấn công DDoS: Arbor Networks APS-2600-500	
8	Có phương án bảo đảm an toàn thông tin cho hệ thống thư điện tử (nếu có)	Không trực tiếp kết nối	
9	Có phương án quản lý truy cập lớp mạng	Được thiết lập chính sách truy cập lớp mạng trên thiết bị Sophos Firewall XG650.	

STT	Yêu cầu	Giải pháp/thiết bị/phương án đang triển khai	Ghi chú
10	Có phương án giám sát hệ thống thông tin tập trung	Hệ thống được triển khai giải pháp giám sát mạng: Hiện đang dùng sản phẩm Splunk (từ năm 2020 đến nay).	
11	Có phương án giám sát an toàn hệ thống thông tin tập trung	- Triển khai giám sát an toàn hệ thống thông tin của tỉnh (SOC) và được thiết lập kết nối, chia sẻ thông tin với hệ thống kỹ thuật của Trung tâm Giám sát an toàn không gian mạng quốc gia. - Toàn bộ log của các máy chủ, thiết bị được lưu trữ trên hệ thống Security Information & Event Management (SIEM).	
12	Có phương án quản lý sao lưu dự phòng tập trung	VMware Site Recovery Manager (SRM): hệ thống SAN V7000 (dung lượng 140TB), NetApp EF300 (dung lượng 46TB, sao lưu dữ liệu của hệ thống thông tin giải quyết thủ tục hành chính tỉnh.	
13	Có phương án quản lý phần mềm phòng chống mã độc trên máy chủ/máy tính người dùng	Sử dụng giải pháp phòng chống mã độc: Kaspersky Endpoint Security và được thiết lập kết nối, chia sẻ thông tin với hệ thống kỹ thuật của Trung tâm Giám sát an toàn không gian mạng quốc gia. Toàn bộ máy chủ của hệ thống thông tin giải quyết thủ tục hành chính tỉnh tại Trung tâm lưu trữ dữ liệu được cài đặt phần mềm Kaspersky Endpoint Security.	
14	Có phương án phòng, chống thất thoát dữ liệu	- Bảo vệ dữ liệu của hệ thống, tránh việc bị đánh cắp, rò rỉ bằng cách kết hợp sử dụng: tường lửa nội bộ của máy chủ cơ sở dữ liệu, tường lửa Imperva bảo vệ các cơ sở dữ liệu, tường lửa WAF, tường	

STT	Yêu cầu	Giải pháp/thiết bị/phương án đang triển khai	Ghi chú
		lừa chống IDS, IPS và hệ thống SOC giám sát hoạt động của hệ thống. - Chống thất thoát dữ liệu trên đường truyền và máy trạm bằng cách: thiết lập kết nối an toàn giữa máy chủ cơ sở dữ liệu và máy chủ ứng dụng với người dung theo chuẩn TLS và https; sử dụng phần mềm Kaspersky Endpoint Security. Thực hiện nghiêm quy chế vận hành hệ thống, bảo đảm cho hoạt động của Trung tâm dữ liệu và Trung tâm dữ liệu dự phòng, bảo đảm khả năng khôi phục hệ thống trước sự cố.	
15	Có phương án dự phòng kết nối mạng Internet cho các máy chủ dịch vụ	Hệ thống thông tin giải quyết thủ tục hành chính tỉnh hiện sử dụng 02 đường truyền: - 01 đường truyền internet dạng kênh truyền trực tiếp do nhà mạng VNPT cung cấp để hosting các ứng dụng dùng chung. - 01 đường truyền internet dạng kênh truyền trực tiếp do nhà mạng Viettel cung cấp để hosting các ứng dụng dùng chung.	
16	Có phương án bảo đảm an toàn cho mạng không dây (nếu có)	Không kết nối trực tiếp với với hệ thống cơ sở dữ liệu quốc gia về dân cư, hệ thống định danh và xác thực điện tử.	

2.2. Hệ thống thông tin 2

2.2.1. Tên hệ thống thông tin: **Công báo điện tử tỉnh Cà Mau**

2.2.2. Hiện trạng phê duyệt Hồ sơ đề xuất cấp độ: 3

- Đã phê duyệt : ☒ Quyết định số: 05/QĐ-UBND Ngày phê duyệt: 04/1/2022

- Chưa phê duyệt : ☐

2.2.3. 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)			
1	Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn	Sử dụng giải pháp VPN trên thiết bị Sophos Firewall XG650. Đối với các đơn vị thứ 3 khi hỗ trợ, phối hợp khắc phục lỗi phần mềm khi kết nối vào hệ thống, Trung tâm đã áp dụng các chính sách bảo mật như: giải pháp truy cập bằng key và mật khẩu, giới hạn, chỉ cho phép truy cập theo địa chỉ IP Public của đơn vị đó đã đăng ký. Sau khi khắc phục sự cố xong thực hiện đóng cổng.	
2	Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập	Giữa các vùng mạng trong hệ thống được trang bị thiết bị tường lửa IDS/IPS Sophos Firewall XG650; Tường lửa Fortinet 1000C; Tường lửa Web Barracuda Web Application Firewall 660; tường lửa mềm trên các máy chủ Ubuntu Server 20.04.	
3	Có phương án phòng chống tấn công mạng cho ứng dụng web	Hệ thống được trang bị: - 02 thiết bị tường lửa Sophos XG650. - 02 thiết bị tường lửa Fortinet 1000C.	

