UBND TỈNH HƯNG YÊN
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 136 /QĐ-STTTT

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

Hưng Yên, ngày 14 tháng 11 năm 2022

QUYẾT ĐỊNH
Về việc phê duyệt cấp độ và phương án an toàn hệ thống thông tin đối với Hệ thống Sàn giao dịch công nghệ tỉnh Hưng Yên

GIÁM ĐỐC SỞ THÔNG TIN VÀ TRUYỀN THÔNG HƯNG YÊN

Căn cứ Luật an toàn thông tin mạng số 86/2015/QH13 ngày 19 tháng 11 năm 2015 của Quốc hội;

Căn cứ Nghị định 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 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ trưởng Bộ Thông tin và Truyền thông Quy định chi tiết và hướng dẫn một số điều của Nghị định 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ tiêu chuẩn Quốc gia TCVN: 11930:2017 về Công nghệ thông tin- các kỹ thuật an toàn- Yêu cầu cơ bản về an toàn hệ thông thông tin theo cấp độ;

Xét đề nghị của Sở Khoa học và Công nghệ tại Tờ trình số 41/TTr-SKHCN ngày 02/11/2022 về việc phê duyệt đề xuất cấp độ an toàn thông tin,

QUYẾT ĐỊNH:

Điều 1. Phê duyệt cấp độ an toàn hệ thống thông tin đối với Hệ thống Sàn giao dịch công nghệ tỉnh Hưng Yên, cụ thể như sau:

1. Thông tin chung:

a) Tên hệ thống thông tin: Hệ thống Sàn giao dịch công nghệ tỉnh Hưng Yên.

b) Đơn vị vận hành hệ thống thông tin: Sở Khoa học và Công nghệ.

c) Địa chỉ: Đường An Vũ, phường Hiến Nam, thành phố Hưng Yên, tỉnh Hưng Yên.

2. Cấp độ an toàn hệ thống thông tin: Cấp độ 2

3. Phương án bảo đảm an toàn thông tin:

a) Phương án bảo đảm an toàn thông tin trong thiết kế hệ thống thông tin tương ứng với cấp độ 2 là phù hợp với Thông tư 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ trưởng Bộ Thông tin và Truyền thông và Tiêu chuẩn Quốc gia

TCVN 11930:2017 về Công nghệ thông tin - các kỹ thuật an toàn - Yêu cầu cơ bản về an toàn hệ thông thông tin theo cấp độ.

b) Phương án bảo đảm an toàn thông tin trong quá trình vận hành hệ thống tương ứng với cấp độ 2 là phù hợp với Thông tư 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ trưởng Bộ Thông tin và Truyền thông và Tiêu chuẩn Quốc gia TCVN 11930:2017 về Công nghệ thông tin - các kỹ thuật an toàn - Yêu cầu cơ bản về an toàn hệ thông thông tin theo cấp độ.

Điều 2. Sở Khoa học và Công nghệ chịu trách nhiệm

1. Thực hiện trách nhiệm bảo đảm an toàn hệ thống thông tin đối với Hệ thống Sàn giao dịch công nghệ tỉnh Hưng Yên theo hồ sơ đính kèm Tờ trình số 41/TTr-SKHCN ngày 02/11/2022 của Sở Khoa học và Công nghệ và theo các quy định tại Điều 22 Nghị định số 85/2016/NĐ-CP của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

2. Thực hiện chế độ báo cáo, chia sẻ thông tin theo quy định tại Điều 13, Điều 14 Thông tư 12/2022/TT-BTTTT, báo cáo định kỳ gửi về Sở Thông tin và Truyền thông trước ngày 10 tháng 12 hàng năm.

Điều 3. Điều khoản thi hành

1. Sở Khoa học và Công nghệ chịu trách nhiệm thi hành Quyết định này.

2. Sở Thông tin và Truyền thông chịu trách nhiệm kiểm tra, giám sát việc thực hiện Quyết định này, báo cáo Uỷ ban nhân dân tỉnh theo quy định của pháp luật./.

Nơi nhận:
- UBND tỉnh (để báo cáo);
- Như Điều 3;
- Giám đốc, Phó Giám đốc Sở(đc Quang);
- Lưu: VT, BCVTCNTT.

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HOÀ XH CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH HƯNG YÊN

Đỗ Đình Quang

PHƯƠNG ÁN ĐẢM BẢO AN TOÀN THÔNG TIN CỦA SỞ KH&CN

(Kèm theo Quyết định số: /QĐ-STTTT ngày /11/2022 của Sở Thông tin và Truyền thông về việc phê duyệt cấp độ và phương án an toàn hệ thống thông tin đối với Hệ thống Sàn giao dịch công nghệ tỉnh Hưng Yên)

PHỤ LỤC I. Thuyết minh phương án bảo đảm an toàn hệ thống thông tin

1. Thiết lập chính sách an toàn thông tin

1.1. Chính sách an toàn thông tin

Yêu cầu	Quản lý an toàn mạng
Hiện trạng	Đáp ứng
Phương án	Sàn GDCN HY đã đáp ứng các nguyên tắc sau: 1. Mục tiêu: Bảo vệ thông tin, hệ thống thông tin trên môi trường mạng tránh bị xâm 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. Nguyên tắc bảo đảm an toàn thông tin: a) 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. b) Tổ chức, cá nhân không được xâm phạm an toàn thông tin mạng của tổ chức, cá nhân khác. c) 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. d) Truy cập và quản lý cấu hình hệ thống phải được bảo mật và quản lý chặt chẽ đảm bảo an toàn thông tin mạng. e)Thường xuyên nâng cấp đảm bảo cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống (cứng hóa) để vận hành, khai thác. f) Hoạt động an toàn thông tin mạng phải được thực hiện

	thường xuyên, liên tục, kịp thời và hiệu quả đảm bảo mức độ an toàn 6.1.5.1 theo TCVN 11930:2017. 3. Yêu cầu kỹ thuật đảm bảo an toàn mạng a) Hệ thống mạng phải được thiết kế thống nhất, cùng kết hợp và hỗ trợ, tương tác hoạt động với nhau, được tổ chức quản lý định danh, xác thực đối với tất cả người sử dụng nhằm mục đích quản lý hệ thống chặt chẽ, bảo đảm an toàn và bảo mật. b) Hệ thống mạng phải được thiết lập cấu hình để: Kiểm soát truy cập từ bên ngoài mạng; Kiểm soát truy cập từ bên trong mạng; Kết nối về hệ thống giám sát tập trung; Phòng chống xâm nhập giữa các vùng mạng; Phòng chống phần mềm độc hại trên môi trường mạng. c) Các thiết bị mạng phải được cấu hình chức năng xác thực; Chỉ cho phép sử dụng các kết nối mạng an toàn (nếu hỗ trợ) khi truy cập, quản trị thiết bị từ xa; Giới hạn các địa chỉ mạng có thể kết nối, quản trị thiết bị từ xa; Hạn chế được số lần đăng nhập sai; Phân quyền truy cập, quản trị; Nâng cấp, xử lý điểm yếu an toàn thông tin của thiết bị hệ thống trước khi đưa vào sử dụng. d) Hệ thống mạng phải được trang bị hệ thống kỹ thuật, công nghệ hiện đại để thường xuyên, liên tục quản lý, giám sát, kiểm soát mạng nhằm phát hiện, ngăn chặn các truy cập trái phép của người sử dụng, tin tặc tấn công; triển khai cơ chế phòng chống vi rút tin học, thư rác cho những hệ thống xung yếu (máy chủ thư điện tử, máy chủ website, máy chủ tên miền, v.v...) và tại các máy chủ, máy trạm khác trong hệ thống. e) Việc thanh lý, tiêu hủy thiết bị, vật mang thông tin trong mạng Bộ phải đảm bảo yêu cầu không để lộ, lọt thông tin Nhà nước. Phải có quy trình cụ thể và phải lưu giữ hồ sơ, biên bản việc thanh lý, tiêu hủy. f) Các yêu cầu đối với phòng máy chủ:

	- Phòng máy chủ của các cơ quan là khu vực hạn chế tiếp cận và được lắp đặt hệ thống camera giám sát. Chỉ những người có trách nhiệm theo quy định của Thủ trưởng cơ quan mới được phép vào phòng máy chủ. - Phòng máy chủ phải có hệ thống lưu điện đủ công suất và duy trì thời gian hoạt động của các máy chủ tối thiểu 15 phút khi có sự cố mất điện. - Bố trí cán bộ có năng lực chuyên môn cao để quản lý, vận hành phòng máy chủ và duy trì chế độ trực để đảm bảo an toàn thông tin mạng. g) Đối với các thiết bị mạng chính - Phải lắp đặt thiết bị chống sét để bảo vệ hệ thống CNTT, phải xây dựng ít nhất 02 thiết bị chống sét: một cho một đường cung cấp điện và một đường của mạng nội bộ (LAN). - Thiết bị chuyển mạch (switch): Thiết bị chuyển mạch mạng tin học của các cơ quan phải đảm bảo khả năng cung cấp các chức năng quản trị nhằm tăng cường độ an toàn và bảo mật cho hệ thống mạng như: cung cấp khả năng từ chối các kết nối không mong muốn vào hệ thống trên từng cổng, quy định địa chỉ IP cho từng cổng và khống chế số lượng kết nối vào hệ thống mạng nội bộ thông qua thiết bị chuyển mạch. Phải có ít nhất 01 thiết bị chuyển mạch có hỗ trợ định tuyến IP (IP routing) cho mỗi mạng nội bộ, hỗ trợ chức năng điều khiển truy cập (Access Control List), hỗ trợ chức năng xác thực thiết bị và người sử dụng (User & Device Authentication) và chức năng bảo mật quản trị mạng (Network Administration Security). - Tường lửa (firewall): Các cơ quan phải xây dựng tường lửa đảm bảo các yêu cầu gồm khả năng xử lý được số lượng kết nối đồng thời cao, hỗ trợ các công nghệ mạng riêng, ảo, thông dụng và có phần cứng mã hóa tích hợp để tăng tốc độ mã hóa dữ liệu, cung cấp đầy đủ các cơ chế bảo mật cơ bản như NAT,

	PAT, quản lý luồng dữ liệu vào, ra và có khả năng bảo vệ hệ thống trước các loại tấn công từ chối dịch vụ (DDoS). h) Tệp tin cấu hình, sơ đồ mạng logic và vật lý phải được cập nhật, sao lưu dự phòng. i) Có biện pháp bảo vệ, dự phòng, phòng chống các nguy cơ do mất cắp, cháy nổ, ngập lụt, động đất và các thảm họa khác do thiên nhiên hoặc con người gây ra và các phương án khôi phục hệ thống sau thảm họa.
Yêu cầu	Quản lý an toàn máy chủ và ứng dụng
Hiện trạng	Đáp ứng
Phương án	Sàn GDCN HY được giao cho Trung tâm Thông tin, Thống kê, Ứng dụng KHCNquản lý, khai thác chịu sự quản lý của Sở Khoa học và Công nghệ, trong đó đã quy định trách nhiệm của Sở KH&CN trên địa bàn tỉnh trong công tác bảo đảm an toàn thông tin: 1. UBND tỉnh có trách nhiệm thực hiện các nhiệm vụ của chủ quản hệ thống thông tin đối với các hệ thống thông tin trên địa bàn theo quy định tại Điều 20, Nghị định 85, trong đó có Sàn Giao dịch công nghệ Hưng Yên. 2. Trách nhiệm của Sở KH&CN quản lý, giao Trung tâm TTTKƯDKHCN thực hiện: a) Sở Khoa học và Công nghệ thực hiện trách nhiệm của đơn vị vận hành đối với các hệ thống máy chủ và các dịch vụ, đảm bảo an toàn thông tin thuộc phạm vụ quản lý. b) Giao Trung tâm TTTKƯDKHCN quyền quản trị, truy cập mạng của máy chủ theo quyền admin và chịu trách nhiệm đảm bảo an toàn thông tin mạng cũng như nội dung đăng tải thông tin theo quy định. Thường xuyên cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố; Cài đặt, gỡ bỏ hệ điều hành, dịch vụ, phần mềm trên hệ thống khi cần thiết; Kết nối và gỡ bỏ hệ thống máy chủ và dịch vụ khỏi hệ thống; Hàng năm rà

	soát, đề xuất nâng cấp cấu hình tối ưu và tăng cường bảo mật cho hệ thống máy chủ để vận hành, khai thác hiệu quả đảm bảo yêu cầu an toàn tương ứng 6.1.5.2 trong TCVN 11930:2017 c) Tổng hợp báo cáo về tình hình an toàn thông tin mạng theo định kỳ gửi Sở Thông tin và Truyền thông, UBND tỉnh theo quy định của pháp luật. d) Cử cán bộ tham gia chương trình đào tạo, tập huấn về công tác bảo đảm an toàn thông tin mạng cho cán bộ, công chức phụ trách an toàn thông tin mạng của đơn vị. e) Tổ chức tuyên truyền, hướng dẫn về công tác bảo đảm an toàn thông tin mạng. 3. Trách nhiệm của các cơ quan, đơn vị thuộc Sở a) Phụ trách các phòng, đơn vị và các công chức Sở KH&CN có trách nhiệm tổ chức thực hiện các quy định tại Quy chế này và chịu trách nhiệm trong công tác bảo đảm an toàn thông tin mạng của cơ quan, đơn vị mình. b) Thực hiện trách nhiệm của đơn vị vận hành theo quy định tại Điều 22, Nghị định 85. c) Phân công một bộ phận cán bộ phụ trách bảo đảm an toàn thông tin mạng của đơn vị, tạo điều kiện để các cán bộ được học tập, nâng cao trình độ về an toàn thông tin mạng. d) Bố trí, tạo điều kiện làm việc cho cán bộ phụ trách về công nghệ thông tin trong các cơ quan, đơn vị phù hợp với chuyên môn, được ưu tiên bồi dưỡng nghiệp vụ về an toàn thông tin mạng. đ) Xây dựng quy chế, quy trình về bảo đảm an toàn thông tin mạng phù hợp với Quy chế này và các quy định của pháp luật. e) Phối hợp, cung cấp thông tin và tạo điều kiện cho các đơn vị có thẩm quyền triển khai công tác kiểm tra khắc phục sự số xảy ra một cách kịp thời, nhanh chóng và đạt hiệu quả.

