BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 1694/BTTTT-CATTT V/v hướng dẫn yêu cầu an toàn thông tin cơ bản đối với hệ thống thông tin kết nối vào mạng TSLCD	*Hà Nội, ngày 31 tháng 5 năm 2019*

Kính gửi:

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

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Nghị định số 17/2017/NĐ-CP ngày 17 tháng 02 năm 2017 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Thông tin và Truyền thông;

Căn cứ Thông tư số 03/2017/TT-BTTTT ngày 24/04/2017 quy định chi tiết và hướng dẫn một số điều của Nghị định 85/2016/NĐ-CP ngày 01/7/2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ;

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

Bộ Thông tin và Truyền thông công bố Tài liệu hướng dẫn về "Yêu cầu an toàn thông tin cơ bản đối với hệ thống thông tin khi kết nối vào Mạng truyền số liệu chuyên dùng". Tài liệu hướng dẫn này đưa ra các yêu cầu an toàn thông tin cơ bản và hướng dẫn cơ quan, tổ chức phương án bảo đảm an toàn thông tin khi kết nối vào mạng TSLCD.

Bản mềm tài liệu hướng dẫn có thể được tải về từ cổng thông tin điện tử của Bộ Thông tin và Truyền thông tại địa chỉ: http://www.mic.gov.vn.

Chi tiết liên hệ:

- Ông Trần Mạnh Thắng, Cục An toàn thông tin, Điện thoại: 0963791366; Thư điện tử: tmthang@mic.gov.vn;

- Ông Nguyễn Phú Dũng, Cục An toàn thông tin, Điện thoại: 0376611700; Thư điện tử: npdung@mic.gov.vn.

Trong quá trình thực hiện, nếu có điều gì vướng mắc, đề nghị các cơ quan, tổ chức phản ánh về Bộ Thông tin và Truyền thông (Cục An toàn thông tin) để được hướng dẫn thực hiện./.

Nơi nhận:
- Như trên;
- Bộ trưởng (để b/c);
- Các Thứ trưởng;
- Cổng Thông tin điện tử Chính phủ;
- Đơn vị chuyên trách về CNTT của các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Đơn vị chuyên trách về CNTT của Văn phòng Trung ương Đảng, Văn phòng Chủ tịch nước, Văn phòng Quốc hội, Tòa án nhân dân tối cao, Viện kiểm sát nhân dân tối cao, Kiểm toán nhà nước;
- Đơn vị chuyên trách về CNTT của Cơ quan Trung ương của các đoàn thể;
- Sở TT&TT các tỉnh, thành phố trực thuộc Trung ương;
- Cổng thông tin điện tử Bộ TT&TT;
- Lưu: VT, CATTT.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Nguyễn Thành Hưng

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

TÀI LIỆU HƯỚNG DẪN

YÊU CẦU AN TOÀN THÔNG TIN CƠ BẢN ĐỐI VỚI HỆ THỐNG THÔNG TIN KHI KẾT NỐI VÀO MẠNG TRUYỀN SỐ LIỆU CHUYÊN DÙNG

(Kèm theo Công văn số 1699/BTTTT-CATTT ngày 31 tháng 5 năm 2019 của Bộ Thông tin và Truyền thông)

Hà Nội, 2019

MỤC 1
PHẠM VI, ĐỐI TƯỢNG ÁP DỤNG

1.1. Phạm vi áp dụng

Tài liệu hướng dẫn này đưa ra các yêu cầu an toàn thông tin cơ bản đối với các hệ thống thông tin khi kết nối trực tiếp vào Mạng truyền số liệu chuyên dùng (TSLCD) của các cơ quan Đảng, Nhà nước.

1.2. Đối tượng áp dụng

Tổ chức, cá nhân tham gia quản lý, vận hành, kết nối và sử dụng mạng TSLCD của các cơ quan Đảng, Nhà nước.

Đơn vị chuyên trách về công nghệ thông tin của các cơ quan Đảng, Nhà nước, Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương.