STT	Yêu cầu	Giải pháp/thiết bị/phương án đang triển khai	Ghi chú
		- 02 thiết bị tường lửa ứng dụng Barracuda WAF 660 có tích hợp tính năng chống ATP, Bot Protection. - 01 thiết bị phòng chống DDoS Arbor (lớp ngoài).	
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)	Hệ thống được trang bị: - 02 thiết bị Peplink Balance 710. - 02 thiết bị Core Switch Aruba 5412R.	
5	Có phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu	Giải pháp: các máy chủ dữ liệu được đặt nằm trong vùng an toàn (vùng không kết nối mạng internet), Vùng mạng này được bảo vệ bằng thiết bị tường lửa Sophos Firewall XG650; Tường lửa Fortinet 1000C (trên thiết bị thiết lập các chính sách mở cổng kết nối về dữ liệu), các máy chủ được cài đặt phần mềm phòng chống mã độc Kaspersky Endpoint Security. Giải pháp bảo vệ cơ sở dữ liệu Imperva.	
6	Có phương án chặn lọc phần mềm độc hại trên môi trường mạng	Hệ thống Trung tâm lưu trữ dữ liệu được trang bị các thiết bị tường lửa (Sophos Firewall XG650; Tường lửa Fortinet 1000C; Barracuda Web Application Firewall 660); phần mềm phòng chống mã độc Kaspersky Endpoint Security.	
7	Có phương án phòng chống tấn công từ chối dịch vụ	Hệ thống có 01 thiết bị phòng chống tấn công DDoS: Arbor Networks APS-2600-500	

STT	Yêu cầu	Giải pháp/thiết bị/phương án đang triển khai	Ghi chú
8	Có phương án bảo đảm an toàn thông tin cho hệ thống thư điện tử (nếu có)	Không trực tiếp kết nối	
9	Có phương án quản lý truy cập lớp mạng	Được thiết lập chính sách truy cập lớp mạng trên thiết bị Sophos Firewall XG650.	
10	Có phương án giám sát hệ thống thông tin tập trung	Hệ thống được triển khai giải pháp giám sát mạng: Hiện đang dùng sản phẩm Splunk (từ năm 2020 đến nay).	
11	Có phương án giám sát an toàn hệ thống thông tin tập trung	- Triển khai giám sát an toàn hệ thống thông tin của tỉnh (SOC) và được thiết lập kết nối, chia sẻ thông tin với hệ thống kỹ thuật của Trung tâm Giám sát an toàn không gian mạng quốc gia. - Toàn bộ log của các máy chủ, thiết bị được lưu trữ trên hệ thống Security Information & Event Management (SIEM).	
12	Có phương án quản lý sao lưu dự phòng tập trung	VMware Site Recovery Manager (SRM): hệ thống SAN V7000 (dung lượng 140TB), NetApp EF300 (dung lượng 46TB, sao lưu dữ liệu của hệ thống thông tin giải quyết thủ tục hành chính tỉnh.	
13	Có phương án quản lý phần mềm phòng chống mã độc trên máy chủ/máy tính người dùng	Sử dụng giải pháp phòng chống mã độc: Kaspersky Endpoint Security và được thiết lập kết nối, chia sẻ thông tin với hệ thống kỹ thuật của Trung tâm Giám sát an toàn không gian mạng quốc gia. Toàn bộ máy chủ của hệ thống thông tin giải quyết thủ tục hành chính tỉnh tại Trung tâm lưu trữ dữ	

STT	Yêu cầu	Giải pháp/thiết bị/phương án đang triển khai	Ghi chú
		liệu được cài đặt phần mềm Kaspersky Endpoint Security.	
14	Có phương án phòng, chống thất thoát dữ liệu	- Bảo vệ dữ liệu của hệ thống, tránh việc bị đánh cắp, rò rỉ bằng cách kết hợp sử dụng: tường lửa nội bộ của máy chủ cơ sở dữ liệu, tường lửa Imperva bảo vệ các cơ sở dữ liệu, tường lửa WAF, tường lửa chống IDS, IPS và hệ thống SOC giám sát hoạt động của hệ thống. - Chống thất thoát dữ liệu trên đường truyền và máy trạm bằng cách: thiết lập kết nối an toàn giữa máy chủ cơ sở dữ liệu và máy chủ ứng dụng với người dung theo chuẩn TLS và https; sử dụng phần mềm Kaspersky Endpoint Security. Thực hiện nghiêm quy chế vận hành hệ thống, bảo đảm cho hoạt động của Trung tâm dữ liệu và Trung tâm dữ liệu dự phòng, bảo đảm khả năng khôi phục hệ thống trước sự cố.	
15	Có phương án dự phòng kết nối mạng Internet cho các máy chủ dịch vụ	Hệ thống thông tin giải quyết thủ tục hành chính tỉnh hiện sử dụng 02 đường truyền: - 01 đường truyền internet dạng kênh truyền trực tiếp do nhà mạng VNPT cung cấp để hosting các ứng dụng dùng chung. - 01 đường truyền internet dạng kênh truyền trực tiếp do nhà mạng Viettel cung cấp để hosting các ứng dụng dùng chung.	

STT	Yêu cầu	Giải pháp/thiết bị/phương án đang triển khai	Ghi chú
16	Có phương án bảo đảm an toàn cho mạng không dây (nếu có)	Không kết nối trực tiếp với với hệ thống cơ sở dữ liệu quốc gia về dân cư, hệ thống định danh và xác thực điện tử.	

2.3. Hệ thống thông tin 3

2.3.1. Tên hệ thống thông tin: **Hệ thống thông tin giải quyết Thủ tục hành chính tỉnh Cà Mau**

2.3.2. Hiện trạng phê duyệt Hồ sơ đề xuất cấp độ: 3

- Đã phê duyệt : ☒ Quyết định số: 03/QĐ-UBND Ngày phê duyệt: 04/1/2022

- Chưa phê duyệt : ☐

2.3.3. 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)			
1	Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn	Sử dụng giải pháp VPN trên thiết bị Sophos Firewall XG650. Đối với các đơn vị thứ 3 khi hỗ trợ, phối hợp khắc phục lỗi phần mềm khi kết nối vào hệ thống, Trung tâm đã áp dụng các chính sách bảo mật như: giải pháp truy cập bằng key và mật khẩu, giới hạn, chỉ cho phép truy cập theo địa chỉ IP Public của đơn vị đó đã đăng ký. Sau khi khắc phục sự cố xong thực hiện đóng cổng.	