	g) Phối hợp chặt chẽ với Sở Thông tin và Truyền thông, Công an tỉnh trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn thông tin mạng. h) Khuyến khích các cơ quan, đơn vị liên kết các tổ chức, cá nhân, doanh nghiệp CNTT mở các khóa đào tạo nhân lực trong lĩnh vực an toàn thông tin mạng. i) Hàng năm bố trí kinh phí cho việc ứng dụng công nghệ thông tin nói chung và công tác bảo đảm an toàn thông tin mạng nói riêng trong nội bộ cơ quan, đơn vị mình; lập kế hoạch nâng cấp, bảo trì, sửa chữa, gia hạn bản quyền Sàn GDCN HY, … hỗ trợ hệ thống phần cứng, các phần mềm liên quan nhằm thực hiện tốt công tác bảo mật, bảo đảm an toàn thông tin mạng đưa vào dự toán chi năm sau để triển khai thực hiện. 4. Trách nhiệm của cán bộ, công chức, viên chức và người lao động trong đơn vị a) Trách nhiệm của bộ phận phụ trách về an toàn thông tin: - Chịu trách nhiệm bảo đảm an toàn thông tin mạng của đơn vị; - Tham mưu lãnh đạo cơ quan ban hành các quy chế, quy trình nội bộ, triển khai các giải pháp kỹ thuật bảo đảm an toàn thông tin mạng; - Thực hiện việc giám sát, đánh giá, báo cáo Thủ trưởng cơ quan, đơn vị các rủi ro mất an toàn thông tin mạng và mức độ nghiêm trọng của các rủi ro đó; - Phối hợp với các cá nhân, đơn vị có liên quan trong việc kiểm soát, phát hiện và khắc phục các sự cố an toàn thông tin mạng; - Thường xuyên cập nhật nâng cao kiến thức, trình độ chuyên môn đáp ứng yêu cầu bảo đảm an toàn thông tin mạng của đơn vị. b) Trách nhiệm của người sử dụng: - Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các

	quy định khác của pháp luật về an toàn thông tin mạng. Chịu trách nhiệm bảo đảm an toàn thông tin mạng trong phạm vi trách nhiệm và quyền hạn được giao; - Có trách nhiệm tự quản lý, bảo trì thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng; - Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo ngay với cấp trên và bộ phận phụ trách công nghệ thông tin của cơ quan, đơn vị để kịp thời ngăn chặn và xử lý; - Tham gia các chương trình đào tạo, hội nghị về an toàn thông tin mạng được tỉnh hoặc đơn vị chuyên môn tổ chức. 5. Trách nhiệm của các tổ chức, cá nhân liên quan - Các tổ chức, cá nhân, doanh nghiệp khi tham gia thực hiện chào bán, giới thiệu sản phẩm, công nghệ trên Sàn và giao dịch cần tuân thủ nghiêm ngặt các quy định của Sàn đảm bảo việc đăng kí, đăng tải và các thông tin liên quan đảm bảo đúng nguyên tắc bảo mật thông tin theo quy định. - Các tổ chức, cá nhân liên quan tham gia Sàn với tư cách người tiêu dùng, tra cứu thông tin, mua bán, giao dịch các sản phẩm, công nghệ được chào bán cần thực hiện theo đúng quy định của Sàn và phải đảm bảo an toàn thông tin theo quy định. 6. Đảm bảo yêu cầu kỹ thuật a) Quy định với máy chủ - Hệ thống máy chủ phải có tính năng sẵn sàng cao, cơ chế dự phòng linh hoạt để đảm bảo hoạt động liên tục. - Có biện pháp bảo vệ, dự phòng, phòng chống các nguy cơ do mất cắp, cháy nổ, ngập lụt, động đất và các thảm họa khác do thiên nhiên hoặc con người gây ra và các phương án khôi phục sau thảm họa cho hệ thống máy chủ. - Máy chủ phải được thiết lập chính sách xác thực; Kiểm soát truy cập; Kết nối về hệ thống giám sát tập trung; Thực hiện

	biện pháp phòng chống xâm nhập; Phòng chống phần mềm độc hại và xử lý dữ liệu trên máy chủ khi chuyển giao. - Máy chủ phải được nâng cấp, xử lý điểm yếu an toàn thông tin trên máy chủ trước khi đưa vào sử dụng. - Việc kết nối, gỡ bỏ máy chủ khỏi hệ thống phải được sự cho phép của Thủ trưởng đơn vị và thực hiện theo quy trình đã được phê duyệt. - Phần mềm hệ điều hành cài lên máy chủ ưu tiên là phần mềm hệ điều hành có bản quyền hoặc là phần mềm mã nguồn mở được sử dụng rộng rãi trong nước và quốc tế. - Có tài liệu liệt kê, cài đặt với những phần mềm hệ thống cài trong máy chủ. b) Đối với ứng dụng: - Các yêu cầu, thiết kế về an toàn bảo mật của phần mềm ứng dụng cần được xác định rõ trong tài liệu phân tích, thiết kế. Trong quá trình triển khai, vận hành các phần mềm ứng dụng cần đảm bảo nghiêm ngặt theo các yêu cầu, thiết kế về an toàn bảo mật. - Ứng dụng phải được thiết lập chính sách xác thực; Kiểm soát truy cập; Kết nối về hệ thống giám sát tập trung; Có phương án bảo mật thông tin liên lạc, chống chối bỏ và biện pháp bảo đảm an toàn ứng dụng và mã nguồn. - Có phương án xác định và khắc phục rủi ro trước, trong quá trình triển khai và khi vận hành các phần mềm ứng dụng. - Ứng dụng phải kiểm tra, thử nghiệm và có biên bản đánh giá tính an toàn, bảo mật đối với phần mềm ứng dụng theo yêu cầu khi nghiệm thu các phần mềm này. Việc tiến hành thử nghiệm phải đảm bảo trên môitrường riêng biệt, không ảnh hưởng tới hoạt động và dữ liệu của đơn vị. c)Đối với ứng dụng thư điện tử

	- Không sử dụng các hộp thư điện tử công cộng. Không sử dụng thư điện tử chính thức của đơn vị vào mục đích cá nhân. - Mỗi cá nhân cần đặt mật khẩu đủ mạnh cho hộp thư điện tử của mình. - Đơn vị quản lý hệ thống thư điện tử cần có quy định về việc khóa và xóa bỏ hộp thư điện tử cá nhân khi cá nhân đó không còn làm việc tại đơn vị. - Đơn vị quản lý hệ thống thư điện tử cần xây dựng phương án đảm bảo an toàn và tính khả dụng truy cập cho hệ thống thư điện tử trong nội bộ và trên Internet, phương án chống thư rác cho thư điện tử. - Bảo đảm an toàn cho hệ thống thư điện tử: Thực hiện theo hướng dẫn tại công văn số 430/BTTTT-CATTT ngày 09 tháng 2 năm 2015 của Bộ TT&TT về việc hướng dẫn đảm bảo an toàn thông tin cho hệ thống thư điện tử của cơ quan, tổ chức nhà nước. d)Đối với trang Web Sàn - Quản lý toàn bộ các phiên bản của mã nguồn, phối hợp với đơn vị thực hiện dịch vụ hosting tổ chức mô hình trang web hợp lý, tránh khả năng tấn công leo thang đặc quyền. Yêu cầu đơn vị cung cấp dịch vụ hosting phải cài đặt các hệ thống phòng vệ như tường lửa thiết bị phát hiện/phòng chống xâm nhập (IDS/IPS) ở mức ứng dụng web (WAF- Web Application Firewall). - Khi Sàn đưa vào sử dụng hoặc khi bổ sung thêm các chức năng, mới cần đánh giá kiểm định nhằm tránh được các lỗi bảo mật thường xảy ra trên ứng dụng web như: SQL Injection, Cross-Site Scripting (xss), … - Phối hợp với các nhà cung cấp dịch vụ hosting xây dựng phương án phục hồi trang web, trong đó chú ý mỗi tháng thực hiện việc backup toàn bộ nội dung trang web một lần bao gồm

	mã nguồn, cơ sở dữ liệu, dữ liệu phi cấu trúc, ... để bảo đảm khi có sự cố có thể khắc phục lại ngay trong vòng 24 giờ. - Bảo đảm an toàn cho Sàn giao dịch công nghệ Hưng Yên theo hướng dẫn tại công văn số 2132/BTTTT-VNCERT ngày 18 tháng 7 năm 2011 củaBộ TT&TT về việc hướng dẫn đảm bảo an toàn thông tin cho các Cổng/Trang thông tin điện tử.
Yêu cầu	Quản lý an toàn dữ liệu
Hiện trạng	Đáp ứng
Phương án	1. Sở Khoa học và Công nghệ chịu trách nhiệm chính về quản lý, vận hành của Sàn dựa trên quy chế đã được xây dựng để đảm bảo việc bảo mật an ninh mạng theo quy định, đồng thời giao Trung tâm TTTKƯDKHCN truy cập, quản trị hệ thống máy chủ và dịch vụ theo quy trình thực hiện quản lý an toàn dữ liệu. 2. Trung tâm TTTKƯDKHCN chị trách nhiệm truy cập, quản trị hệ thống máy chủ và dịch vụ theo quy trình thực hiện quản lý an toàn dữ liệu bao gồm: a) Yêu cầu an toàn đối với phương pháp mã hóa: Các sản phẩm được đăng tải giới thiệu, chào bán phải được mã hóa theo đúng quy định và phải đảm bảo an toàn thông tin, được admin xem xét mức độ an toan và duyệt trước khi đăng tải lên Sàn. b) Các sản phẩm khi đăng kí và trước khi đăng tải chào bán, giới thiệu phải được hệ thống nhân viên kỹ thuật, chuyên môn phân loại, quản lý và sử dụng khóa bí mật và dữ liệu mã hóa nhằm đảm bảo an toàn thông tin rồi mới xem xét, duyệt trước khi đăng tải. c) Hệ thống kỹ thuật viên phải thực hiện cơ chế mã hóa và kiểm tra tính nguyên vẹn của dữ liệu trước khi đăng tải. d)Các dữ liệu, thông tin phảo được xem xét và kiểm soát mã độc trước khi đăng tải để trao đổi dữ liệu qua môi trường mạng và phương tiện lưu trữ.

	e) Kỹ thuật viên phải tiến hành thường xuyên Định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ. Lưu trữ có mã hóa các thông tin, dữ liệu (không phải là thông tin, dữ liệu công khai) trên hệ thống lưu trữ/phương tiện lưu trữ f) Cập nhật đồng bộ thông tin, dữ liệu giữa hệ thống sao lưu dự phòng chính và hệ thống phụ. g) Hệ thống dữ liệu phải được quản lý đảm bảo yêu cầu an toàn tương ứng 6.1.5.3 trong TCVN 11930:2017.
Yêu cầu	Quản lý an toàn thiết bị đầu cuối
Hiện trạng	Đáp ứng
Phương án	* Các thiết bị đầu cuối khi kết nối vào hệ thống phải được quản lý như sau: 1. Thông tin về thiết bị đầu cuối (tên, chủng loại, địa chỉ MAC, địa chỉ IP) phải được quản lý và cập nhật. 2. Các thiết bị đầu cuối phải được quản lý khi kết nối vào hệ thống mạng theo địa chỉ MAC, IP. 3. Khi truy cập và sử dụng thiết bị đầu cuối từ xa phải có cơ chế xác thực và sử dụng giao thức mạng an toàn. 4. Việc cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống phải được cho phép bởi người có thẩm quyền và thực hiện theo quy trình được phê duyệt. * Sở Khoa học thực hiện các nhiệm vụ chính sau: 1) Sở Khoa học và Công nghệ quy định về nội dung, chính sách và quy trình thực hiện quản lý thiết bị, người dùng đầu cuối, đảm bảo yêu cầu an toàn tương ứng 6.1.5.5 trong TCVN 11930:2017. Giao Trung tâm TTTKƯDKHCN truy cập, quản trị hệ thống máy chủ và dịch vụ theo quy trình thực hiện quản lý an toàn thiết bị đầu cuối.

	2. Trung tâm TTTKƯDKHCN chị trách nhiệm truy cập, quản trị hệ thống máy chủ và dịch vụ theo quy trình thực hiện quản lý an toàn thiết bị đầu cuối bao gồm: a) Quản lý vận hành hoạt động bình thường cho thiết bị đầu cuối đảm bảo các thông tin được đăng tải, bảo mật, an toàn cho cả hệ thống thông tin và cho người sử dụng. b) Quản trị, đảm bảo thường xuyên kết nối, truy cập và sử dụng thiết bị đầu cuối từ xa an toàn. c) Phải tiến hành cài đặt, kết nối hoặc gỡ bỏ thiết bị đầu cuối trong hệ thống khi cần thiết. d) Hàng năm rà soát, đề xuất với Sở Khoa học và Công nghệ nâng cấp cấu hình tối ưu và tăng cường bảo mật cho máy tính người sử dụng e) Các thiết bị đầu cuối khi kết nối và hệ thống phải được quản lý như sau:Thông tin về thiết bị đầu cuối (tên, chủng loại, địa chỉ MAC, địa chỉ IP) phải được quản lý và cập nhật; Các thiết bị đầu cuối phải được quản lý khi kết nối vào hệ thống mạng theo địa chỉ MAC, IP; Khi truy cập và sử dụng thiết bị đầu cuối từ xa phải có cơ chế xác thực và sử dụng giao thức mạng an toàn.Việc cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống phải được cho phép bởi người có thẩm quyền và thực hiện theo quy trình được phê duyệt. f) Thường xuyên kiểm tra, đánh giá, xử lý điểm yếu an toàn thông tin cho thiết bị đầu cuối, xử lý kịp thời khi có sự cố và báo cáo Sở khi cần thiết.

1.2. Xây dựng và công bố

Yêu cầu	Chính sách được tổ chức/ bộ phận được ủy quyền thông qua trước khi công bố áp dụng.
Hiện trạng	Đáp ứng
Phương án	1. Sở Khoa học và Công nghệ tiến hành xây dựng dự thảo Quy chế bảo đảm an toàn thông tin cho Sàn giao dịch công nghệ

	Hưng Yên theo Nghị định số 85/2016/NĐ-CP ngày 01 tháng 07 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ. 2. Quy chế được lấy ý kiến tại các phòng, đơn vụ trực thuộc Sở trước khi xin ý kiến cấp có thẩm quyền, các đơn vị liên quan. Tiến hành tổng hợp, hoàn thiện trước khi công bố áp dụng. 3. Quy chế được Sở KH&CN tỉnh Hưng Yên ban hành.