1.3. Giải thích từ ngữ

a) Mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước là hệ thống thông tin quan trọng quốc gia, được sử dụng riêng trong hoạt động truyền số liệu và ứng dụng công nghệ thông tin của các cơ quan Đảng, Nhà nước (sau đây gọi là mạng truyền số liệu chuyên dùng và viết tắt là "mạng TSLCD") do Cục Bưu điện Trung ương là chủ mạng, quản lý, điều hành hoạt động của mạng.

b) Mạng TSLCD cấp I là phân hệ của mạng TSLCD kết nối tới các thiết bị đầu cuối tại Văn phòng Trung ương Đảng, Văn phòng Chính phủ, Văn phòng Chủ tịch nước, Văn phòng Quốc hội, các Bộ, Ban, Ngành và các cơ quan tương đương trực thuộc Trung ương, Tỉnh ủy/Thành ủy, Hội đồng nhân dân, Ủy ban nhân dân tỉnh, thành phố trực thuộc Trung ương do Cục Bưu điện Trung ương cung cấp, quản lý, vận hành và khai thác.

c) Mạng TSLCD cấp II là phân hệ của mạng TSLCD kết nối tới các thiết bị đầu cuối tại các Sở/Ban/Ngành cấp tỉnh; các cơ quan cấp huyện bao gồm Quận/Huyện/Thị ủy, Hội đồng nhân dân, Ủy ban nhân dân Quận/Huyện; các cơ quan cấp xã bao gồm Đảng ủy xã/phường, các cơ quan tương đương cấp xã/phường do doanh nghiệp viễn thông cung cấp, quản lý, vận hành và khai thác trên địa bàn.

d) Đơn vị sử dụng mạng TSLCD là các cơ quan Đảng, Nhà nước tại Trung ương và địa phương có điểm kết nối vào mạng TSLCD.

đ) Cổng kết nối là hệ thống bao gồm các phần cứng, phần mềm cung cấp chức năng bảo vệ và kết nối hệ thống thông tin của cơ quan, tổ chức với mạng TSLCD. Cổng kết nối có thể là một thiết bị chuyên dụng có tích hợp cung cấp nhiều chức

năng bảo mật khác nhau, ví dụ như thiết bị tường lửa tích hợp hoặc thiết bị định tuyến có tích hợp các chức năng bảo mật.

e) Giải pháp phần cứng chuyên dụng là thiết bị phần cứng được thiết kế để cung cấp một số chức năng chuyên dụng hoặc tích hợp một số tính năng chuyên dụng (Ví dụ: Thiết bị tường lửa hoặc thiết bị tường lửa tích hợp; Thiết bị phòng chống xâm nhập; Thiết bị phòng, chống tấn công từ chối dịch vụ phân tán...).

CHƯƠNG 2
YÊU CẦU AN TOÀN THÔNG TIN CƠ BẢN KHI KẾT NỐI VÀO MẠNG TSLCD

2.1. Yêu cầu chung

Yêu cầu an toàn thông tin đưa ra trong Tài liệu này bao gồm: (1) Yêu cầu an toàn thông tin trong thiết kế Cổng kết nối hệ thống thông tin của cơ quan, tổ chức với mạng TSLCD; (2) Yêu cầu an toàn thông tin trong thiết lập, cấu hình hệ thống; (3) Yêu cầu an toàn thông tin trong kiểm tra, đánh giá an toàn thông tin; (4) Yêu cầu an toàn thông tin trong quản lý vận hành hệ thống.