STT	Yêu cầu	Giải pháp/thiết bị/phương án đang triển khai	Ghi chú
2	Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập	Giữa các vùng mạng trong hệ thống được trang bị thiết bị tường lửa IDS/IPS Sophos Firewall XG650; Tường lửa Fortinet 1000C; Tường lửa Web Barracuda Web Application Firewall 660; tường lửa mềm trên các máy chủ Ubuntu Server 20.04.	
3	Có phương án phòng chống tấn công mạng cho ứng dụng web	Hệ thống được trang bị: - 02 thiết bị tường lửa Sophos XG650. - 02 thiết bị tường lửa Fortinet 1000C. - 02 thiết bị tường lửa ứng dụng Barracuda WAF 660 có tích hợp tính năng chống ATP, Bot Protection. - 01 thiết bị phòng chống DDoS Arbor (lớp ngoài).	
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)	Hệ thống được trang bị: - 02 thiết bị Peplink Balance 710. - 02 thiết bị Core Switch Aruba 5412R.	
5	Có phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu	Giải pháp: các máy chủ dữ liệu được đặt nằm trong vùng an toàn (vùng không kết nối mạng internet), Vùng mạng này được bảo vệ bằng thiết bị tường lửa Sophos Firewall XG650; Tường lửa Fortinet 1000C (trên thiết bị thiết lập các chính sách mở cổng kết nối về dữ liệu), các máy chủ được cài đặt phần mềm phòng chống mã độc Kaspersky Endpoint Security. Giải pháp bảo vệ cơ sở dữ liệu Imperva.	

STT	Yêu cầu	Giải pháp/thiết bị/phương án đang triển khai	Ghi chú
6	Có phương án chặn lọc phần mềm độc hại trên môi trường mạng	Hệ thống Trung tâm lưu trữ dữ liệu được trang bị các thiết bị tường lửa (Sophos Firewall XG650; Tường lửa Fortinet 1000C; Barracuda Web Application Firewall 660); phần mềm phòng chống mã độc Kaspersky Endpoint Security.	
7	Có phương án phòng chống tấn công từ chối dịch vụ	Hệ thống có 01 thiết bị phòng chống tấn công DDoS: Arbor Networks APS-2600-500	
8	Có phương án bảo đảm an toàn thông tin cho hệ thống thư điện tử (nếu có)	Không trực tiếp kết nối	
9	Có phương án quản lý truy cập lớp mạng	Được thiết lập chính sách truy cập lớp mạng trên thiết bị Sophos Firewall XG650.	
10	Có phương án giám sát hệ thống thông tin tập trung	Hệ thống được triển khai giải pháp giám sát mạng: Hiện đang dùng sản phẩm Splunk (từ năm 2020 đến nay).	
11	Có phương án giám sát an toàn hệ thống thông tin tập trung	- Triển khai giám sát an toàn hệ thống thông tin của tỉnh (SOC) và được thiết lập kết nối, chia sẻ thông tin với hệ thống kỹ thuật của Trung tâm Giám sát an toàn không gian mạng quốc gia. - Toàn bộ log của các máy chủ, thiết bị được lưu trữ trên hệ thống Security Information & Event Management (SIEM).	
12	Có phương án quản lý sao lưu dự phòng tập trung	VMware Site Recovery Manager (SRM): hệ thống SAN V7000 (dung lượng 140TB), NetApp EF300 (dung lượng 46TB, sao lưu dữ liệu của hệ thống thông tin giải quyết thủ tục hành chính tỉnh.	

STT	Yêu cầu	Giải pháp/thiết bị/phương án đang triển khai	Ghi chú
13	Có phương án quản lý phần mềm phòng chống mã độc trên máy chủ/máy tính người dùng	Sử dụng giải pháp phòng chống mã độc: Kaspersky Endpoint Security và được thiết lập kết nối, chia sẻ thông tin với hệ thống kỹ thuật của Trung tâm Giám sát an toàn không gian mạng quốc gia. Toàn bộ máy chủ của hệ thống thông tin giải quyết thủ tục hành chính tỉnh tại Trung tâm lưu trữ dữ liệu được cài đặt phần mềm Kaspersky Endpoint Security.	
14	Có phương án phòng, chống thất thoát dữ liệu	- Bảo vệ dữ liệu của hệ thống, tránh việc bị đánh cắp, rò rỉ bằng cách kết hợp sử dụng: tường lửa nội bộ của máy chủ cơ sở dữ liệu, tường lửa Imperva bảo vệ các cơ sở dữ liệu, tường lửa WAF, tường lửa chống IDS, IPS và hệ thống SOC giám sát hoạt động của hệ thống. - Chống thất thoát dữ liệu trên đường truyền và máy trạm bằng cách: thiết lập kết nối an toàn giữa máy chủ cơ sở dữ liệu và máy chủ ứng dụng với người dùng theo chuẩn TLS và https; sử dụng phần mềm Kaspersky Endpoint Security. Thực hiện nghiêm quy chế vận hành hệ thống, bảo đảm cho hoạt động của Trung tâm dữ liệu và Trung tâm dữ liệu dự phòng, bảo đảm khả năng khôi phục hệ thống trước sự cố.	
15	Có phương án dự phòng kết nối mạng Internet cho các máy chủ dịch vụ	Hệ thống thông tin giải quyết thủ tục hành chính tỉnh hiện sử dụng 02 đường truyền:	

STT	Yêu cầu	Giải pháp/thiết bị/phương án đang triển khai	Ghi chú
		- 01 đường truyền internet dạng kênh truyền trực tiếp do nhà mạng VNPT cung cấp để hosting các ứng dụng dùng chung. - 01 đường truyền internet dạng kênh truyền trực tiếp do nhà mạng Viettel cung cấp để hosting các ứng dụng dùng chung.	
16	Có phương án bảo đảm an toàn cho mạng không dây (nếu có)	Không kết nối trực tiếp với với hệ thống cơ sở dữ liệu quốc gia về dân cư, hệ thống định danh và xác thực điện tử.	