1.3. Rà soát, sửa đổi

Yêu cầu	Có quy định về việc rà soát, sửa đổi Quy chế bảo đảm an toàn thông tin
Hiện trạng	Đáp ứng
Phương án	Tiến hành rà soát, sửa đổi Quy chế bảo đảm an toàn thông tin: 1. Định kỳ 03 năm hoặc khi có thay đổi Quy chế bảo đảm an toàn thông tin, kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung. 2. Trong quá trình thực hiện Quy chế nếu có vướng mắc, phát sinh, các đơn vị phản ánh kịp thời về Sở Khoa học và Công nghệ để tổng hợp báo cáo Thông tin và Truyền thông trình UBND tỉnh để điều chỉnh, bổ sung.

2. Tổ chức bảo đảm an toàn thông tin

2.1. Đơn vị chuyên trách về an toàn thông tin

Yêu cầu	Sở Khoa học và Công nghệ giao Trung tâm Thông tin, Thống kê, Ứng dụng KHCN quản lí, vận hành và chịu trách nhiệm về an toàn thông tin của Sàn GDCN HY
Hiện trạng	Đáp ứng
Phương án	1) Bộ phận Hành chính Tổng hợp của Trung tâm phân công viên chức, cán bộ kiêm nhiệm phụ trách về CNTT dự thảo Quyết định báo cáo Giám đốc Trung tâm trình Giám Đốc Sở KH&CN giao nhiệm vụ là bộ phận phụ trách về An toàn thông tin đối với Sàn GDCN HY. 2) Trung tâm sau khi được Sở giao nhiệm vụ chịu trách nhiệm

	về an toàn thông tin của Sàn tiến hành xây dựng các phương án thực hiện theo Quy chế an toàn thông tin mạng theo cấp độ đã được Sở ban hành để quản lý, quản trị và phát triển Sàn đảm bảo an toàn thông tin theo quy định.

2.2. Phối hợp với những cơ quan/tổ chức có thẩm quyền

Yêu cầu	Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin
Hiện trạng	Đáp ứng
Phương án	1. Sở Khoa học và Công nghệ giao Phòng Quản lý chuyên ngành chịu trách nhiệm đầu mối về quản lý thông tin, thống kê khoa học công nghệ của Sở. Chủ trì, phối hợp với Trung tâm Thông tin, Thống kê, Ứng dụng KH&CN trong xây dựng và thực hiện an toàn thông tin mạng. Chịu trách nhiệm quản lý, báo cáo về lĩnh vực quản lý thông tin, thống kê và công nghệ thông tin đảm bảo an toàn mạng trước Giám đốc Sở, thường xuyên nắm bắt và báo cáo kịp thời về khả năng phát triển thông tin, phát triển Sàn giao dịch công nghệ Hưng Yên về đảm bảo an toàn thông tin mạng. 2. Sở Khoa học và Công nghệ giao Trung tâm Thông tin, Thống kê, Ứng dụng KH&CN quản lý, quản trị, truy cập máy chủ và là đầu mối trong việc phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý an toàn thông tin, báo cáo và chịu trách nhiệm trước Giám đốc Sở về an toàn thông tin mạng của Sàn.
Yêu cầu	Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin
Hiện trạng	Đáp ứng
Phương án	1. Sở Khoa học và Công nghệ giao Phòng Quản lý chuyên ngành chịu trách nhiệm đầu mối về quản lý thông tin, thống kê khoa học công nghệ của Sở. Chủ trì, phối hợp với Trung tâm Thông tin, Thống kê, Ứng dụng KH&CN trong xây dựng và tham mưu hỗ trợ điều phối xử lý sự cố an toàn thông tin. Chịu trách nhiệm quản lý, báo cáo về lĩnh vực quản lý thông tin,

	thống kê và công nghệ thông tin đảm bảo an toàn mạng trước Giám đốc Sở, thường xuyên nắm bắt và báo cáo kịp thời về khả năng phát triển thông tin, phát triển Sàn giao dịch công nghệ Hưng Yên về hỗ trợ điều phối xử lý sự cố an toàn thông tin nhằm đảm bảo an toàn thông tin mạng của Sàn theo quy định. 2. Sở Khoa học và Công nghệ giao Trung tâm Thông tin, Thống kê, Ứng dụng KH&CN quản lý, quản trị, truy cập máy chủ và là đầu mối, chủ động trong việc liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin; báo cáo và chịu trách nhiệm trước Giám đốc Sở về việc xử lý sự cố an toàn thông tin của Sàn đảm bảo yêu cầu tương ứng 6.1.2 trong TCVN 11930:2017.
Yêu cầu	Tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của tổ chức có thẩm quyền.
Hiện trạng	Đáp ứng
Phương án	1. Sở Khoa học và Công nghệ giao Phòng Quản lý chuyên ngành chịu trách nhiệm đầu mối về quản lý thông tin, thống kê khoa học công nghệ của Sở. Chủ trì, phối hợp với Trung tâm Thông tin, Thống kê, Ứng dụng KH&CN trong xây dựng và tham mưu hỗ trợ điều phối xử lý sự cố an toàn thông tin. Chịu trách nhiệm quản lý, báo cáo về lĩnh vực quản lý thông tin, thống kê và công nghệ thông tin đảm bảo an toàn mạng trước Giám đốc Sở, thường xuyên nắm bắt và báo cáo kịp thời về khả năng phát triển thông tin, phát triển Sàn giao dịch công nghệ Hưng Yên về hỗ trợ điều phối xử lý sự cố an toàn thông tin nhằm đảm bảo an toàn thông tin mạng của Sàn theo quy định. 2. Sở Khoa học và Công nghệ giao Trung tâm Thông tin, Thống kê, Ứng dụng KH&CN quản lý, quản trị, truy cập máy chủ và là đầu mối, chủ động trong việc liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin; báo cáo và chịu trách nhiệm trước Giám đốc Sở về việc xử lý sự cố an toàn thông tin của Sàn đảm bảo yêu cầu tương ứng

	6.1.2 trong TCVN 11930:2017.

3. Bảo đảm nguồn nhân lực

3.1. Tuyển dụng

Yêu cầu	Cán bộ được tuyển dụng vào vị trí làm về an toàn thông tin có trình độ, chuyên ngành phù hợp với vị trí tuyển dụng (tối thiểu phải có trình độ chuyên môn về công nghệ thông tin trình độ Đại học trở lên).
Hiện trạng	Tạm thời đáp ứng
Phương án	1. Sở Khoa học và Công nghệ đã tiến hành tuyển dụng theo vị trí việc làm với 01 công chức cử nhân công nghệ thông tin làm việc tại văn phòng Sở, tuy nhiên từ tháng 8/2021 đã luân chuyển sang phòng Hành chính tổng hợp của Chi cục Tiêu chuẩn, Đo lường, Chất lượng (trực thuộc Sở). Sở đã xây dựng vị trí việc làm của Sở và của Trung tâm Thông tin, Thống kê, Ứng dụng KH&CN đảm bảo tuyển dụng công chức, viên chức có trình độ công nghệ thông tin. Sở Khoa học và Công nghệ giao Trung tâm Thông tin, Thống kê, Ứng dụng KH&CN xây dựng vị trí việc làm và đề nghị Sở tuyển dụng ít nhất 01 viên chức có trình độ đại học chuyên ngành công nghệ thông tin vào làm việc tại Trung tâm. 2. Trung tâm Thông tin, Thống kê, Ứng dụng KH&CN a) Xây dựng vị trí việc làm và đề nghị Sở tuyển dụng ít nhất 01 viên chức có trình độ đại học chuyên ngành công nghệ thông tin vào làm việc tại Trung tâm (năm 2022 dự kiến tuyển dụng thêm 05 viê chức). b) Tiến hành tuyển dụng 01 viên chức có trình độ đại học chuyên ngành công nghệ thông tin để thực hiện vị trí việc làm về quản trị mạng, quản trị Sàn Giao dịch công nghệ và đảm bảo an toàn thông tin. Thường xuyên cử đi đào tạo và bồi dưỡng các kiến thức về an toàn, an ninh mạng. c) Viên chức thực hiện nhiệm vụ quản trị mạng và an toàn thông tin được đảm bảo các quyền và nghĩa vụ theo đúc Luật Viên chức và thực hiện đánh giá thực hiện công việc theo quý trước Trung tâm. Nếu trong quá trình làm việc xảy ra nhiều sự cố nghiêm trọng hoặc hạn chế về chuyên môn, ý thức kỷ luật, chịu trách nhiệm kém sẽ được thay đổi công việc sang vị trí khác

	hoặc không hoàn thành nhiệm vụ 03 năm liên tiếp thì buộc thôi việc theo đúng Luật Viên chức. d) Viên chức chịu trách nhiệm quản trị mạng và an toàn thông tin của Sàn đảm bảo yêu cầu tương ứng 6.1.3 trong TCVN 11930:2017.

3.2. Trong quá trình làm việc

Yêu cầu	Có quy định về việc thực hiện bảo đảm an toàn thông tin cho người sử dụng, cán bộ quản lý và vận hành hệ thống
Hiện trạng	Tạm thời đáp ứng
Phương án	1. Sở Khoa học và Công nghệ có trách nhiệm quản lý chung về viên chức thực hiện quản lý, vận hành hệ thống; giao Trung tâm Thông tin, Thống kê, Ứng dụng KH&CN quản lý trực tiếp và thực hiện bảo đảm an toàn thông tin cho người sử dụng, cán bộ quản lý và vận hành hệ thống. 2. Trung tâm Thông tin, Thống kê, Ứng dụng KH&CN có trách nhiệm bảo đảm an toàn thông tin cho người sử dụng, cán bộ quản lý và vận hành hệ thống a) Với người sử dụng: - Người sử dụng có trách nhiệm bảo đảm ATTT đối với từng vị trí công việc. Trước khi tham gia vào hệ thống phải được kiểm tra khả năng đáp ứng các yêu cầu về ATTT. - Phải được thường xuyên tổ chức quán triệt các quy định về ATTT, nhằm nâng cao nhận thức về trách nhiệm bảo đảm ATTT. b) Với cán bộ quản lý và vận hành hệ thống - Cán bộ chuyên trách phải thiết lập phương pháp hạn chế truy cập mạng không dây, giám sát và điều khiển truy cập không dây, tổ chức sử dụng chứng thực và mã hóa để bảo vệ truy cập không dây tới hệ thống thông tin. - Cán bộ chuyên trách phải tổ chức quản lý định danh đối với tất cả người dùng tham gia sử dụng hệ thống thông tin.

	2. Định kỳ hàng năm người sử dụng được tổ chức phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin theo chương trình, nội dung tại Quyết định số 893/QĐ-TTg ngày 19/6/2015 về việc phê duyệt Đề án Tuyên truyền, phổ biến, nâng cao nhận thức và trách nhiệm về an toàn thông tin đến năm 2020. 3. Định kỳ hàng năm người sử dụng được tổ chức đào tạo các kỹ năng cơ bản về an toàn thông tin theo chương trình, nội dung tại: Quyết định số 99/QĐ-TTg ngày 14/01/2014 phê duyệt Đề án Đào tạo và phát triển nguồn nhân lực an toàn, an ninh thông tin đến năm 2020.
Yêu cầu	Có kế hoạch và định kỳ hàng năm tổ chức phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin cho người sử dụng.
Hiện trạng	Tạm thời đáp ứng
Phương án	1. Sở Khoa học và Công nghệ có trách nhiệm xây dựng kế hoạch đào tạo bồi dưỡng chuyên môn nghiệp vụ chung cho toàn Sở trong đó có mảng về thông tin và quản lý, vận hành hệ thống; giao Trung tâm Thông tin, Thống kê, Ứng dụng KH&CN quản lý trực tiếp xây dựng kế hoạch và định kỳ hàng năm tổ chức phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin cho người sử dụng. 2. Trung tâm Thông tin, Thống kê, Ứng dụng KH&CN có trách nhiệm xây dựng kế hoạch và định kỳ hàng năm người sử dụng được tổ chức phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin theo chương trình, nội dung tại Quyết định số 893/QĐ-TTg ngày 19/6/2015 về việc phê duyệt Đề án Tuyên truyền, phổ biến, nâng cao nhận thức và trách nhiệm về an toàn thông tin đến năm 2020.cơ bản về an toàn thông tin theo chương trình, nội dung tại - Quyết định số 99/QĐ-TTg ngày 14/01/2014 phê duyệt Đề án Đào tạo và phát triển nguồn nhân lực an toàn, an ninh thông tin đến năm 2020.