2.2. Yêu cầu đối với thiết bị tại Cổng kết nối

a) Đối với hệ thống thông tin từ cấp độ 1 đến cấp độ 3 kết nối vào Mạng TSLCD cấp II: Cổng kết nối vào mạng TSLCD có thể sử dụng giải pháp phần cứng, phần mềm hoặc một phần tài nguyên sẵn có của hệ thống hiện tại và đáp ứng các yêu cầu an toàn thông tin theo hướng dẫn này.

b) Đối với hệ thống thông tin từ cấp độ 1 đến cấp độ 3 kết nối vào Mạng TSLCD cấp I: Cổng kết nối sử dụng giải pháp phần cứng chuyên dụng, có thể sử dụng tài nguyên sẵn có của hệ thống hiện tại và đáp ứng các yêu cầu an toàn thông tin theo hướng dẫn này.

c) Đối với hệ thống thông tin cấp độ 4 hoặc cấp độ 5 kết nối vào Mạng TSLCD: Cổng kết nối sử dụng giải pháp phần cứng chuyên dụng, độc lập và đáp ứng các yêu cầu an toàn thông tin theo hướng dẫn này.

d) Mạng của doanh nghiệp viễn thông cung cấp kết nối Mạng TSLCD cấp II: Cổng kết nối vào Mạng TSLCD cấp II sử dụng giải pháp phần cứng chuyên dụng, độc lập và đáp ứng các yêu cầu an toàn thông tin theo hướng dẫn này.

đ) Việc thiết lập cấu hình bảo mật trên các thiết bị tại Cổng kết nối đáp ứng các yêu cầu an toàn thông tin tại Phụ lục kèm theo.

e) Các thiết bị sử dụng tại Cổng kết nối được kiểm tra, đánh giá an toàn thông tin trước khi đưa vào sử dụng và thực hiện định kỳ theo hướng dẫn tại Mục 3.3.4.

2.3. Yêu cầu an toàn thông tin cơ bản khi kết nối vào Mạng TSLCD cấp I

a) Hệ thống khi kết nối vào Mạng TSLCD cấp I đáp ứng các yêu cầu an toàn thông tin cơ bản tương ứng với yêu cầu đối với Mạng TSLCD cấp I tại Phụ lục của hướng dẫn này.

b) Các yêu cầu an toàn thông tin cơ bản đối với hệ thống có kết nối vào Mạng TSLCD cấp I được đánh dấu là "x" và yêu cầu đối với hệ thống thông tin cấp 4 hoặc cấp 5 được đánh dấu là "xx" tại Phụ lục của hướng dẫn này.

2.4. Yêu cầu an toàn thông tin cơ bản khi kết nối vào Mạng TSLCD cấp II

a) Hệ thống khi kết nối vào Mạng TSLCD cấp II đáp ứng các yêu cầu an toàn thông tin cơ bản tương ứng với yêu cầu đối với Mạng TSLCD cấp II tại Phụ lục của hướng dẫn này.

b) Các yêu cầu đối với hệ thống có kết nối vào Mạng TSLCD cấp II được đánh dấu là "x" và đối với hệ thống thông tin cấp 4 hoặc cấp 5 được đánh dấu là "xx" tại Phụ lục của hướng dẫn này.

2.5. Yêu cầu an toàn đối với hệ thống của doanh nghiệp viễn thông cung cấp kết nối Mạng TSLCD cấp II

Hệ thống mạng của doanh nghiệp cung cấp kết nối Mạng TSLCD cấp II khi kết nối vào Mạng TSLCD cấp I đáp ứng các yêu cầu an toàn tương ứng với yêu cầu đối với Mạng DNVT tại Phụ lục của hướng dẫn này.

CHƯƠNG 3
HƯỚNG DẪN BẢO ĐẢM AN TOÀN THÔNG TIN KHI KẾT NỐI VÀO MẠNG TSLCD

3.1. Quy trình kết nối vào mạng TSLCD

3.1.1. Xây dựng phương án kết nối

a) Đơn vị sử dụng thuyết minh về phương án kết nối mạng TSLCD đáp ứng các yêu cầu tại theo các yêu cầu tại điểm b, c và d khoản này trước khi kết nối vào mạng TSLCD.