2.4. Hệ thống thông tin 4

2.4.1. Tên hệ thống thông tin: **Phần mềm Quản lý Cán bộ Công chức Viên chức tỉnh Cà Mau**

2.4.2. Hiện trạng phê duyệt Hồ sơ đề xuất cấp độ: 3

- Đã phê duyệt : ☒ Quyết định số: 3126/QĐ-UBND Ngày phê duyệt: 31/12/2022

- Chưa phê duyệt : ☐

2.4.3. 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)			
1	Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn	Sử dụng giải pháp VPN trên thiết bị Sophos Firewall XG650. Đối với các đơn vị thứ 3 khi hỗ trợ, phối hợp khắc phục lỗi phần mềm khi kết nối	

STT	Yêu cầu	Giải pháp/thiết bị/phương án đang triển khai	Ghi chú
		vào hệ thống, Trung tâm đã áp dụng các chính sách bảo mật như: giải pháp truy cập bằng key và mật khẩu, giới hạn, chỉ cho phép truy cập theo địa chỉ IP Public của đơn vị đó đã đăng ký. Sau khi khắc phục sự cố xong thực hiện đóng cổng.	
2	Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập	Giữa các vùng mạng trong hệ thống được trang bị thiết bị tường lửa IDS/IPS Sophos Firewall XG650; Tường lửa Fortinet 1000C; Tường lửa Web Barracuda Web Application Firewall 660; tường lửa mềm trên các máy chủ Ubuntu Server 20.04.	
3	Có phương án phòng chống tấn công mạng cho ứng dụng web	Hệ thống được trang bị: - 02 thiết bị tường lửa Sophos XG650. - 02 thiết bị tường lửa Fortinet 1000C. - 02 thiết bị tường lửa ứng dụng Barracuda WAF 660 có tích hợp tính năng chống ATP, Bot Protection. - 01 thiết bị phòng chống DDoS Arbor (lớp ngoài).	
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)	Hệ thống được trang bị: - 02 thiết bị Peplink Balance 710. - 02 thiết bị Core Switch Aruba 5412R.	
5	Có phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu	Giải pháp: các máy chủ dữ liệu được đặt nằm trong vùng an toàn (vùng không kết nối mạng internet), Vùng mạng này được bảo vệ bằng thiết bị tường lửa Sophos Firewall XG650; Tường lửa	

STT	Yêu cầu	Giải pháp/thiết bị/phương án đang triển khai	Ghi chú
		Fortinet 1000C (trên thiết bị thiết lập các chính sách mở cổng kết nối về dữ liệu), các máy chủ được cài đặt phần mềm phòng chống mã độc Kaspersky Endpoint Security. Giải pháp bảo vệ cơ sở dữ liệu Imperva.	
6	Có phương án chặn lọc phần mềm độc hại trên môi trường mạng	Hệ thống Trung tâm lưu trữ dữ liệu được trang bị các thiết bị tường lửa (Sophos Firewall XG650; Tường lửa Fortinet 1000C; Barracuda Web Application Firewall 660); phần mềm phòng chống mã độc Kaspersky Endpoint Security.	
7	Có phương án phòng chống tấn công từ chối dịch vụ	Hệ thống có 01 thiết bị phòng chống tấn công DDoS: Arbor Networks APS-2600-500	
8	Có phương án bảo đảm an toàn thông tin cho hệ thống thư điện tử (nếu có)	Không trực tiếp kết nối	
9	Có phương án quản lý truy cập lớp mạng	Được thiết lập chính sách truy cập lớp mạng trên thiết bị Sophos Firewall XG650.	
10	Có phương án giám sát hệ thống thông tin tập trung	Hệ thống được triển khai giải pháp giám sát mạng: Hiện đang dùng sản phẩm Splunk (từ năm 2020 đến nay).	
11	Có phương án giám sát an toàn hệ thống thông tin tập trung	- Triển khai giám sát an toàn hệ thống thông tin của tỉnh (SOC) và được thiết lập kết nối, chia sẻ thông tin với hệ thống kỹ thuật của Trung tâm Giám sát an toàn không gian mạng quốc gia.	

STT	Yêu cầu	Giải pháp/thiết bị/phương án đang triển khai	Ghi chú
		- Toàn bộ log của các máy chủ, thiết bị được lưu trữ trên hệ thống Security Information & Event Management (SIEM).	
12	Có phương án quản lý sao lưu dự phòng tập trung	VMware Site Recovery Manager (SRM): hệ thống SAN V7000 (dung lượng 140TB), NetApp EF300 (dung lượng 46TB, sao lưu dữ liệu của hệ thống thông tin giải quyết thủ tục hành chính tỉnh.	
13	Có phương án quản lý phần mềm phòng chống mã độc trên máy chủ/máy tính người dùng	Sử dụng giải pháp phòng chống mã độc: Kaspersky Endpoint Security và được thiết lập kết nối, chia sẻ thông tin với hệ thống kỹ thuật của Trung tâm Giám sát an toàn không gian mạng quốc gia. Toàn bộ máy chủ của hệ thống thông tin giải quyết thủ tục hành chính tỉnh tại Trung tâm lưu trữ dữ liệu được cài đặt phần mềm Kaspersky Endpoint Security.	
14	Có phương án phòng, chống thất thoát dữ liệu	- Bảo vệ dữ liệu của hệ thống, tránh việc bị đánh cắp, rò rỉ bằng cách kết hợp sử dụng: tường lửa nội bộ của máy chủ cơ sở dữ liệu, tường lửa Imperva bảo vệ các cơ sở dữ liệu, tường lửa WAF, tường lửa chống IDS, IPS và hệ thống SOC giám sát hoạt động của hệ thống. - Chống thất thoát dữ liệu trên đường truyền và máy trạm bằng cách: thiết lập kết nối an toàn giữa máy chủ cơ sở dữ liệu và máy chủ ứng dụng với người dung theo chuẩn TLS và https; sử dụng phần mềm Kaspersky Endpoint Security.	