3.3. Chấm dứt hoặc thay đổi công việc

Yêu cầu	Nếu cán bộ được giao phụ trách quản lý, vận hành Sàn mà chấm dứt hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác (nếu có) thuộc sở hữu của tổ chức.
Hiện trạng	Đáp ứng
Phương án	1. Sở Khoa học và Công nghệ sau khi tiến hành luân chuyển cán bộ phụ trách công nghệ thông tin của Sở đã thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm. Giao toàn bộ quyền truy cập và các thong tin liên quan cho Trung tâm Thông tin, Thống kê, Ứng dụng KH&CN. 2. Trung tâm Thông tin, Thống kê, Ứng dụng KH&CN đã giao nhiệm vụ chuyên trách cho 01 viên chức thực hiện đảm bảo các nguyên tắc và đảm bảo an toàn mạng của Sàn theo quy định. Kế hoạch sau khi tuyển dụng viên chức có trình độ công nghệ thông tin sẽ giao nhiệm vụ phụ trách quản lý, vận hành Sàn đảm bảo an toàn thông tin mạng theo quy định. Trường hợp viên chức được giao nhiệm vụ phụ trách quản lý, vận hành Sàn mà chấm dứt hoặc thay đổi công việc thì Trung tâm sẽ thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác (nếu có) thuộc sở hữu của Trung tâm.
Yêu cầu	Phải có quy trình và thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc.
Hiện trạng	Đáp ứng
Phương án	1. Sở Khoa học và Công nghệ giao Trung tâm Thông tin, Thống kê, Ứng dụng KH&CN xây dựng quy trình và thực hiện quy trình, đồng thời thực hiện vô hiệu hóa tất cả các quyền ra, vào,

	truy cập tài nguyên, quản trị hệ thống sau khi viên chức thôi việc. 2. Trung tâm Thông tin, Thống kê, Ứng dụng KH&CN xây dựng quy trình và thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi viên chức thôi việc báo cáo Sở phê duyệt, cụ thể: a) Viên chức trước khi được thôi việc phải báo cáo Lãnh đạo Trung tâm trước 03 tháng. b) Trung tâm sẽ cử viên chức khác tiếp cận các nội dung công việc của viên chức cũ (bàn giao các nội dung về chuyên môn và quyền truy cập, quản trị) đảm bảo duy trì, vận hành Sàn bình thường, liên tục tránh dán đoạn và tiếp cận công việc quản lý, vận hành Sàn thuận lợi. c) Sau khi viên chức mới được phân công tiếp cận đã thành thạo việc quản lý, truy cập, quản trị Sàn, tiến hành giao chuyên trách nhiệm vụ vận hành Sàn. Đồng thời sao lưu toàn bộ các thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác (nếu có) thuộc sở hữu của Trung tâm từ viên chức cũ để lưu trữ và thực hiện nhiệm vụ vận hành Sàn đảm bảo an toàn mạng. d) Tiến hành vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc

4. Quản lý thiết kế, xây dựng hệ thống thông tin

4.1. Thiết kế an toàn hệ thống thông tin

Yêu cầu	Có quy định về thiết kế an toàn hệ thống thông tin
Hiện trạng	Đáp ứng
Phương án	Quy định đối với tài liệu thiết kế hệ thống cho Sàn GDCN HY thống kê khoa học và công nghệ 1. Có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành Sàn GDCN HY.

<table>
<tr><td></td><td>2. Có tài liệu mô tả thiết kế và các thành phần của Sàn GDCN HY.
3. Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin.
4. khi thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống.</td></tr>
<tr><td>Yêu cầu</td><td>Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin</td></tr>
<tr><td>Hiện trạng</td><td>Đáp ứng</td></tr>
<tr><td>Phương án</td><td>Tiến hành thiết kế các thành phần của hệ thống thông tin như sau
<table>
<tr><th>STT</th><th>Yêu cầu</th><th>P/A</th><th>Ghi chú/ Mô tả</th></tr>
<tr><td>1</td><td>Vùng mạng nội bộ</td><td>Không có</td><td>Vùng mạng nội bộ độc lập, tách riêng khỏi hệ thống của trung tâm dữ liệu</td></tr>
<tr><td>2</td><td>Vùng mạng biên</td><td>Có</td><td>Kết nối hệ thống với mạng Internet v mạng diện rộng</td></tr>
<tr><td>3</td><td>Vùng mạng DMZ</td><td>Có</td><td>Vùng máy chủ dịch vụ. cung cấp dịch vụ trực tiếp ra bên ngoài Internet</td></tr>
<tr><td>4</td><td>Vùng máy chủ nội bộ</td><td>Có</td><td>Vùng máy chủ nội bộ, cung cấp các dịch vụ nội bộ</td></tr>
<tr><td>5</td><td>Vùng mạng máy chủ cơ sở dữ liệu</td><td>Có</td><td>Lưu trữ và quản lý cơ sở dữ liệu tập trung của các hệ thống thành phần</td></tr>
<tr><td>6</td><td>Vùng mạng không dây</td><td>Không có</td><td>Trung tâm dữ liệu không cho phép sử dụng mạng không dây.</td></tr>
<tr><td>7</td><td>Vùng quản trị</td><td>Có</td><td>Chưa thiết kế vùng mạng riêng cho vùng quản trị. Sẽ bổ sung vùng mạng này</td></tr>
</table></td></tr>
<tr><td>Yêu cầu</td><td>Có tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ</td></tr>
<tr><td>Hiện trạng</td><td>Đang hoàn thiện</td></tr>
<tr><td>Phương án</td><td>Thực hiện các phương án sau:
1. Phương án quản lý truy cập, quản trị hệ thống từ xa an toàn bằng việc
sử dụng cấu hình chức năng VPN trên thiết bị tường lửa…
2. Phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập thông qua hệ thống mạng sử dụng thiết bị tường lửa hoặc thiết bị có chức năng tương đương để quản lý truy cập và phòng chống xâm nhập giữa các vùng mạng.
3. Phương án cân bằng tải, dự phòng nóng cho các thiết bị mạng được</td></tr>
</table>

	kết nối với nhau theo cấu hình HA hoặc AA… 4. Phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu bằng sử dụng thiết bị chuyên dụng như tường lửa cơ sở dữ liệu hoặc phần mềm chống mã đọc xâm phạm để bảo đảm an toàn cho máy chủ cơ sở dữ liệu. 5.Phương án phòng chống tấn công từ chối dịch vụ bằng hình thức thuê dịch vụ để phòng chống tấn công từ chối dịch vụ cho hệ thống. 6. Phương án giám sát hệ thống thông tin tập trung bằng việc sử dụng giải pháp chuyên dụng (ArcSight, Splunk, QRadar, LogRhythm) hoặc giải pháp tương đương khác để thực hiện giám sát hệ thống thông tin tập trung 7. Phương án giám sát an toàn hệ thống thông tin tập trung bằng các sử dụng giải pháp chuyên dụng (HP OpenView, Solarwinds…) hoặc giải pháp tương đương khác (Cacti, Nagios, MRTG…) để thực hiện giám sát hoạt động của hệ thống mạng, bảo đảm tínhsẵn sàng của hệ thống. 8. Phương án quản lý sao lưu dự phòng tập trung bằng việc sử dụng giải pháp chuyên dụng hoặc giải pháp tương đương sử dụng các giải pháp như SAN, NAS… 9. Phương án quản lý phần mềm phòng chống mã độc trên các máy chủ/máy tính người dùng tập trung được cài đặt trên các máy tính /máy chủ được sử dụng thông qua một máy chủ quản lý tập trung nhằm phòng, chống thất thoát dữ liệu. 10. Phương án duy trì ít nhất 02 kết nối mạng Internet từ các ISP sử dụng hạ tầng kết nối trong nước khác nhau (nếu hệ thống bộc phải có kết nối mạng Internet); 11. Phương án bảo đảm an toàn cho mạng không dây bằng việc thực hiện giải pháp chuyên dụng hoặc việc thiết lập cấu hình bảo mật trên hệ thống để bảo đảm an toàn cho mạng không dây. 12. Phương án quản lý tài khoản đặc quyền cho phép quản lý tập trung việc xác thực, phân quyền, giám sát hành vi và các chức năng bảo mật

khác để quản lý các tài khoản quản trị trong hệ thống.

13. Phương án dự phòng hệ thống ở vị trí địa lý khác nhau.

14. Phương án dự phòng cho kết nối mạng giữa hệ thống chính và hệ thống dự hòng.

Sử dụng kết nối mạng giữa hệ thống chính và hệ thống dự phòng để thực hiện đồng bộ dữ liệu và dự phòng nóng khi hệ thống chính xảy ra sự cố.

STT	Yêu cầu	P/A	Ghi chú/ mô tả
1	Phương án quản lý truy cập, quản trị hệ thống từ xa an toàn	**Có**	Các thiết bị hệ thống/máy chủ được thiết lập cấu hình cho phép quản trị từ xa an toàn.
2	Phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập	**Có**	Truy cập giữa các vùng mạng đượ quản lý và phòng chống xâm nhập s dụng các thiết bị tường lửa chuyê dùng có tích hợp chức năng phòn chống xâm nhập
3	Phương án cân bằng tải, dự phòng nóng cho các thiết bị mạng	**Có**	Các thiết bị mạng chính được thiết kế và cấu hình hoạt động ở chế độ A-A (Thiết kế chi tiết tại sơ đồ vật lý và logic gửi kèm theo).
4	Phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu	**Có**	Các phương án đảm bảo an toàn đ được phê duyệt
5	Phương án phòng chống tấn công từ chối dịch vụ	**Chưa có**	Sẽ xây dựng phương án và thuê dịc vụ phòng chống tấn công, từ chối dịc vụ
6	Phương án giám sát hệ thống thông tin tập trung	**Có**	Hệ thống giải pháp của HI Solarwind, Nagios…
7	Phương án giám sát an toàn hệ thống thông tin tập trung	**Có**	Hệ thống giải pháp của ArcSigh Splunk,Qradar….
8	Phương án quản lý sao lưu dự phòng tập trung	**Có**	Sử dụng hệ thống SAN của hãng HP
9	Phương án quản lý phần mềm phòng chống mã độc trên các máy chủ/máy tính người dùng tập trung	**Có**	Sử dụng tường lửa, giải pháp chuyê dụng để hạn chế và chống mã độc hại
10	Phương án duy trì ít nhất 02 kết nối mạng Internet từ các ISP sử dụng hạ tầng kết nối trong nước khác nhau	**Có**	Sử dụng 02 đường kết nối Internet củ 02 ISP là Viettel và VNPT

		(nếu hệ thống bộc phải có kết nối mạng Internet)		
	11	Phương án bảo đảm an toàn cho mạng không dây	**Chưa có**	Chưa có phương án. Sẽ xây dựng phương án bổ sung
	12	Phương án quản lý tài khoản đặc quyền	**Chưa có**	Chưa có phương án. Sẽ xây dựng phương án bổ sung
	13	Phương án dự phòng hệ thống ở vị trí địa lý khác nhau	**Chưa có**	Chưa có phương án. Sẽ xây dựng phương án bổ sung
	14	Phương án dự phòng cho kết nối mạng giữa hệ thống chính và hệ thống dự phòng	**Chưa có**	Chưa có phương án. Sẽ xây dựng phương án bổ sung
Yêu cầu	Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin			
Hiện trạng	Đang hoàn thiện			
Phương án	Xây dựng phương án và thực hiện các giải pháp sau: 1. Kiểm soát truy cập từ bên ngoài mạng theo chiều đi vào hệ thống tới các máy chủ dịch vụ bên trong mạng, bao gồm: Các dịch vụ/ứng dụng cho phép từ truy cập từ bên ngoài; Thời gian mất kết nối; Phân quyền truy cập; Giới hạn kết nối; Thiết lập chính sách ưu tiên... đảm bảo yêu cầu an toàn tương ứng 6.2.1.2 trong TCVN 11930:2017. 2. Kiểm soát truy cập từ các máy tính/máy chủ bên trong mạng theo chiều đi ra các mạng bên ngoài và các mạng khác bên trong mạng, bao gồm: Các ứng dụng/dịch vụ nào được truy cập; Quản lý truy cập theo địa chỉ thiết bị; phương án ưu tiên truy cập,… đảm bảo yêu cầu an toàn tương ứng 6.2.1.3 trong TCVN 11930:2017. 3. Phải thực hiện nhật ký hệ thống (log) trên các thiết bị hệ thống về bật chức năng ghi log; thông tin ghi log; thời gian, dung lượng ghi log; quản lý log… đảm bảo yêu cầu an toàn tương ứng 6.2.1.4 trong TCVN 11930:2017. 4. Phòng chống xâm nhập bằng cách thiết lập cấu hình của thiết bị phòng, chống xâm nhập IDS/IPS hoặc chức năng IDS/IPS trên thiết bị tường lửa có trong hệ thống nhằm đáp ứng yêu cầu an toàn,… đảm bảo yêu cầu an toàn tương ứng 6.2.1.5trong TCVN 11930:2017. 5. Phòng chống phần mềm độc hại trên môi trường mạng bằng thiết			

	lập cấu hình của thiết bị để thực hiện chức năng phòng chống phần mềm độc hại trên môi trường mạng đáp ứng yêu cầu an toàn đảm bảo. 6. Bảo vệ thiết bị hệ thống bằng thiết lập cấu hình chức năng bảo mật trên các thiết bị có trong hệ thống nhằm bảo đảm an toàn cho thiết bị trong quá trình sử dụng và quản lý vận hành đảm bảo yêu cầu an toàn tương ứng 6.2.1.6 trong TCVN 11930:2017.
Yêu cầu	Khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống
Hiện trạng	Đáp ứng
Phương án	Căn cứ thực tiễn, khi có thay đổi thiết kế, sẽ tiến hành thành lập tổ tư vấn thuộc Sở và mời các chuyên gia liên quan tiến hành đánh giá lại tính phù hợp của phương án thiết kế đối với yêu cầu an toàn của toàn bộ hệ thống. Trên cơ sở đó tiến hành xây dựng kế hoạch, thiết kế lại hệ thống các modul của Sàn cho phù hợp với thực tiễn nhưng vẫn đảm bảo được tính an toàn thông tin mạng.

4.2. Phát triển Sàn GDCN HY thuê khoán

Yêu cầu	Có quy định về phát triển Sàn GDCN HY và các Sàn GDCN trong và ngoài nước liên quan
Hiện trạng	Đáp ứng
Phương án	Quy định đối với việc phát triển Sàn GDCN HY đối với bên thuê khoán: 1. Có điều khoản hợp đồng và các cam kết đối với bên thuê khoán khi thực hiện các nội dung liên quan đến việc phát triển Sàn GDCN HY thuê khoán. 2. Các nhà phát triển cung cấp mã nguồn Sàn GDCN HY. 3. Sàn GDCN HY thuê khoán phải được kiểm thử Sàn GDCN HY trên môi trường thử nghiệm trước khi đưa vào sử dụng. 4. Sàn GDCN HY thuê khoán phải được kiểm tra, đánh giá an toàn thông tin trước khi đưa vào sử dụng.
Yêu cầu	Yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm
Hiện trạng	Đáp ứng
Phương án	Sở Khoa học và Công nghệ giao Trung tâm Thông tin, Thống kê, Ứng dụng KH&CN chủ động yêu cầu nhà phát triển Sàn

	giao dịch công nghệ tỉnh Hưng Yên thực hiện cung cấp mã nguồn theo quy định, đảm bảo: 1. Có điều khoản hợp đồng và các cam kết đối với nhà phát triển khi thực hiện các nội dung liên quan đến việc phát triển Sàn GDCN HY phải cung cấp mã nguồn của Sàn. 2. Mã nguồn Sàn GDCN HY được Trung tâm Thông tin, Thống kê, Ứng dụng KH&CN quản lý và sử dụng khi xây dựng phương án thiết kế mới. 3. Mã nguồn Sàn GDCN HY phải được bảo mật và nhà phát triển phải bàn giao bản quyền cho Sở Khoa học và Công nghệ, tránh lộ.