b) Đối với hệ thống kết nối vào Mạng TSLCD cấp I, đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin (đơn vị chuyên trách về an toàn thông tin), Cục An toàn thông tin (ATTT), Cục Bưu điện Trung ương (BĐTW) đánh giá,

cho ý kiến về mặt chuyên môn đối với phương án bảo đảm an toàn thông tin khi kết nối. Chủ quản hệ thống thông tin căn cứ vào ý kiến chuyên môn của các đơn vị được gửi xin ý kiến ở trên, để phê duyệt phương án trước khi kết nối vào mạng TSLCD.

c) Đối với hệ thống kết nối vào Mạng TSLCD cấp II, đơn vị chuyên trách về an toàn thông tin đánh giá, cho ý kiến về mặt chuyên môn đối với phương án bảo đảm an toàn thông tin khi kết nối. Chủ quản hệ thống thông tin căn cứ vào ý kiến chuyên môn của đơn vị chuyên trách về an toàn thông tin để phê duyệt phương án trước khi kết nối vào mạng TSLCD.

d) Đối với hệ thống mạng của doanh nghiệp cung cấp kết nối Mạng TSLCD cấp II khi kết nối vào Mạng TSLCD cấp I, đơn vị chuyên trách về an toàn thông tin, Cục ATTT, Cục BĐTW đánh giá, cho ý kiến chuyên môn đối với phương án bảo đảm an toàn thông tin khi kết nối. Chủ quản hệ thống thông tin căn cứ vào ý kiến chuyên môn của các đơn vị được gửi xin ý kiến để phê duyệt phương án trước khi kết nối vào mạng TSLCD.

3.1.2. Thực hiện phương án kết nối

a) Đơn vị sử dụng xây dựng kế hoạch và hồ sơ triển khai thực hiện kết nối theo phương án đã được phê duyệt trước khi thực hiện kết nối.

b) Hồ sơ triển khai cung cấp các thông tin về sơ đồ vật lý, sơ đồ logic, thông tin liên hệ của các bên tham gia và phương án triển khai.

c) Kế hoạch và hồ sơ triển khai được thống nhất giữa đơn vị sử dụng, đơn vị đầu mối của Cục BĐTW (kết nối vào Mạng TSLCD cấp I) và đầu mối của doanh nghiệp cung cấp hạ tầng cho Mạng TSLCD cấp II (kết nối vào Mạng TSLCD cấp II).

d) Triển khai kết nối giữa Cổng kết nối với mạng TSLCD theo kế hoạch đã thống nhất tại điểm c mục này. Lưu ý, chỉ thực hiện kết nối Cổng kết nối với mạng TSLCD chưa kết nối hệ thống mạng của cơ quan, tổ chức vào Cổng kết nối tránh việc kết nối làm ảnh hưởng đến hoạt động của cơ quan, tổ chức.

3.1.3. Kiểm thử và đưa vào vận hành khai thác

a) Sau khi kết nối thành công Cổng kết nối vào mạng TSLCD, đơn vị sử dụng chuẩn bị môi trường thử nghiệm và kết nối vào mạng TSLCD.

b) Đơn vị sử dụng và đơn vị đầu mối của Cục BĐTW (kết nối vào Mạng TSLCD cấp I) hoặc doanh nghiệp cung cấp hạ tầng cho Mạng TSLCD cấp II (kết nối vào Mạng TSLCD cấp II) phối hợp kiểm tra, đánh giá hoạt động của môi trường thử nghiệm, các yêu cầu an toàn đã đáp ứng theo phương án được phê duyệt.

c) Trường hợp kết quả đánh giá là đạt thì hai bên có biên bản xác nhận và đưa vào sử dụng.

d) Trường hợp chưa đạt thì hai bên tiếp tục phối hợp, xử lý để hoàn thiện theo phương án phê duyệt.

3.2. Trách nhiệm quản lý của các bên

3.2.1. Cục Bưu điện Trung ương

Cục BĐTW có trách nhiệm quản lý và bảo đảm an toàn thông tin đối với hạ tầng Mạng TSLCD cấp I bao gồm: Cổng cung cấp kết nối vào Mạng TSLCD cấp I; Thiết bị trung tâm và kênh kết nối; Hệ thống phục vụ quản lý vận hành và các hệ thống phụ trợ khác phục vụ bảo đảm an toàn thông tin cho Mạng TSLCD cấp I.