STT	Yêu cầu	Giải pháp/thiết bị/phương án đang triển khai	Ghi chú
		Thực hiện nghiêm quy chế vận hành hệ thống, bảo đảm cho hoạt động của Trung tâm dữ liệu và Trung tâm dữ liệu dự phòng, bảo đảm khả năng khôi phục hệ thống trước sự cố.	
15	Có phương án dự phòng kết nối mạng Internet cho các máy chủ dịch vụ	Hệ thống thông tin giải quyết thủ tục hành chính tỉnh hiện sử dụng 02 đường truyền: - 01 đường truyền internet dạng kênh truyền trực tiếp do nhà mạng VNPT cung cấp để hosting các ứng dụng dùng chung. - 01 đường truyền internet dạng kênh truyền trực tiếp do nhà mạng Viettel cung cấp để hosting các ứng dụng dùng chung.	
16	Có phương án bảo đảm an toàn cho mạng không dây (nếu có)	Không kết nối trực tiếp với với hệ thống cơ sở dữ liệu quốc gia về dân cư, hệ thống định danh và xác thực điện tử.	

2.5. Hệ thống thông tin 5

2.5.1. Tên hệ thống thông tin: **Phần mềm Quản lý Văn bản và điều hành**

2.5.2. Hiện trạng phê duyệt Hồ sơ đề xuất cấp độ: 3

- Đã phê duyệt : ☒ Quyết định số: 04/QĐ-UBND Ngày phê duyệt: 04/1/2022

- Chưa phê duyệt : ☐

2.5.3. 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			

STT	Yêu cầu	Giải pháp/thiết bị/phương án đang triển khai	Ghi chú
(- 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)			
1	Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn	Sử dụng giải pháp VPN trên thiết bị Sophos Firewall XG650. Đối với các đơn vị thứ 3 khi hỗ trợ, phối hợp khắc phục lỗi phần mềm khi kết nối vào hệ thống, Trung tâm đã áp dụng các chính sách bảo mật như: giải pháp truy cập bằng key và mật khẩu, giới hạn, chỉ cho phép truy cập theo địa chỉ IP Public của đơn vị đó đã đăng ký. Sau khi khắc phục sự cố xong thực hiện đóng cổng.	
2	Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập	Giữa các vùng mạng trong hệ thống được trang bị thiết bị tường lửa IDS/IPS Sophos Firewall XG650; Tường lửa Fortinet 1000C; Tường lửa Web Barracuda Web Application Firewall 660; tường lửa mềm trên các máy chủ Ubuntu Server 20.04.	
3	Có phương án phòng chống tấn công mạng cho ứng dụng web	Hệ thống được trang bị: - 02 thiết bị tường lửa Sophos XG650. - 02 thiết bị tường lửa Fortinet 1000C. - 02 thiết bị tường lửa ứng dụng Barracuda WAF 660 có tích hợp tính năng chống ATP, Bot Protection. - 01 thiết bị phòng chống DDoS Arbor (lớp ngoài).	

STT	Yêu cầu	Giải pháp/thiết bị/phương án đang triển khai	Ghi chú
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)	Hệ thống được trang bị: - 02 thiết bị Peplink Balance 710. - 02 thiết bị Core Switch Aruba 5412R.	
5	Có phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu	Giải pháp: các máy chủ dữ liệu được đặt nằm trong vùng an toàn (vùng không kết nối mạng internet), Vùng mạng này được bảo vệ bằng thiết bị tường lửa Sophos Firewall XG650; Tường lửa Fortinet 1000C (trên thiết bị thiết lập các chính sách mở cổng kết nối về dữ liệu), các máy chủ được cài đặt phần mềm phòng chống mã độc Kaspersky Endpoint Security. Giải pháp bảo vệ cơ sở dữ liệu Imperva.	
6	Có phương án chặn lọc phần mềm độc hại trên môi trường mạng	Hệ thống Trung tâm lưu trữ dữ liệu được trang bị các thiết bị tường lửa (Sophos Firewall XG650; Tường lửa Fortinet 1000C; Barracuda Web Application Firewall 660); phần mềm phòng chống mã độc Kaspersky Endpoint Security.	
7	Có phương án phòng chống tấn công từ chối dịch vụ	Hệ thống có 01 thiết bị phòng chống tấn công DDoS: Arbor Networks APS-2600-500	
8	Có phương án bảo đảm an toàn thông tin cho hệ thống thư điện tử (nếu có)	Không trực tiếp kết nối	
9	Có phương án quản lý truy cập lớp mạng	Được thiết lập chính sách truy cập lớp mạng trên thiết bị Sophos Firewall XG650.	