4.3. Thử nghiệm và nghiệm thu hệ thống

Yêu cầu	Có quy định về thử nghiệm và nghiệm thu hệ thống
Hiện trạng	Đáp ứng
Phương án	Quy định đối với việc thử nghiệm và nghiệm thu hệ thống: 1. Bên triển khai xây dựng kế hoạch, nội dung thử nghiệm hệ thống, trình cấp có thẩm quyền phê duyệt, trước khi thực hiện thử nghiệm và nghiệm thu hệ thống. 2. Hệ thống phải được kiểm thử trước khi đưa vào vận hành, khai thác sử dụng theo nội dung, kế hoạch được phê duyệt. 3. Có bộ phận có trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống. 4. Có đơn vị độc lập (Bên thứ ba hoặc bộ phận độc lập) thuộc đơn vị thực hiện tư vấn và giám sát quá trình thử nghiệm và nghiệm thu hệ thống. 5. Có báo cáo nghiệm thu được xác nhận của bộ phận chuyên trách và phê duyệt của chủ quản hệ thống thông tin trước khi đưa vào sử dụng.
Yêu cầu	Có nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống;
Hiện trạng	Đáp ứng
Phương án	Sở Khoa học và Công nghệ chỉ đạo Trung tâm Thông tin, Thống kê, Ứng dụng KH&CN xây dựng kế hoạch và thực hiện chạy thử nghiệm, tiến hành nghiệm thu sản phẩm hệ thống và đã đưa vào vận hành hiệu quả.
Yêu cầu	Có bộ phận có trách nhiệm thực hiện thử nghiệm và nghiệm thu

	hệ thống
Hiện trạng	Đáp ứng
Phương án	Sở Khoa học và Công nghệ chỉ đạo Trung tâm Thông tin, Thống kê, Ứng dụng KH&CN xây dựng kế hoạch và bố trí bộ phận có trách nhiệm thực hiện chạy thử nghiệm, tiến hành nghiệm thu sản phẩm hệ thống và đã đưa vào vận hành hiệu quả.

5. Quản lý vận hành Sàn GDCN HY

5.1. Quản lý an toàn mạng

Yêu cầu	Quản lý, vận hành hoạt động bình thường của hệ thống
Hiện trạng	Đáp ứng
Phương án	- Xây dựng Quy chế, quy trình vận hành Sàn GDCN HY - Sở Khoa học và công nghệ giao Trung tâm Thông tin, Thống kê, Ứng dụng KH&CN trực tiếp quản lý, quản trị và vận hành Sàn GDCN HY - Đến nay Sàn đang được vận hành tốt, đảm bảo: 1. Hệ thống mạng phải được thiết kế thống nhất, cùng kết hợp và hỗ trợ, tương tác hoạt động với nhau, được tổ chức quản lý định danh, xác thực đối với tất cả người sử dụng nhằm mục đích quản lý hệ thống chặt chẽ, bảo đảm an toàn và bảo mật. 2. Hệ thống mạng phải được thiết lập cấu hình để: Kiểm soát truy cập từ bên ngoài mạng; Kiểm soát truy cập từ bên trong mạng; Kết nối về hệ thống giám sát tập trung; Phòng chống xâm nhập giữa các vùng mạng; Phòng chống phần mềm độc hại trên môi trường mạng. 3. Các thiết bị mạng phải được cấu hình chức năng xác thực; Chỉ cho phép sử dụng các kết nối mạng an toàn (nếu hỗ trợ) khi truy cập, quản trị thiết bị từ xa; Giới hạn các địa chỉ mạng có thể kết nối, quản trị thiết bị từ xa; Hạn chế số lần đăng nhập sai; Phân quyền truy cập, quản trị; Nâng cấp, xử lý điểm yếu an toàn thông tin của thiết bị hệ thống trước khi đưa vào sử dụng. 4. Hệ thống mạng phải được trang bị hệ thống kỹ thuật, công nghệ hiện đại để thường xuyên, liên tục quản lý, giám sát, kiểm

	soát mạng nhằm phát hiện, ngăn chặn các truy cập trái phép của người sử dụng, tin tặc tấn công; triển khai cơ chế phòng chống virus, thư rác cho những hệ thống xung yếu (máy chủ website, máy chủ tên miền, …) và tại các máy chủ, máy trạm khác trong hệ thống. 5. Việc thanh lý, tiêu hủy thiết bị, vật mang thông tin trong mạng phải bảo đảm yêu cầu không để lộ, lọt thông tin Nhà nước. Phải có quy trình cụ thể và phải lưu giữ hồ sơ, biên bản việc thanh lý, tiêu hủy. 7. Đối với các thiết bị mạng chính đáp ứng: a) Phải lắp đặt thiết bị chống sét để bảo vệ hệ thống CNTT b) Thiết bị chuyển mạch (Switch): Thiết bị chuyển mạch mạng tin học của các cơ quan phải bảo đảm khả năng cung cấp các chức năng quản trị nhằm tăng cường độ an toàn và bảo mật cho hệ thống mạng như: Cung cấp khả năng từ chối các kết nối không mong muốn vào hệ thống trên từng cổng, quy định địa chỉ IP cho từng cổng và khống chế số lượng kết nối vào hệ thống mạng nội bộ thông qua thiết bị chuyển mạch. Phải có ít nhất 01 thiết bị chuyển mạch có hỗ trợ định tuyến IP (IP Routing) cho mỗi mạng nội bộ, hỗ trợ chức năng điều khiển truy cập (Access Control List), hỗ trợ chức năng xác thực thiết bị và người sử dụng (User & Device Authentication) và chức năng bảo mật quản trị mạng (Network Administration Security). c) Tường lửa (Firewall): Các cơ quan phải xây dựng tường lửa bảo đảm các yêu cầu gồm khả năng xử lý được số lượng kết nối đồng thời cao, hỗ trợ các công nghệ mạng riêng ảo thông dụng và có phần cứng mã hóa tích hợp để tăng tốc độ mã hóa dữ liệu, cung cấp đầy đủ các cơ chế bảo mật cơ bản như NAT, PAT, quản lý luồng dữ liệu vào, ra và có khả năng bảo vệ hệ thống trước các loại tấn công từ chối dịch vụ (DDoS). 8. Tập tin cấu hình, sơ đồ mạng logic và vật lý phải được cập nhật, sao lưu dự phòng.

	9. Có biện pháp bảo vệ, dự phòng, phòng chống các nguy cơ do mất cắp, cháy nổ, ngập lụt, động đất và các thảm họa khác do thiên nhiên hoặc con người gây ra và các phương án khôi phục hệ thống sau thảm họa.
Yêu cầu	Cập nhật; sao lưu dự phòng các tập tin cấu hình hệ thống và khôi phục hệ thống sau khi xảy ra sự cố
Hiện trạng	Đáp ứng
Phương án	- Xây dựng kế hoạch, phương án cụ thể thường xuyên, định kì tiến hành sao lưu dự phòng các tập tin, dữ liệu các tổ chức, cá nhân, doanh nghiệp gửi đến để lưu trữ và sao lưu cấu hình hệ thống nhằm khôi phục và khắc phục toàn hệ thống khi có sự cố xảy ra, đảm bảo an toàn về thông tin mạng.
Yêu cầu	Truy cập và quản lý cấu hình hệ thống
Hiện trạng	Đáp ứng
Phương án	Giao quyền truy cập và quản lý cấu hình hệ thống trực tiếp cho Phó Giám đốc Trung tâm Thông tin, Thống kê, Ứng dụng KH&CN và 01 viên chức phụ trách chính của Sàn để đảm bảo tính bí mật và phối hợp quản lý, vận hành tốt Sàn theo quy định.

5.2. Quản lý an toàn máy chủ và ứng dụng trên cổng thông tin điện tử của Sở và liên kết các Sàn

Yêu cầu	Quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ
Hiện trạng	Đáp ứng
Phương án	- Sở Khoa học và Công nghệ giao Trung tâm Thông tin, Thống kê, Ứng dụng KH&CN trực tiếp xây dựng quy chế quản lý và thực hiện quản lý Sàn vận hành tốt. - Trung tâm Thông tin, Thống kê, Ứng dụng KH&CN cử viên chức chuyên trách thực hiện chức năng vận hành admin và đầu vào đầu cuối thành thạo, hiệu quả, đảm bảo quy định về quản lý an toàn máy chủ và ứng dụng: 1. Quy định với máy chủ - Máy chủ cài đặt vật lý là HP Proliant DL 360 Gen 10 với hệ điều hành là Windows Server 2019,

	CenOS 7 (với máy chủ SOC BKAV) hiệu năng cao đáp ứng: a) Hệ thống máy chủ phải có tính năng sẵn sàng cao, cơ chế dự phòng linh hoạt để bảo đảm hoạt động liên tục. b) Có biện pháp bảo vệ, dự phòng, phòng chống các nguy cơ do mất cắp, cháy nổ, ngập lụt, động đất và các thảm họa khác do thiên nhiên hoặc con người gây ra và các phương án khôi phục sau thảm họa cho hệ thống máy chủ. c) Máy chủ phải được thiết lập chính sách xác thực; Kiểm soát truy cập; Kết nối về hệ thống giám sát tập trung; Thực hiện biện pháp phòng chống xâm nhập; Phòng chống phần mềm độc hại và xử lý dữ liệu trên máy chủ khi chuyển giao. d) Máy chủ phải được nâng cấp, xử lý điểm yếu an toàn thông tin trên máy chủ trước khi đưa vào sử dụng. đ) Việc kết nối, gỡ bỏ máy chủ khỏi hệ thống phải được sự cho phép của Thủ trưởng đơn vị và thực hiện theo quy trình đã được phê duyệt. e) Phần mềm hệ điều hành cài lên máy chủ ưu tiên là phần mềm hệ điều hành có bản quyền hoặc là phần mềm mã nguồn mở được sử dụng rộng rãi trong nước và quốc tế. g) Có tài liệu liệt kê, cài đặt với những phần mềm hệ thống cài trong máy chủ. 2. Quy định với ứng dụng: a) Các yêu cầu, thiết kế về an toàn bảo mật của phần mềm ứng dụng cần được xác định rõ trong tài liệu phân tích, thiết kế. Trong quá trình triển khai, vận hành các phần mềm ứng dụng cần đảm bảo nghiêm ngặt theo các yêu cầu, thiết kế về an toàn bảo mật. b) Ứng dụng phải được thiết lập chính sách xác thực; Kiểm soát truy cập; Kết nối về hệ thống giám sát tập trung; Có phương án bảo mật thông tin liên lạc, chống chối bỏ và biện pháp bảo đảm an toàn ứng dụng và mã nguồn. c) Có phương án xác định và khắc phục rủi ro trước, trong quá trình triển khai và khi vận hành các phần mềm ứng dụng. d) Ứng dụng phải kiểm tra, thử nghiệm và có biên bản đánh giá tính an toàn, bảo mật đối với phần mềm ứng dụng theo yêu cầu

	khi nghiệm thu các phần mềm này. Việc tiến hành thử nghiệm phải đảm bảo trên môi trường riêng biệt, không ảnh hưởng tới hoạt động và dữ liệu của đơn vị. 3. Khi vận hành, sử dụng, khai thác website người dùng đáp ứng quy định với việc sử dụng kèm theo ứng dụng thư điện tử: a) Tài khoản admin cần đặt mật khẩu đủ mạnh. c) Đơn vị quản lý cần có quy định về việc khóa và xóa bỏ tài khoản admin khi cá nhân đó không còn làm việc tại đơn vị. d) Đơn vị quản lý cần xây dựng phương án đảm bảo an toàn và tính khả dụng truy cập cho website trong nội bộ và trên Internet. 4. Khi cài đặt, vận hành, sử dụng, khai thác Hệ thống thông tin quản trị viên cần lưu ý với loại hình cổng/trang thông tin điện tử. a) Quản lý toàn bộ các phiên bản của mã nguồn, phối hợp với đơn vị thực hiện dịch vụ hosting tổ chức mô hình trang web hợp lý, tránh khả năng tấn công leo thang đặc quyền. Yêu cầu đơn vị cung cấp dịch vụ hosting phải cài đặt các hệ thống phòng vệ như tường lửa thiết bị phát hiện/phòng chống xâm nhập (IDS/IPS) ở mức ứng dụng web (WAP – Web Application Firewall). b) Các trang web khi đưa vào sử dụng hoặc bổ sung thêm các chức năng, dịch vụ công mới cần đánh giá kiểm định nhằm tránh được các lỗi bảo mật thường xảy ra trên ứng dung web như: SQL Injection, Cross – Site Scripting (XSS), … c) Phối hợp với các nhà cung cấp dịch vụ hosting xây dựng phương án phục hồi trang web, trong đó chú ý mỗi tháng thực hiện backup toàn bộ nội dung trang web một lần bao gồm mã nguồn, cơ sở dữ liệu, dữ liệu phi cấu trúc, … để bảo đảm khi có sự cố có thể khắc phục lại ngay trong vòng 24 giờ. d) Bảo đảm an toàn cho Cổng/Trang thông tin điện tử: Thực hiện theo hướng dẫn tại công văn số 2132/BTTTT-VNCERT ngày 18 tháng 7 năm 2011 của Bộ TT&TT về việc hướng dẫn bảo đảm an toàn thông tin cho các Cổng/Trang thông tin điện tử.
Yêu cầu	Truy cập mạng của máy chủ
Hiện trạng	Đáp ứng
Phương án	- Sở Khoa học và Công nghệ giao Trung tâm Thông tin, Thống

	kê, Ứng dụng KH&CN trực tiếp xây dựng quy chế quản lý và thực hiện quyền truy cập máy chủ quản lý Sàn. - Trung tâm Thông tin, Thống kê, Ứng dụng KH&CN phối hợp đơn vị quản lý hosting thực hiện quyền truy cập máy chủ quản lý Sàn để thực hiện các chức năng của Sàn.
Yêu cầu	Truy cập và quản trị máy chủ và ứng dụng
Hiện trạng	Đáp ứng
Phương án	Chỉ Phó giám đốc Trung tâm Thông tin, Thống kê, Ứng dụng KH&CN và viên chức được giao phụ trách Sàn được quyền truy cập và quản trị máy chủ cũng như quản lý các ứng dụng của Sàn đảm bảo hiệu quả, bí mật.
Yêu cầu	Cập nhật; sao lưu dự phòng và khôi phục sau khi xảy ra sự cố
Hiện trạng	Đáp ứng
Phương án	Thường xuyên, định kỳ sử dụng giải pháp chuyên dụng hoặc giải pháp tương đương sử dụng các giải pháp như SAN, NAS… để tiến hành cập nhật hệ thống, phần mềm, đề đồng bộ hóa hệ thống. Tiến hành sao lưu dự phòng thường xuyên dữ liệu nhằm khôi phục dữ liệu và khắc phục khi có sự cố xảy ra.