3.2.2. Cục An toàn thông tin

Cục ATTT có trách nhiệm phối hợp thẩm định phương án bảo đảm an toàn thông tin khi kết nối Mạng TSLCD, hỗ trợ các đơn vị trong việc triển khai giám sát bảo đảm an toàn thông tin mạng.

3.2.3. Cơ quan, tổ chức có hệ thống thông tin kết nối vào mạng TSLCD

Cơ quan, tổ chức có hệ thống thông tin kết nối vào mạng TSLCD có trách nhiệm quản lý và bảo đảm an toàn thông tin đối với hệ thống thông tin của mình và Cổng kết nối vào mạng TSLCD. Có trách nhiệm quản lý truy nhập, giám sát và ngăn chặn nguy cơ mất an toàn thông tin từ hệ thống mạng của mình vào mạng TSLCD và các mạng bên ngoài.

3.2.4. Doanh nghiệp viễn thông cung cấp kết nối Mạng TSLCD cấp II

Doanh nghiệp viễn thông cung cấp kết nối Mạng TSLCD cấp II có trách nhiệm quản lý và bảo đảm an toàn thông tin đối với hạ tầng Mạng TSLCD cấp II bao gồm: Cổng cung cấp kết nối vào Mạng TSLCD cấp I; Thiết bị trung tâm và kênh kết nối; hệ thống phục vụ quản lý vận hành và các hệ thống phụ trợ khác phục vụ bảo đảm an toàn thông tin cho hệ thống cung cấp kết nối Mạng TSLCD cấp II.

3.3. Quản lý vận hành hệ thống

3.3.1. Xây dựng ban hành quy định về kết nối và sử dụng mạng TSLCD

a) Đơn vị có hệ thống thông tin kết nối vào mạng TSLCD căn cứ vào các yêu cầu an toàn theo quy định của pháp luật và tại Tài liệu hướng dẫn này xây dựng quy định về việc kết nối và sử dụng mạng TSLCD, trình chủ quản hệ thống thông tin ban hành.

b) Nội dung quy định áp dụng cho đối tượng là cán bộ quản lý vận hành và người sử dụng trong hệ thống.

c) Thực hiện công bố, phổ biến quy định cho các đối tượng tại khoản 2 Điều này khi quy định này được ban hành.

3.3.2. Đầu mối phối hợp trong công tác bảo đảm an toàn thông tin

a) Đơn vị sử dụng và đơn vị cung cấp kết nối mạng TSLCD cung cấp đầu mối phối hợp trong quá trình thiết lập, quản lý vận hành hệ thống.

b) Chỉ định đầu mối phối hợp với Trung tâm Giám sát an toàn không gian mạng quốc gia – Cục An toàn thông tin trong công tác bảo đảm an toàn thông tin cho hệ thống.

c) Thiết lập kênh liên lạc, chia sẻ thông tin giữa các bên tại khoản 2 Điều này, bảo đảm tính kịp thời và an toàn.

3.3.3. Triển khai phương án giám sát an toàn thông tin

a) Đơn vị sử dụng và doanh nghiệp cung cấp kết nối Mạng TSLCD cấp II thực hiện giám sát an toàn hệ thống thông tin, bao gồm và không giới hạn ở các hoạt động: (1) Giám sát hoạt động của hệ thống để có được thông tin trạng thái hoạt động của hệ thống về hiệu năng, trạng thái tăng/giảm (Up/Down), băng thông kết nối; (2) Giám sát an toàn thông tin để phát hiện và cảnh báo sớm tấn công mạng và các nguy cơ mất an toàn thông tin.