STT	Yêu cầu	Giải pháp/thiết bị/phương án đang triển khai	Ghi chú
10	Có phương án giám sát hệ thống thông tin tập trung	Hệ thống được triển khai giải pháp giám sát mạng: Hiện đang dùng sản phẩm Splunk (từ năm 2020 đến nay).	
11	Có phương án giám sát an toàn hệ thống thông tin tập trung	- Triển khai giám sát an toàn hệ thống thông tin của tỉnh (SOC) và được thiết lập kết nối, chia sẻ thông tin với hệ thống kỹ thuật của Trung tâm Giám sát an toàn không gian mạng quốc gia. - Toàn bộ log của các máy chủ, thiết bị được lưu trữ trên hệ thống Security Information & Event Management (SIEM).	
12	Có phương án quản lý sao lưu dự phòng tập trung	VMware Site Recovery Manager (SRM): hệ thống SAN V7000 (dung lượng 140TB), NetApp EF300 (dung lượng 46TB, sao lưu dữ liệu của hệ thống thông tin giải quyết thủ tục hành chính tỉnh.	
13	Có phương án quản lý phần mềm phòng chống mã độc trên máy chủ/máy tính người dùng	Sử dụng giải pháp phòng chống mã độc: Kaspersky Endpoint Security và được thiết lập kết nối, chia sẻ thông tin với hệ thống kỹ thuật của Trung tâm Giám sát an toàn không gian mạng quốc gia. Toàn bộ máy chủ của hệ thống thông tin giải quyết thủ tục hành chính tỉnh tại Trung tâm lưu trữ dữ liệu được cài đặt phần mềm Kaspersky Endpoint Security.	
14	Có phương án phòng, chống thất thoát dữ liệu	- Bảo vệ dữ liệu của hệ thống, tránh việc bị đánh cắp, rò rỉ bằng cách kết hợp sử dụng: tường lửa nội bộ của máy chủ cơ sở dữ liệu, tường lửa Imperva bảo vệ các cơ sở dữ liệu, tường lửa WAF, tường	

STT	Yêu cầu	Giải pháp/thiết bị/phương án đang triển khai	Ghi chú
		lừa chống IDS, IPS và hệ thống SOC giám sát hoạt động của hệ thống. - Chống thất thoát dữ liệu trên đường truyền và máy trạm bằng cách: thiết lập kết nối an toàn giữa máy chủ cơ sở dữ liệu và máy chủ ứng dụng với người dung theo chuẩn TLS và https; sử dụng phần mềm Kaspersky Endpoint Security. Thực hiện nghiêm quy chế vận hành hệ thống, bảo đảm cho hoạt động của Trung tâm dữ liệu và Trung tâm dữ liệu dự phòng, bảo đảm khả năng khôi phục hệ thống trước sự cố.	
15	Có phương án dự phòng kết nối mạng Internet cho các máy chủ dịch vụ	Hệ thống thông tin giải quyết thủ tục hành chính tỉnh hiện sử dụng 02 đường truyền: - 01 đường truyền internet dạng kênh truyền trực tiếp do nhà mạng VNPT cung cấp để hosting các ứng dụng dùng chung. - 01 đường truyền internet dạng kênh truyền trực tiếp do nhà mạng Viettel cung cấp để hosting các ứng dụng dùng chung.	
16	Có phương án bảo đảm an toàn cho mạng không dây (nếu có)	Không kết nối trực tiếp với với hệ thống cơ sở dữ liệu quốc gia về dân cư, hệ thống định danh và xác thực điện tử.	

2.6. Hệ thống thông tin 6

2.6.1. Tên hệ thống thông tin: **Hệ thống thư điện tử tỉnh Cà Mau**

2.6.2. Hiện trạng phê duyệt Hồ sơ đề xuất cấp độ: 3

- Đã phê duyệt : ☒ Quyết định số: 1512/QĐ-UBND Ngày phê duyệt: 09/6/2022

- Chưa phê duyệt : ☐

2.6.3. 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)			
1	Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn	Sử dụng giải pháp VPN trên thiết bị Sophos Firewall XG650. Đối với các đơn vị thứ 3 khi hỗ trợ, phối hợp khắc phục lỗi phần mềm khi kết nối vào hệ thống, Trung tâm đã áp dụng các chính sách bảo mật như: giải pháp truy cập bằng key và mật khẩu, giới hạn, chỉ cho phép truy cập theo địa chỉ IP Public của đơn vị đó đã đăng ký. Sau khi khắc phục sự cố xong thực hiện đóng cổng.	
2	Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập	Giữa các vùng mạng trong hệ thống được trang bị thiết bị tường lửa IDS/IPS Sophos Firewall XG650; Tường lửa Fortinet 1000C; Tường lửa Web Barracuda Web Application Firewall 660; tường lửa mềm trên các máy chủ Ubuntu Server 20.04.	
3	Có phương án phòng chống tấn công mạng cho ứng dụng web	Hệ thống được trang bị: - 02 thiết bị tường lửa Sophos XG650. - 02 thiết bị tường lửa Fortinet 1000C.	

STT	Yêu cầu	Giải pháp/thiết bị/phương án đang triển khai	Ghi chú
		- 02 thiết bị tường lửa ứng dụng Barracuda WAF 660 có tích hợp tính năng chống ATP, Bot Protection. - 01 thiết bị phòng chống DDoS Arbor (lớp ngoài).	
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)	Hệ thống được trang bị: - 02 thiết bị Peplink Balance 710. - 02 thiết bị Core Switch Aruba 5412R.	
5	Có phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu	Giải pháp: các máy chủ dữ liệu được đặt nằm trong vùng an toàn (vùng không kết nối mạng internet), Vùng mạng này được bảo vệ bằng thiết bị tường lửa Sophos Firewall XG650; Tường lửa Fortinet 1000C (trên thiết bị thiết lập các chính sách mở cổng kết nối về dữ liệu), các máy chủ được cài đặt phần mềm phòng chống mã độc Kaspersky Endpoint Security. Giải pháp bảo vệ cơ sở dữ liệu Imperva.	
6	Có phương án chặn lọc phần mềm độc hại trên môi trường mạng	Hệ thống Trung tâm lưu trữ dữ liệu được trang bị các thiết bị tường lửa (Sophos Firewall XG650; Tường lửa Fortinet 1000C; Barracuda Web Application Firewall 660); phần mềm phòng chống mã độc Kaspersky Endpoint Security.	
7	Có phương án phòng chống tấn công từ chối dịch vụ	Hệ thống có 01 thiết bị phòng chống tấn công DDoS: Arbor Networks APS-2600-500	