5.3. Quản lý an toàn dữ liệu

Yêu cầu	Chính sách, quy trình dự phòng và khôi phục dữ liệu;
Hiện trạng	Đáp ứng
Phương án	- Xây dựng chính sách dự phòng và khôi phục dữ liệu thường xuyên, định kỳ 01 tháng sao lưu các dữ liệu hệ thống và tự sao lưu dữ liệu cập nhật trong 24 giờ. - Xây dựng quy trình thực hiện các bước sao lưu dữ liệu và khôi phục dữ liệu khi sự cố xảy ra. Dữ liệu sao lưu dự phòng được lưu trữ trên máy tính khác của Trung tâm. Đảm bảo các quy định về qan toàn dữ liệu: 1. Thực hiện quản lý, lưu trữ dữ liệu quan trọng trong hệ thống cùng với mã kiểm tra tính nguyên vẹn. 2. Có cơ chế sao lưu dữ liệu dự phòng, lưu trữ dữ liệu tại nơi an toàn đồng thời thường xuyên kiểm tra để bảo đảm sẵn sàng phục hồi nhằm ngăn ngừa và hạn chế khi sự cố an toàn thông tin mạng xảy ra.

	3. Tiến hành cập nhật đồng bộ thông tin, dữ liệu giữa hệ thống sao lưu dự phòng chính và hệ thống phụ được thực hiện theo yêu cầu của đơn vị vận hành hệ thống. 4. Sử dụng mật mã để bảo đảm an toàn và bảo mật dữ liệu trong lưu trữ. 5. Quản lý chặt chẽ các thiết bị lưu trữ dữ liệu, nghiêm cấm việc di chuyển, thay đổi vị trí khi chưa được phép của người có thẩm quyền. 6. Quản lý và phân quyền truy cập phần mềm ứng dụng và cơ sở dữ liệu phù hợp với chức năng, nhiệm vụ của người sử dụng. Quyền truy cập phải được phân ra theo từng cấp độ tương ứng với từng nhiệm vụ của nhân viên và phải được phê duyệt từ cấp trên. 7. Định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: Tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ. 8. Lưu trữ có mã hóa các thông tin, dữ liệu (không phải là thông tin, dữ liệu công khai) trên hệ thống lưu trữ/phương tiện lưu trữ.
Yêu cầu	Định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.
Hiện trạng	Đáp ứng
Phương án	Định kỳ 01 tháng hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ để lưu trữ tại máy tính khác của Trung tâm nhằm khắc phục và khôi phục dữ liệu hệ thống khi có sự cố xảy ra.
Yêu cầu	Có quy định về quản lý phòng chống phần mềm độc hại
Hiện trạng	Đáp ứng
Phương án	Quy định về quản lý phòng chống phần mềm độc hại:

	1. Tất cả các máy trạm, máy chủ phải được trang bị phần mềm phòng chống mã độc. Các phần mềm phòng chống mã độc phải được thiết lập chế độ tự động cập nhật; chế độ tự động quét mã độc khi sao chép, mở các tập tin. 2. Khi cập nhật dữ liệu lên website phải có định dạng theo danh mục tiêu chuẩn kỹ thuật về ứng dụng CNTT trong cơ quan nhà nước như: (.txt), (.doc), (.odt), (.pdf) và các định dạng khác theo quy định, không được gửi các file thực thi (.com), (.bat), (.exe) … 3. Cán bộ, công chức, viên chức và người lao động trong cơ quan phải được hướng dẫn về phòng chống mã độc, 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. 4. Tất cả các máy tính của đơn vị phải được cấu hình nhằm vô hiệu hóa tính năng tự động thực thi (autoplay) các tập tin trên các thiết bị lưu trữ di động. 5. Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm mã độc trên máy trạm (ví dụ: máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống mã độc, mất dữ liệu, …), người sử dụng phải báo trực tiếp cho bộ phận có trách nhiệm của đơn vị để xử lý. 6. Phần mềm ứng dụng trước khi được cài đặt, sử dụng phải được kiểm tra xem có phần mềm độc hại tồn tại hay không? Tất cả các tập tin, thư mục phải được quét mã độc trước khi sao chép, sử dụng. 7. Định kỳ hàng năm thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống website; Thực hiện kiểm tra và xử lý phần mềm độc hại khi phát hiện dấu hiệu hoặc cảnh báo về dấu hiệu phần mềm độc hại xuất hiện trên hệ thống.

5.4. Quản lý sự cố an toàn thông tin

Yêu cầu	Phân nhóm sự cố an toàn thông tin mạng
Hiện trạng	Đáp ứng
Phương án	Xây dựng phương án phân nhóm sự cố an toàn thông tin mạng

	như: hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ để có giải pháp phòng chống các mã độc xâm hại. Khi các mã độc xâm hại có thể nhanh chóng khoanh vung và xử lý loại bỏ mã nguồn độc và khắc phục khôi phục dữ liệu hoặc sử dụng dữ liệu dự phòng để khôi phục.
Yêu cầu	Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng;
Hiện trạng	Đáp ứng
Phương án	- Khi sự cố an toàn mạng xảy ra tiến hành xem xét, phán đoán, khoanh vùng dữ liệu bị xâm hại. - Xác định mã độc xâm hại thuộc loại nào - Tự xử lý bằng các ứng dụng như diệt virus, tường lửa để ngăn chặn và loại trừ. - Trường hợp không thực hiện được phải phối hợp với bên thứ ba có nghiệp vụ, kinh nghiệm để xử lý phần mềm độc hại hoặc sự cố xảy ra. - Trường hợp không thể khắc phục tiến hành xóa bỏ và khôi phục lại dữ liệ thông qua dữ liệu đã được sao lưu trước đó.
Yêu cầu	Kế hoạch ứng phó sự cố an toàn thông tin mạng
Hiện trạng	Đáp ứng
Phương án	- Xây dựng, ban hành văn bản chỉ đạo điều hành, văn bản hướng dẫn về công tác giám sát, đảm bảo an toàn thông tin mạng trong hoạt động của toàn Sở; Ban hành kế hoạch triển khai nhiệm vụ giám sát, ứng phó sự cố an toàn thông tin mạng hàng năm lồng ghép vào nội dung Kế hoạch ứng dụng CNTT của từng đơn vị, của Sở KH&CN… - Xây dựng, duy trì hệ thống giám sát, đảm bảo an toàn thông tin của Sở: Thành lập tổ Giám sát, kiểm soát an toàn thông tin, giao Trung tâm Thông tin, Thống kê, Ứng dụng KHCN làm thường trực; Thực hiện quan trắc, giám sát an toàn thông tin mạng cho

	các hệ thống dùng chung của Sở;Triển khai kiểm tra, rà soát, đánh giá an toàn, an ninh thông tin mạng; Triển khai giám sát an toàn thông tin mạng cho phần dịch vụ, hạ tầng mạng phục vụ xây dựng Chính quyền điện tử của toàn Sở. - Thường xuyên đề xuất, cử cán bộ đi đào tạo, tập huấn và tuyên truyền về an toàn thông tin: Đào tạo, tập huấn, phát triển nguồn nhân lực về giám sát và đảm bảo an toàn thông tin mạng cho đội ngũ cán bộ chuyên trách CNTT và thành viên Đội ứng cứu sự cố an toàn thông tin mạng khi tỉnh tổ chức. * Thực hiện tốt các quy định sau: a) Phân nhóm sự cố an toàn thông tin mạng theo quy định tại Quyết định số 05/2017/NĐ-CP của Thủ tướng Chính phủ ngày 16/3/2017 quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia (Quyết định 05); Xây dựng phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng, ứng phó sự cố an toàn thông tin mạng. b) Xây dựng quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng theo quy định tại Điều 13,14 Quyết định số 05. c) Xây dựng và triển khai kế hoạch ứng phó sự cố an toàn thông tin theo quy định tại Điều 16, Quyết định số 05. d) Quyết định toàn diện về mặt kỹ thuật đối với các cơ quan trong quá trình khắc phục sự cố về ATTT; Hỗ trợ, phối hợp và hướng dẫn các cơ quan khắc phục sự cố mất ATTT; Yêu cầu ngưng hoạt động một phần hoặc toàn bộ các hệ thống thông tin của các cơ quan nhằm phục vụ công tác khắc phục sự cố về ATTT; Phối hợp với đơn vị chức năng trong điều tra các nguyên nhân gây ra sự cố mất an toàn thông tin theo chỉ đạo của Lãnh đạo đơn vị. đ) Phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an

	toàn thông tin; Yêu cầu bên cung cấp, hỗ trợ cung cấp quy trình xử lý sự cố cho các dịch vụ do bên cung cấp, hỗ trợ cung cấp liên quan đến hệ thống. 2. Trách nhiệm của người dùng: Thông tin, báo báo kịp thời cho cán bộ chuyên trách về ATTT của đơn vị khi phát hiện các sự cố gây mất ATTT trong quá trình tham gia vào hệ thống thông tin của đơn vị; Phối hợp tích cực trong suốt quá trình giải quyết và khắc phục sự cố.
Yêu cầu	Giám sát, phát hiện và cảnh báo sự cố an toàn thông tin
Hiện trạng	Đáp ứng
Phương án	- Xây dựng, duy trì hệ thống giám sát, đảm bảo an toàn thông tin của Sở: Thành lập tổ Giám sát, kiểm soát an toàn thông tin, giao Trung tâm Thông tin, Thống kê, Ứng dụng KHCN làm thường trực; Thực hiện quan trắc, giám sát an toàn thông tin mạng cho các hệ thống dùng chung của Sở;Triển khai kiểm tra, rà soát, đánh giá an toàn, an ninh thông tin mạng; Triển khai giám sát an toàn thông tin mạng cho phần dịch vụ, hạ tầng mạng phục vụ xây dựng Chính quyền điện tử của toàn Sở. - Thường xuyên đề xuất, cử cán bộ đi đào tạo, tập huấn và tuyên truyền về an toàn thông tin: Đào tạo, tập huấn, phát triển nguồn nhân lực về giám sát và đảm bảo an toàn thông tin mạng cho đội ngũ cán bộ chuyên trách CNTT và thành viên Đội ứng cứu sự cố an toàn thông tin mạng khi tỉnh tổ chức. - Đầu tư, thiết lập hệ thống thiết bị và thường xuyên triển khai kiểm tra, đánh giá, giám sát mức độ an toàn thông tin cho hệ thống thông tin phục vụ chính phủ điện tử thuộc quyền quản lý. Thường xuyên cung cấp các thông tin kỹ thuật về hạ tầng, hệ thống thông tin, ứng dụng, dịch vụ, địa chỉ IP Internet, bố trí địa điểm, cổng kết nối, các điều kiện kỹ thuật, thiết lập, cấu hình, lắp đặt các thiết bị cần thiết theo yêu cầu; quan trắc và thực hiện

	giám sát trực tiếp hoặc gián tiếp cho các hệ thống thông tin phục vụ Chính phủ điện tử và hệ thống thông tin quan trọng khác do mình quản lý. Cung cấp các thông tin, nhật ký, dữ liệu giám sát và phối hợp chặt chẽ, thực hiện các yêu cầu của Cơ quan điều phối của tỉnh trong công tác giám sát, ứng cứu xử lý sự cố, bảo đảm an toàn thông tin mạng cho hệ thống thông tin phục vụ Chính phủ điện tử và hệ thống thông tin quan trọng của toàn tỉnh. Định kỳ 6 tháng và hàng năm tổ chức kiểm tra, đánh giá hoạt động của hệ thống quan trắc, giám sát an toàn thông tin mạng cơ sở và việc kết nối, phối hợp, trao đổi thông tin, dữ liệu giám sát, cảnh báo sự cố an toàn thông tin mạng, báo cáo Sở Thông tin truyền thông để tổng hợp, báo cáo UBND tỉnh. * Sở thực hiện nghiêm các quy định về quản lý giám sát an toàn hệ thống thông tin: 1. Triển khai hệ thống giám sát trung tâm phải đáp ứng yêu cầu tại Khoản 1, Điều 5, Thông tư 31/2017/TT-BTTTT. 2. Thông tin giám sát và danh mục các đối tượng giám sát phải đáp ứng yêu cầu tại Khoản 2, Điều 5, Thông tư 31/2017/TT-BTTTT. Kết nối và gửi nhật ký hệ thống từ đối tượng giám sát về hệ thống giám sát. 3. Thực thi nhiệm vụ giám sát theo quy định tại Khoản 3, Điều 5, Thông tư số 31/2017/TT-BTTTT. 4. Định kỳ hàng năm tổ chức nâng cao năng lực hoạt động giám sát theo quy định tại Điều 9, Thông tư số 31/2017/TT-BTTTT. 5. Chủ quản hệ thống thông tin có trách nhiệm giám sát an toàn thông tin theo quy định tại Điều 14, Thông tư số 31/2017/TT-BTTTT.
Yêu cầu	Quy trình ứng cứu sự cố an toàn thông tin mạng thông thường
Hiện trạng	Đáp ứng
Phương án	Khi xảy ra sự cố tấn công mạng, Sở Khoa học và Công nghệ giao Trung tâm Thông tin, Thống kê, Ứng dụng KH&CN thực hiện theo quy trình gồm 5 bước:

	- Phát hiện, báo cáo sự cố: phát hiện sự cố mạng ở về thời gian, khả năng lây lan, thiệt hại, kịp thời báo cáo Giám đốc Sở để xin ý kiến xử lí. - Xác định hình thức tấn công, mức độ khẩn cấp xem hình thức tấn công như thế nào, mức độ nguy hiểm của các mã độc hoặc các trang web lạ,… và độ khẩn cấp để thực hiện xử lí thông thường đối với sự cố an ninh mạng thông thường và báo cáo Sở Thông tin Truyền thông và UBND tỉnh để xin ý kiến chỉ đạo xử lý về chuyên môn đối với sự cố an ninh mạng nghiêm trọng - Ứng cứu sự cố, khôi phục hệ thống: Huy động tối đa tổ ứng phó và xử lí sự cố của Sở đã được thành lập; phối hợp với các đơn vị Sàn của các tỉnh bạn trong cả nước để có giải pháp khắc phục triệt để. - Điều phối, ứng cứu sự cố: Tiến hành xác định và ứng phó xử lí sự cố rút điểm hạn chế tối đa thiệt hại do sự cố gây ra. -Kết thúc xử lý sự cố: Xử lí triệt để sự số thông thường, báo cáo Giám đốc Sở và đề xuất yêu cầu (nếu có). Tổng thời gian từ lúc phát hiện sự cố đến lúc hoàn thành ứng cứu ban đầu tối đa là 33 giờ. Sau khi hoàn thành ứng cứu ban đầu, yêu cầu Sở Thông tin Truyền thông tiếp tục hỗ trợ theo dõi khắc phục sự cố trong vòng 1 tuần nhằm khắc phục triệt để sự cố. * Ngoài ra có thể bổ sung thêm các biện pháp sau để thực hiện quy trình được tốt hơn: + Xây dựng phương án và quy trình ứng cứu sự cố an toàn thông tin mạng thông thường bằng phương án thành lập tổ giám sát và ứng cứu sự cố an toàn thông tin mạng của Sở, giao Trung tâm Thông tin, Thống kê, Ứng dụng KH&CN làm thường trực, các thành viên là Trưởng các phòng, đơn vị thuộc Sở và Thường trực thường xuyên báo cáo Giám đốc Sở xin ý kiến chỉ đạo khi có sự cố xảy ra và thực hiện theo quy trình: + Phối hợp với Sở Thông tin và Truyền thông và các đầu mối khác liên quan trong mạng lưới ứng cố máy tính, thông tin mạng trong toàn tỉnh. Liên kết, phối hợp các bộ phận ứng phó sự cố của các sàn trong cả nước để khắc phục sự cố khi xảy ra. + Thu thập thông tin thông báo, cung cấp kịp thời các thông tin sự cố bằng văn bản đến các đầu mối, các sàn hoặc trên cổng thông tin điện tử của tỉnh, trên mục thông báo của Sàn. + Báo cáo Sở Thông tin Truyền thông về sự cố máy tính và các điểm yếu, lỗ hổng bảo mật, các mã độc hại, các nguồn tấn công để xin ý kiến chỉ đạo chuyên môn. + Báo cáo khó khăn, đề xuất giải pháp ứng phó, khắc phục với UBND tỉnh. + Đầu tư, thiết lập hệ thống thiết bị và thường xuyên triển khai

	kiểm tra, đánh giá, giám sát mức độ an toàn thông tin cho hệ thống thông tin phục vụ chính phủ điện tử thuộc quyền quản lý. Thường xuyên cung cấp các thông tin kỹ thuật về hạ tầng, hệ thống thông tin, ứng dụng, dịch vụ, địa chỉ IP Internet, bố trí địa điểm, cổng kết nối, các điều kiện kỹ thuật, thiết lập, cấu hình, lắp đặt các thiết bị cần thiết theo yêu cầu; + Thường xuyên đề xuất, cử cán bộ đi đào tạo, tập huấn và tuyên truyền về an toàn thông tin: Đào tạo, tập huấn, phát triển nguồn nhân lực về giám sát và đảm bảo an toàn thông tin mạng cho đội ngũ cán bộ chuyên trách CNTT và thành viên Đội ứng cứu sự cố an toàn thông tin mạng khi tỉnh tổ chức.
Yêu cầu	Quy trình ứng cứu sự cố an toàn thông tin mạng nghiêm trọng;
Hiện trạng	Đáp ứng
Phương án	Khi xảy ra sự cố cố an toàn thông tin mạng nghiêm trọng, Sở Khoa học và Công nghệ giao Trung tâm Thông tin, Thống kê, Ứng dụng KH&CN thực hiện theo quy trình gồm 5 bước: - Phát hiện, báo cáo sự cố: phát hiện sự cố mạng ở về thời gian, khả năng lây lan, thiệt hại, kịp thời báo cáo Giám đốc Sở để xin ý kiến xử lí, đặc biệt lưu ý nếu là sự cố nghiêm trọng phải thực hiện khẩn cấp các bước tiếp theo. - Xác định hình thức tấn công, mức độ khẩn cấp xem hình thức tấn công như thế nào, mức độ nguy hiểm của các mã độc hoặc các trang web lạ,… và độ khẩn cấp để thực hiện báo cáo Sở Thông tin Truyền thông và UBND tỉnh để xin ý kiến chỉ đạo xử lý về chuyên môn đối với sự cố an ninh mạng nghiêm trọng - Ứng cứu sự cố, khôi phục hệ thống: Huy động tối đa tổ ứng phó và xử lí sự cố của Sở đã được thành lập; phối hợp với Sở Thông tin truyền thông, các đơn vị chuyên môn liên quan và các đơn vị Sàn của các tỉnh bạn trong cả nước để có giải pháp khắc phục triệt để. - Điều phối, ứng cứu sự cố: Tiến hành xác định và ứng phó xử lí sự cố rứt điểm hạn chế tối đa thiệt hại do sự cố gây ra. - Kết thúc xử lý sự cố: Xử lí triệt để sự cố nghiêm trọng, báo cáo

	UBND tỉnh để đề xuất và thực hiện các giải pháp an toàn trong thời gian tiếp theo. Tổng thời gian từ lúc phát hiện sự cố đến lúc hoàn thành ứng cứu ban đầu là 33 giờ (có thể dài hơn phụ thuộc mức độ nghiêm trọng của sợ cố). Sau khi hoàn thành ứng cứu ban đầu, yêu cầu Sở Thông tin Truyền thông tiếp tục hỗ trợ theo dõi khắc phục sự cố trong vòng 1 tuần nhằm khắc phục triệt để sự cố. * Ngoài ra có thể bổ sung thêm các biện pháp sau để thực hiện quye trình được tốt hơn: + Xây dựng phương án và quy trình ứng cứu sự cố an toàn thông tin mạng thông thường bằng phương án thành lập tổ giám sát và ứng cứu sự cố an toàn thông tin mạng của Sở, giao Trung tâm Thông tin, Thống kê, Ứng dụng KH&CN làm thường trực, các thành viên là Trưởng các phòng, đơn vị thuộc Sở và Thường trực thường xuyên báo cáo Giám đốc Sở xin ý kiến chỉ đạo khi có sự cố xảy ra và thực hiện theo quy trình: + Phối hợp với Sở Thông tin và Truyền thông và các đầu mối khác liên quan trong mạng lưới ứng cố máy tính, thông tin mạng trong toàn tỉnh. Liên kết, phối hợp các bộ phận ứng phó sự cố của các sàn trong cả nước để khắc phục sự cố khi xảy ra. + Thu thập thông tin thông báo, cung cấp kịp thời các thông tin sự cố bằng văn bản đến các đầu mối, các sàn hoặc trên cổng thông tin điện tử của tỉnh, trên mục thông báo của Sàn. + Báo cáo Sở Thông tin Truyền thông về sự cố máy tính và các điểm yếu, lỗ hổng bảo mật, các mã độc hại, các nguồn tấn công để xin ý kiến chỉ đạo chuyên môn. + Báo cáo khó khăn, đề xuất giải pháp ứng phó, khắc phục với UBND tỉnh. + Đầu tư, thiết lập hệ thống thiết bị và thường xuyên triển khai kiểm tra, đánh giá, giám sát mức độ an toàn thông tin cho hệ thống thông tin phục vụ chính phủ điện tử thuộc quyền quản lý.

	Thường xuyên cung cấp các thông tin kỹ thuật về hạ tầng, hệ thống thông tin, ứng dụng, dịch vụ, địa chỉ IP Internet, bố trí địa điểm, cổng kết nối, các điều kiện kỹ thuật, thiết lập, cấu hình, lắp đặt các thiết bị cần thiết theo yêu cầu; + Thường xuyên đề xuất, cử cán bộ đi đào tạo, tập huấn và tuyên truyền về an toàn thông tin: Đào tạo, tập huấn, phát triển nguồn nhân lực về giám sát và đảm bảo an toàn thông tin mạng cho đội ngũ cán bộ chuyên trách CNTT và thành viên Đội ứng cứu sự cố an toàn thông tin mạng khi tỉnh tổ chức.
Yêu cầu	Cơ chế phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an toàn thông tin.
Hiện trạng	Đáp ứng
Phương án	Sở Khoa học và Công nghệ xây dựng cơ chế phối hợp với các cơ quan chuyên môn về mạng, an ninh mạng, các nhóm chuyên gia, các Sàn giao dịch công nghệ trong cả nước, đặc biệt là Sở Thông tin, Truyền thông trong thực hiện các giải pháp hỗ trợ đảm bảo an ninh mạng, cụ thể: + Xây dựng phương án và quy trình ứng cứu sự cố an toàn thông tin mạng thông thường bằng phương án thành lập tổ giám sát và ứng cứu sự cố an toàn thông tin mạng của Sở, giao Trung tâm Thông tin, Thống kê, Ứng dụng KH&CN làm thường trực, các thành viên là Trưởng các phòng, đơn vị thuộc Sở và Thường trực thường xuyên báo cáo Giám đốc Sở xin ý kiến chỉ đạo khi có sự cố xảy ra và thực hiện theo quy trình: + Phối hợp với Sở Thông tin và Truyền thông và các đầu mối khác liên quan trong mạng lưới ứng cố máy tính, thông tin mạng trong toàn tỉnh. Liên kết, phối hợp các bộ phận ứng phó sự cố của các sàn trong cả nước để khắc phục sự cố khi xảy ra. + Phối hợp với các đơn vị cung ứng dịch vụ đảm bảo an ninh mạng để cung cấp các dịch vụ, cài đặt và phối hợp xử lý an ninh

	mạng khi có sự cố xảy ra. + Thu thập thông tin thông báo, cung cấp kịp thời các thông tin sự cố bằng văn bản đến các đầu mối, các sàn hoặc trên cổng thông tin điện tử của tỉnh, trên mục thông báo của Sàn. + Báo cáo Sở Thông tin Truyền thông về sự cố máy tính và các điểm yếu, lỗ hổng bảo mật, các mã độc hại, các nguồn tấn công để xin ý kiến chỉ đạo chuyên môn. + Báo cáo khó khăn, đề xuất giải pháp ứng phó, khắc phục với UBND tỉnh. + Đầu tư, thiết lập hệ thống thiết bị và thường xuyên triển khai kiểm tra, đánh giá, giám sát mức độ an toàn thông tin cho hệ thống thông tin phục vụ chính phủ điện tử thuộc quyền quản lý. Thường xuyên cung cấp các thông tin kỹ thuật về hạ tầng, hệ thống thông tin, ứng dụng, dịch vụ, địa chỉ IP Internet, bố trí địa điểm, cổng kết nối, các điều kiện kỹ thuật, thiết lập, cấu hình, lắp đặt các thiết bị cần thiết theo yêu cầu; + Thường xuyên đề xuất, cử cán bộ đi đào tạo, tập huấn và tuyên truyền về an toàn thông tin: Đào tạo, tập huấn, phát triển nguồn nhân lực về giám sát và đảm bảo an toàn thông tin mạng cho đội ngũ cán bộ chuyên trách CNTT và thành viên Đội ứng cứu sự cố an toàn thông tin mạng khi tỉnh tổ chức.

5.5. Quản lý an toàn người sử dụng đầu cuối

Yêu cầu	Quản lý truy cập, sử dụng tài nguyên nội bộ
Hiện trạng	Đáp ứng
Phương án	* Sở xây dựng quy chế về quản lý mạng và sử lí mạng máy tính nội bộ trên cơ sở sau: - Cấp quyền truy cập cho Lãnh đạo Sở, admin và quyền truy cập thông thường cho các thành viên, công chức, viên chức và người lao động trong toàn sở. Trong đó cấp quyền truy cập admin cho Phó Giám đốc Trung tâm và 01 cán bộ phụ trách Sàn thuộc Thông tin, Thống kê, Ứng dụng KH&CN.