b) Đơn vị sử dụng hệ thống thông tin cấp độ 3 trở lên và doanh nghiệp cung cấp kết nối Mạng TSLCD cấp II ban hành các quy định về giám sát an toàn thông tin bao gồm nhưng không giới hạn các nội dung như: Quản lý vận hành hoạt động bình thường của hệ thống giám sát; Đối tượng giám sát bao gồm; Kết nối và gửi nhật ký hệ thống; Truy cập và quản trị hệ thống giám sát; Loại thông tin cần được giám sát; Lưu trữ và bảo vệ thông tin giám sát; Theo dõi, giám sát và cảnh báo sự cố; Bố trí nguồn lực và tổ chức giám sát.

c) Nội dung, phương thức, hệ thống kỹ thuật phục vụ công tác giám sát, cơ quan, tổ chức thực hiện theo quy định tại Điều 5 Thông tư số 31/2017/TT-BTTTT.

d) Thực hiện kết nối, chia sẻ thông tin giám sát thường xuyên với Trung tâm Giám sát an toàn không gian mạng quốc gia – Cục An toàn thông tin.

3.3.4. Kiểm tra đánh giá an toàn thông tin

a) Đơn vị sử dụng và doanh nghiệp cung cấp kết nối Mạng TSLCD cấp II định kỳ hoặc đột xuất theo yêu cầu của cơ quan nhà nước có thẩm quyền thực hiện kiểm tra, đánh giá an toàn thông tin cho Cổng kết nối vào mạng TSLCD.

b) Nội dung, phương án kiểm tra đánh giá an toàn thông tin thực hiện theo quy định tại Điều 13 Thông tư số 03/2017/TT-BTTTT ngày 24/04/2017 quy định chi tiết và hướng dẫn một số điều của Nghị định 85/2016/NĐ-CP ngày 01/7/2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ.

c) Kết quả kiểm tra, đánh giá được báo cáo tới cơ quan có thẩm quyền theo quy định tại chương IV Thông tư số 03/2017/TT-BTTTT.

3.3.5. Xây dựng phương án ứng cứu sự cố an toàn thông tin mạng

a) Đơn vị sử dụng và doanh nghiệp cung cấp kết nối Mạng TSLCD cấp II xây dựng phương án ứng cứu sự cố an toàn thông tin mạng nhằm tăng cường sự chủ động trong việc xử lý sự cố và khôi phục hệ thống sau sự cố.

b) Phương án ứng cứu sự cố an toàn thông tin mạng bao gồm nhưng không giới hạn các nội dung : Phân nhóm sự cố an toàn thông tin; Phương án tiếp nhận, phát hiện, phân loại và xử lý thông tin; Kế hoạch, phương án ứng phó sự cố an toàn thông tin theo quy định tại Quyết định 05/2017/QĐ-TTg; Giám sát, phát hiện và cảnh báo sự cố an toàn thông tin; Quy trình ứng cứu sự cố an toàn thông tin thông thường và sự cố an toàn thông tin nghiêm trọng; Cơ chế phối hợp trong việc xử lý, khắc phục sự cố an toàn thông tin; Diễn tập phương án xử lý sự cố an toàn thông tin.

PHỤ LỤC
YÊU CẦU AN TOÀN KHI KẾT NỐI VÀO MẠNG TSLCD

Yêu cầu an toàn	Mạng TSLCD cấp II	Mạng TSDLCD cấp I	Mạng DNVT
I. Yêu cầu về thiết kế			
1. Hệ thống mạng của cơ quan, tổ chức không được kết nối trực tiếp với mạng TSLCD mà phải thông qua cổng kết nối.	x	x	x
2. Có thiết bị chuyên dụng được sử dụng làm cổng kết nối, để quản lý truy cập giữa mạng của cơ quan, tổ chức vào mạng TSLCD .	x	x	x
3. Cổng kết nối có các chức năng cho phép triển khai các dịch vụ quy định tại Điều 5 Thông tư 27/2017/TT-BTTTT.	x	x	x
4. Cổng kết nối có chức năng phòng chống mã độc trên môi trường Mạng	xx	xx	x
5. Có phương án phòng chống xâm nhập	xx	x	x
6. Có thiết bị chuyên dụng có chức năng phòng chống tấn công từ chối dịch vụ.	xx	xx	x
7. Các thiết bị tại Cổng kết nối được thiết kế cân bằng tải và dự phòng nóng.	xx	xx	x
8. Kết nối mạng phải có kết nối dự phòng vật lý.	xx	xx	x