STT	Yêu cầu	Giải pháp/thiết bị/phương án đang triển khai	Ghi chú
8	Có phương án bảo đảm an toàn thông tin cho hệ thống thư điện tử (nếu có)	Không trực tiếp kết nối	
9	Có phương án quản lý truy cập lớp mạng	Được thiết lập chính sách truy cập lớp mạng trên thiết bị Sophos Firewall XG650.	
10	Có phương án giám sát hệ thống thông tin tập trung	Hệ thống được triển khai giải pháp giám sát mạng: Hiện đang dùng sản phẩm Splunk (từ năm 2020 đến nay).	
11	Có phương án giám sát an toàn hệ thống thông tin tập trung	- Triển khai giám sát an toàn hệ thống thông tin của tỉnh (SOC) và được thiết lập kết nối, chia sẻ thông tin với hệ thống kỹ thuật của Trung tâm Giám sát an toàn không gian mạng quốc gia. - Toàn bộ log của các máy chủ, thiết bị được lưu trữ trên hệ thống Security Information & Event Management (SIEM).	
12	Có phương án quản lý sao lưu dự phòng tập trung	VMware Site Recovery Manager (SRM): hệ thống SAN V7000 (dung lượng 140TB), NetApp EF300 (dung lượng 46TB, sao lưu dữ liệu của hệ thống thông tin giải quyết thủ tục hành chính tỉnh.	
13	Có phương án quản lý phần mềm phòng chống mã độc trên máy chủ/máy tính người dùng	Sử dụng giải pháp phòng chống mã độc: Kaspersky Endpoint Security và được thiết lập kết nối, chia sẻ thông tin với hệ thống kỹ thuật của Trung tâm Giám sát an toàn không gian mạng quốc gia. Toàn bộ máy chủ của hệ thống thông tin giải quyết thủ tục hành chính tỉnh tại Trung tâm lưu trữ dữ	

STT	Yêu cầu	Giải pháp/thiết bị/phương án đang triển khai	Ghi chú
		liệu được cài đặt phần mềm Kaspersky Endpoint Security.	
14	Có phương án phòng, chống thất thoát dữ liệu	- Bảo vệ dữ liệu của hệ thống, tránh việc bị đánh cắp, rò rỉ bằng cách kết hợp sử dụng: tường lửa nội bộ của máy chủ cơ sở dữ liệu, tường lửa Imperva bảo vệ các cơ sở dữ liệu, tường lửa WAF, tường lửa chống IDS, IPS và hệ thống SOC giám sát hoạt động của hệ thống. - Chống thất thoát dữ liệu trên đường truyền và máy trạm bằng cách: thiết lập kết nối an toàn giữa máy chủ cơ sở dữ liệu và máy chủ ứng dụng với người dung theo chuẩn TLS và https; sử dụng phần mềm Kaspersky Endpoint Security. Thực hiện nghiêm quy chế vận hành hệ thống, bảo đảm cho hoạt động của Trung tâm dữ liệu và Trung tâm dữ liệu dự phòng, bảo đảm khả năng khôi phục hệ thống trước sự cố.	
15	Có phương án dự phòng kết nối mạng Internet cho các máy chủ dịch vụ	Hệ thống thông tin giải quyết thủ tục hành chính tỉnh hiện sử dụng 02 đường truyền: - 01 đường truyền internet dạng kênh truyền trực tiếp do nhà mạng VNPT cung cấp để hosting các ứng dụng dùng chung. - 01 đường truyền internet dạng kênh truyền trực tiếp do nhà mạng Viettel cung cấp để hosting các ứng dụng dùng chung.	

STT	Yêu cầu	Giải pháp/thiết bị/phương án đang triển khai	Ghi chú
16	Có phương án bảo đảm an toàn cho mạng không dây (nếu có)	Không kết nối trực tiếp với với hệ thống cơ sở dữ liệu quốc gia về dân cư, hệ thống định danh và xác thực điện tử.	

2.1. Hệ thống thông tin 7

2.7.1. Tên hệ thống thông tin: **Cổng thông tin điện tử Sở Giáo dục và Đào tạo**

2.7.2. Hiện trạng phê duyệt Hồ sơ đề xuất cấp độ: 3

- Đã phê duyệt : ☒ Quyết định số: 3127/QĐ-UBND Ngày phê duyệt: 31/12/2022

- Chưa phê duyệt : ☐

2.7.3. 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)			
1	Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn	Sử dụng giải pháp VPN trên thiết bị Sophos Firewall XG650. Đối với các đơn vị thứ 3 khi hỗ trợ, phối hợp khắc phục lỗi phần mềm khi kết nối vào hệ thống, Trung tâm đã áp dụng các chính sách bảo mật như: giải pháp truy cập bằng key và mật khẩu, giới hạn, chỉ cho phép truy cập theo địa chỉ IP Public của đơn vị đó đã đăng ký. Sau khi khắc phục sự cố xong thực hiện đóng cổng.	