	- Cán bộ, công chức, viên chức và người lao động được quyền truy cập để sử dụng nguồn tài nguyên dữ liệu nội bộ, các file được chuyển tải phục vụ công tác quản lý, chuyên môn,… thông qua tài khoản được cấp và mật khẩu đăng nhập, phải thường xuyên thay đổi mật khẩu đăng nhập để đảm bảo an toàn và bảo mật dữ liệu trên mạng nội bộ. - Người dùng có thể truyền file, đăng tải các thông tin và được admin kiểm duyệt trước khi đăng. - Việc truy cập và sử dụng tài nguyên nội bộ phải tuân thủ theo quy định và phải đảm bảo an ninh, bảo mật mạng nội bộ, cụ thể: 1. Kết nối máy tính/Thiết bị đầu cuối của người sử dụng vào hệ thống: a) Người sử dụng khi truy cập, sử dụng tài nguyên nội bộ, truy cập mạng và tài nguyên trên Internet phải tuân thủ các quy định của pháp luật về bảo đảm an toàn thông tin và các quy định của cơ quan, tổ chức. b) Khi cài đặt, kết nối máy tính/thiết bị đầu cuối phải thực hiện theo hướng dẫn/quy trình dưới sự giám sát của bộ phân chuyên trách về an toàn thông tin. c) Đối với hệ thống thông tin có cấp độ 3 trở lên, máy tính/thiết bị đầu cuối phải được xử lý điểm yếu về an toàn thông tin, cấu hình cứng hóa bảo mật trước khi kết nối vào hệ thống. 2. Trong quá trình sử dụng: a) Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác của pháp luật về an toàn thông tin mạng. Chịu trách nhiệm bảo đảm an toàn thông tin mạng trong phạm vi trách nhiệm và quyền hạn được giao. b) Có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng. c) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cao ngay với cấp trên và bộ phận phụ trách công nghệ

	thông tin của đơn vị để kịp thời ngăn chặn và xử lý. d) Tham gia các chương trình đào tạo, hội nghị về an toàn thông tin mạng được tỉnh hoặc đơn vị chuyên môn tổ chức.
Yêu cầu	Quản lý truy cập mạng và tài nguyên trên Internet.
Hiện trạng	Đáp ứng
Phương án	Sở xây dựng quy chế về quản lý mạng và sử lí mạng máy tính nội bộ trong đó đảm bảo việc truy cập mạng và tài nguyên Internet trên cơ sở sau: - Cấp quyền truy cập cho Lãnh đạo Sở, admin và quyền truy cập thông thường cho các thành viên, công chức, viên chức và người lao động trong toàn sở. Trong đó cấp quyền truy cập admin cho Phó Giám đốc Trung tâm và 01 cán bộ phụ trách Sàn thuộc Thông tin, Thống kê, Ứng dụng KH&CN. - Cán bộ, công chức, viên chức và người lao động được quyền truy cập vào mạng và sử dụng Internet để sử dụng nguồn tài nguyên dữ liệu nội bộ, các file được chuyển tải phục vụ công tác quản lý, chuyên môn,… thông qua tài khoản được cấp và mật khẩu đăng nhập, phải thường xuyên thay đổi mật khẩu đăng nhập để đảm bảo an toàn và bảo mật dữ liệu trên mạng nội bộ. - Người dùng có thể khai thác các dữ liệu, thông tin trên mạng Internet mà ở đây là Sàn hoặc đăng tải các thông tin, dữ liệu lên Sàn phải được admin kiểm duyệt trước khi đăng. - Việc truy cập và sử dụng tài nguyên Internet phải tuân thủ theo quy định và phải đảm bảo an ninh, bảo mật mạng nội bộ, cụ thể: 1. Kết nối máy tính/Thiết bị đầu cuối của người sử dụng vào hệ thống: a) Người sử dụng khi truy cập, sử dụng tài nguyên nội bộ, truy cập mạng và tài nguyên trên Internet phải tuân thủ các quy định của pháp luật về bảo đảm an toàn thông tin và các quy định của cơ quan, tổ chức.

	b) Khi cài đặt, kết nối máy tính/thiết bị đầu cuối phải thực hiện theo hướng dẫn/quy trình dưới sự giám sát của bộ phân chuyên trách về an toàn thông tin. c) Đối với hệ thống thông tin có cấp độ 3 trở lên, máy tính/thiết bị đầu cuối phải được xử lý điểm yếu về an toàn thông tin, cấu hình cứng hóa bảo mật trước khi kết nối vào hệ thống. 2. Trong quá trình sử dụng: a) Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác của pháp luật về an toàn thông tin mạng. Chịu trách nhiệm bảo đảm an toàn thông tin mạng trong phạm vi trách nhiệm và quyền hạn được giao. b) Có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng. c) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cao ngay với cấp trên và bộ phận phụ trách công nghệ thông tin của đơn vị để kịp thời ngăn chặn và xử lý. d) Tham gia các chương trình đào tạo, hội nghị về an toàn thông tin mạng được tỉnh hoặc đơn vị chuyên môn tổ chức.

PHỤ LỤC II.Thuyết minh phương án bảo đảm an toàn thông tin đáp ứng các yêu cầu an toàn cơ bản về kỹ thuật

1. Bảo đảm an toàn mạng

1.1. Thiết kế hệ thống

a) Các vùng mạng trong hệ thống

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Vùng Mạng Nội Bộ	Có	Vùng mạng nội bộ giúp khai thác thông tin nội bộ bên trong hệ thống và thực hiện kết nối với các vùng mạng khác
2	Vùng mạng biên	Có	Kết nối với website với mạng Internet và mạng diện rộng
3	Vùng DMZ	Không có	Chưa thiết kế Vùng mạng DMZ, cung cấp dịch vụ trực tiếp ra bên ngoài Internet
4	Vùng máy chủ nội bộ	Không có	Chưa thiết kế riêng vùng máy chủ nội bộ
5	Vùng mạng không dây	Không có	TT THDL không cho phép kết nối mạng không dây

b) Phương án thiết kế bảo đảm các yêu cầu sau

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Phương án quản lý truy cập, quản trị hệ thống từ xa an toàn	Có	Các thiết bị hệ thống/máy chủ được thiết lập cấu hình cho phép quản trị từ xa an toàn.
2	Phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập	Có	Truy cập giữa các vùng mạng được quản lý và phòng chống xâm nhập sử dụng các thiết bị tường lửa chuyên dụng có tích hợp chức năng phòng chống xâm nhập.
3	Có phương án dự phòng kết nối mạng Internet cho hệ thống	Chưa có	Chưa có dự phòng đường kết nối mạng Internet. Mà chỉ dung một đường mạng cáp quang chung cho toàn bộ các thiết bị và các ứng dụng của nhà cung cấp VNPT Hưng Yên.

1.2. Kiểm soát truy cập từ bên ngoài mạng

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập thông tin của Sàn GDCN HYhoặc quản trị hệ thống từ các mạng bên ngoài và mạng Internet	Có	Hệ thống được thiết lập chỉ cho phép kết nối mạng có hỗ trợ mã hóa, xác thực khi truy cập thông tin nội bộ hoặc quản trị hệ thống từ các mạng bên ngoài và mạng Internet.

2	Kiểm soát truy cập từ bên ngoài vào hệ thống theo từng dịch vụ, ứng dụng cụ thể; chặn tất cả truy cập tới các dịch vụ, ứng dụng mà hệ thống không cung cấp hoặc không cho phép truy cập từ bên ngoài	Có	Hệ thống được thiết lập chỉ cho phép kiểm soát truy cập từ bên ngoài vào hệ như POP3, SMTP, IMAP, …Chính sách được thiết lập trên Firewall Forigate 200D theo chiều từ bên ngoài vào Vùng Mạng Nội Bộ; Từ bên ngoài vào Vùng Mạng Biên.
3	Thiết lập thời gian chờ (timeout) để đóng phiên kết nối khi hệ thống không nhận được yêu cầu từ người dùng	Có	Thiết lập giới hạn thời gian chờ để đóng phiên kết nối khi hệ thống không nhận được yêu cầu từ người dùng được thiết lập trên các Firewall Fortigate 200D

1.3. Kiểm soát truy cập từ bên trong mạng khi Sàn GDCN HY được kích hoạt kết nối

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Chỉ cho phép truy cập các ứng dụng, dịch vụ bên ngoài theo yêu cầu nghiệp vụ, chặn các dịch vụ khác không phục vụ hoạt động nghiệp vụ theo chính sách của tổ chức	Có	Chính sách kiểm soát truy cập từ các vùng mạng trong hệ thống đi ra các mạng bên ngoài và mạng Internet được thiết lập trên Firewall 02 Fortigate 200Dtheo chiều từ bên trong ra ngoài Internet

1.4. Nhật ký hệ thống

Yêu cầu **Thiết bị**	Thiết lập chức năng ghi, lưu trữ nhật ký hệ thống trên các thiết bị hệ thống	Sử dụng máy chủ thời gian trong hệ thống để đồng bộ thời gian
Firewall Fortigate 200D	+	+
Switch 01/ Switch Cisco Catalyst 2900-x Series	+	+

1.5. Phòng chống xâm nhập

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Có phương án phòng chống xâm nhập để bảo vệ các vùng mạng trong hệ thống (bảo vệ vùng DMZ và vùng máy chủ nội bộ)	Có	Các vùng mạng được triển khai hệ thống IDS/IPS, hoạt động ở chế độ Inline cho phép phát hiện và phòng chống xâm nhập
2	Định kỳ cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng(Signatures - chữ ký).	Có	Đã thiết lập chức năng tự động cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng đều

			được thiết lập trên thiết bị Firewall Fortigate 200D

1.6. Bảo vệ thiết bị hệ thống

Yêu cầu **Thiết bị**	Cấu hình chức năng xác thực trên các thiết bị	Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị thiết bị từ xa	Hạn chế các địa chỉ mạng có kết nối, quản trị thiết bị từ xa
Firewall Fortigate 200D	+	+	+
Switch 01/ Switch Cisco Catalyst 2900-x Series	+	+	+
NAS/Synology RS815+	+	+	+

2. Bảo đảm an toàn máy chủ

2.1. Xác thực

Yêu cầu **Máy chủ**	Thiết lập chính sách xác thực trên máy chủ	Thay đổi các tài khoản mặc định trên hệ thống hoặc vô hiệu hóa	Thiết lập chính sách mật khẩu an toàn (Yêu cầu thay đổi mật khẩu mặc định; Thiết lập quy tắc đặt mật khẩu về số ký tự, loại ký tự; Thiết lập thời gian yêu cầu thay đổi mật khẩu; Thiết lập thời gian mật khẩu hợp lệ.
Server 01/Cài đặt Lotus notes Domino/Vùng Mạng Nội Bộ/HĐH Windows Server 2012	+	+	+

2.2. Kiểm soát truy cập

Yêu cầu **Máy chủ**	Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị máy chủ từ xa	Thiết lập giới hạn thời gian chờ (timeout)
Sàn giao dịch công nghệ/Cài đặt Lotus notes Domino/Vùng Mạng Nội	+	+

Bộ/HĐH Windows Server 2012		

2.3. Nhật ký hệ thống

Yêu cầu	Thiết lập chức năng ghi nhật ký hệ thống trên các máy chủ (thông tin kết nối máy chủ, đăng nhập vào máy chủ, lỗi phát sinh, thay đổi cấu hình máy chủ, thông tin truy cập dữ liệu và dịch vụ trên máy chủ).	Đồng bộ thời gian giữa máy chủ với máy chủ thời gian	Lưu nhật ký hệ thống trong khoảng thời gian tối thiểu 01 tháng
Máy chủ			
Sàn GDCN HY/Cài đặt Lotus notes Domino/Vùng Mạng Nội Bộ/HĐH Windows Server 2012	+	+	+

2.4. Phòng chống xâm nhập

Yêu cầu	Loại bỏ các tài khoản không sử dụng, các tài khoản không còn hợp lệ trên máy chủ	Sử dụng tường lửa của hệ điều hành và hệ thống để cấm các truy cập trái phép tới máy chủ	Vô hiệu hóa các giao thức mạng không an toàn, các dịch vụ hệ thống không sử dụng	Thực hiện nâng cấp, xử lý điểm yếu an toàn thông tin trên máy chủ trước khi đưa vào sử dụng
Máy chủ				
Sàn GDCN HY/Cài đặt Lotus notes Domino/Vùng Mạng Nội Bộ/HĐH Windows Server 2012	+	+	+	+

2.5. Phòng chống phần mềm độc hại

Yêu cầu	Cài đặt phần mềm phòng	Kiểm tra, dò quét, xử lý

Máy chủ	chống mã độc và thiết lập chế độ tự động cập nhật	phần mềm độc hại cho Sàn GDCN HY trước khi cài đặt
Sàn GDCN HY/Cài đặt Lotus notes Domino/Vùng Mạng Nội Bộ/HĐH Windows Server 2012	+	+

2.6. Xử lý máy chủ khi chuyển giao

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Có phương án xóa sạch thông tin, dữ liệu trên máy chủ khi chuyển giao hoặc thay đổi mục đích sử dụng	Chưa có bởi Sàn là độc quyền của Sở Khoa học và Công nghệ tỉnh Hưng Yên, nên không có chuyển giao hoặc thay đổi mục đích sử dụng	Chưa thực hiện nên chưa có phương án xử lý máy chủ khi chuyển giao đáp ứng yêu cầu.

3. Bảo đảm an toàn ứng dụng

3.1. Xác thực

Yêu cầu / **Ứng dụng**	Thiết lập cấu hình ứng dụng để xác thực người sử dụng khi truy cập, quản trị, cấu hình ứng dụng	Lưu trữ có mã hóa thông tin xác thực hệ thống	Thiết lập cấu hình ứng dụng để đảm bảo an toàn mật khẩu người sử dụng (thay đổi mật khẩu mặc định, quy tắc đặt mật khẩu, thời gian yêu cầu thay đổi mật khẩu, thời gian mật khẩu hợp lệ)	Hạn chế số lần đăng nhập sai trong khoảng thời gian nhất định với tài khoản nhất định
Dịch vụ Sàn GDCN HY (nếu cần thiết)	+	+	+	+

3.2. Kiểm soát truy cập

Yêu cầu / **Ứng dụng**	Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị ứng dụng từ xa	Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi	Giới hạn địa chỉ mạng quản trị được phép truy cập,

		ứng dụng không nhận được yêu cầu từ người dùng	quản trị ứng dụng từ xa
Sàn GDCN HY khi kết nối	+	+	+

3.3. Nhật ký hệ thống

Yêu cầu **Ứng dụng**	Ghi nhật ký hệ thống bao gồm những thông tin cơ bản sau: (1) Thông tin truy cập ứng dụng (2) Thông tin đăng nhập khi quản trị ứng dụng (3) Thông tin các lỗi phát sinh trong quá trình hoạt động (4) Thông tin thay đổi cấu hình ứng dụng	Nhật ký hệ thống phải được lưu trữ trong khoảng thời gian tối thiểu là 01 tháng
Sàn GDCN HY khi kết nối	+	+

3.4. An toàn ứng dụng và mã nguồn

Yêu cầu **Ứng dụng**	Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu vào trước khi xử lý
Sàn GDCN HY khi kết nối	+

4. Bảo đảm an toàn dữ liệu

4.1. Bảo mật dữ liệu

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Lưu trữ có mã hóa các thông tin, dữ liệu (không phải là thông tin, dữ liệu công khai) trên hệ thống lưu trữ/phương tiện lưu trữ	Có	Dữ liệu được quản lý an toàn trên hệ thống SAN /SAN SWITCH Cisco catalyst 2900-x series

4.2. Sao lưu dự phòng

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Thực hiện sao lưu dự phòng các thông tin, dữ liệu cơ bản sau: (1) Tập tin cấu hình hệ thống (2) Bản dự phòng hệ điều hành máy chủ (3) Cơ sở dữ liệu (4) Dữ liệu, thông tin nghiệp vụ	Có	Dữ liệu được sao lưu dự phòng, quản lý an toàn trên hệ thống thiết bị mạng NAS/Synology RS815+