STT	Yêu cầu	Giải pháp/thiết bị/phương án đang triển khai	Ghi chú
2	Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập	Giữa các vùng mạng trong hệ thống được trang bị thiết bị tường lửa IDS/IPS Sophos Firewall XG650; Tường lửa Fortinet 1000C; Tường lửa Web Barracuda Web Application Firewall 660; tường lửa mềm trên các máy chủ Ubuntu Server 20.04.	
3	Có phương án phòng chống tấn công mạng cho ứng dụng web	Hệ thống được trang bị: - 02 thiết bị tường lửa Sophos XG650. - 02 thiết bị tường lửa Fortinet 1000C. - 02 thiết bị tường lửa ứng dụng Barracuda WAF 660 có tích hợp tính năng chống ATP, Bot Protection. - 01 thiết bị phòng chống DDoS Arbor (lớp ngoài).	
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)	Hệ thống được trang bị: - 02 thiết bị Peplink Balance 710. - 02 thiết bị Core Switch Aruba 5412R.	
5	Có phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu	Giải pháp: các máy chủ dữ liệu được đặt nằm trong vùng an toàn (vùng không kết nối mạng internet), Vùng mạng này được bảo vệ bằng thiết bị tường lửa Sophos Firewall XG650; Tường lửa Fortinet 1000C (trên thiết bị thiết lập các chính sách mở cổng kết nối về dữ liệu), các máy chủ được cài đặt phần mềm phòng chống mã độc Kaspersky Endpoint Security. Giải pháp bảo vệ cơ sở dữ liệu Imperva.	

STT	Yêu cầu	Giải pháp/thiết bị/phương án đang triển khai	Ghi chú
6	Có phương án chặn lọc phần mềm độc hại trên môi trường mạng	Hệ thống Trung tâm lưu trữ dữ liệu được trang bị các thiết bị tường lửa (Sophos Firewall XG650; Tường lửa Fortinet 1000C; Barracuda Web Application Firewall 660); phần mềm phòng chống mã độc Kaspersky Endpoint Security.	
7	Có phương án phòng chống tấn công từ chối dịch vụ	Hệ thống có 01 thiết bị phòng chống tấn công DDoS: Arbor Networks APS-2600-500	
8	Có phương án bảo đảm an toàn thông tin cho hệ thống thư điện tử (nếu có)	Không trực tiếp kết nối	
9	Có phương án quản lý truy cập lớp mạng	Được thiết lập chính sách truy cập lớp mạng trên thiết bị Sophos Firewall XG650.	
10	Có phương án giám sát hệ thống thông tin tập trung	Hệ thống được triển khai giải pháp giám sát mạng: Hiện đang dùng sản phẩm Splunk (từ năm 2020 đến nay).	
11	Có phương án giám sát an toàn hệ thống thông tin tập trung	- Triển khai giám sát an toàn hệ thống thông tin của tỉnh (SOC) và được thiết lập kết nối, chia sẻ thông tin với hệ thống kỹ thuật của Trung tâm Giám sát an toàn không gian mạng quốc gia. - Toàn bộ log của các máy chủ, thiết bị được lưu trữ trên hệ thống Security Information & Event Management (SIEM).	
12	Có phương án quản lý sao lưu dự phòng tập trung	VMware Site Recovery Manager (SRM): hệ thống SAN V7000 (dung lượng 140TB), NetApp EF300 (dung lượng 46TB, sao lưu dữ liệu của hệ thống thông tin giải quyết thủ tục hành chính tỉnh.	

STT	Yêu cầu	Giải pháp/thiết bị/phương án đang triển khai	Ghi chú
13	Có phương án quản lý phần mềm phòng chống mã độc trên máy chủ/máy tính người dùng	Sử dụng giải pháp phòng chống mã độc: Kaspersky Endpoint Security và được thiết lập kết nối, chia sẻ thông tin với hệ thống kỹ thuật của Trung tâm Giám sát an toàn không gian mạng quốc gia. Toàn bộ máy chủ của hệ thống thông tin giải quyết thủ tục hành chính tỉnh tại Trung tâm lưu trữ dữ liệu được cài đặt phần mềm Kaspersky Endpoint Security.	
14	Có phương án phòng, chống thất thoát dữ liệu	- Bảo vệ dữ liệu của hệ thống, tránh việc bị đánh cắp, rò rỉ bằng cách kết hợp sử dụng: tường lửa nội bộ của máy chủ cơ sở dữ liệu, tường lửa Imperva bảo vệ các cơ sở dữ liệu, tường lửa WAF, tường lửa chống IDS, IPS và hệ thống SOC giám sát hoạt động của hệ thống. - Chống thất thoát dữ liệu trên đường truyền và máy trạm bằng cách: thiết lập kết nối an toàn giữa máy chủ cơ sở dữ liệu và máy chủ ứng dụng với người dùng theo chuẩn TLS và https; sử dụng phần mềm Kaspersky Endpoint Security. Thực hiện nghiêm quy chế vận hành hệ thống, bảo đảm cho hoạt động của Trung tâm dữ liệu và Trung tâm dữ liệu dự phòng, bảo đảm khả năng khôi phục hệ thống trước sự cố.	
15	Có phương án dự phòng kết nối mạng Internet cho các máy chủ dịch vụ	Hệ thống thông tin giải quyết thủ tục hành chính tỉnh hiện sử dụng 02 đường truyền:	

STT	Yêu cầu	Giải pháp/thiết bị/phương án đang triển khai	Ghi chú
		- 01 đường truyền internet dạng kênh truyền trực tiếp do nhà mạng VNPT cung cấp để hosting các ứng dụng dùng chung. - 01 đường truyền internet dạng kênh truyền trực tiếp do nhà mạng Viettel cung cấp để hosting các ứng dụng dùng chung.	
16	Có phương án bảo đảm an toàn cho mạng không dây (nếu có)	Không kết nối trực tiếp với với hệ thống cơ sở dữ liệu quốc gia về dân cư, hệ thống định danh và xác thực điện tử.	