Yêu cầu an toàn	Mạng TSLCD cấp II	Mạng TSDLCD cấp I	Mạng DNVT
II. Yêu cầu về thiết lập hệ thống			
2.1. Thiết lập chính sách truy cập từ bên ngoài mạng			
1. Cổng kết nối phải được cấu hình chỉ cho phép truy cập từ bên ngoài các dịch vụ mà hệ thống mạng của cơ quan, tổ chức cung cấp; 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.	x	x	x
2. Cổng kết nối phải được thiết lập cấu hình giới hạn số lượng kết nối đồng thời từ một địa chỉ nguồn và tổng số lượng kết nối đồng thời cho từng ứng dụng, dịch vụ được hệ thống cung cấp theo năng lực thực tế của hệ thống.	xx	xx	x
2.2. Thiết lập chính sách truy cập từ bên trong mạng			
1. Cổng kết nối phải được thiết lập cấu hình chỉ cho phép các dải địa chỉ IP nguồn của cơ quan, tổ chức kết nối ra bên ngoài.	x	x	x
2. Cổng kết nối phải được thiết lập cấu hình 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.	xx	x	
2.3. Nhật ký hệ thống			
1. Thiết lập chức năng ghi, lưu trữ nhật ký hệ thống trên các thiết bị hệ thống.	x	x	x

Yêu cầu an toàn	Mạng TSLCD cấp II	Mạng TSDLCD cấp I	Mạng DNVT
2. Sử dụng máy chủ thời gian trong hệ thống để đồng bộ thời gian giữa các thiết bị mạng, thiết bị đầu cuối và các thành phần khác trong hệ thống tham gia hoạt động giám sát.	xx	xx	x
3. Lưu trữ và quản lý tập trung nhật ký hệ thống thu thập được từ các thiết bị hệ thống.	xx	x	x
4. Lưu trữ nhật ký hệ thống của thiết bị tối thiểu 03 tháng.	x		
5. Lưu trữ nhật ký hệ thống của thiết bị tối thiểu 06 tháng.		x	
6. Lưu trữ nhật ký hệ thống của thiết bị tối thiểu 12 tháng.	xx	xx	x
2.4. Phòng chống xâm nhập			
1. Thiết lập chức năng phòng, chống xâm nhập để giám sát và bảo vệ các tấn công mạng từ mạng của cơ quan, tổ chức vào mạng TSLCD và từ các mạng từ phía mạng TSLCD đi vào mạng của cơ quan, tổ chức.	xx	x	x
2. Sự kiện ghi nhận được trên thiết bị phòng chống xâm nhập được kết nối, chia sẻ với hệ thống của Trung tâm Giám sát an toàn không gian mạng quốc gia.	xx	x	x
2.5.Phòng chống phần mềm độc hại trên môi trường mạng			
1. Thiết lập chức năng phòng, chống mã độc trên môi trường mạng để giám sát và bảo vệ	xx	x	x

Yêu cầu an toàn	Mạng TSLCD cấp II	Mạng TSDLCD cấp I	Mạng DNVT
các tấn công mạng từ mạng của cơ quan, tổ chức vào mạng TSLCD và từ các mạng từ phía mạng TSLCD đi vào mạng của cơ quan, tổ chức.			
2. Sự kiện ghi nhận được trên thiết bị phòng, chống mã độc trên môi trường mạng được kết nối, chia sẻ với hệ thống Giám sát an toàn không gian mạng quốc gia của Cục An toàn thông tin.	xx	x	x
2.6. Thiết lập chính sách bảo mật cho thiết bị hệ thống			
1. Thiết bị hệ thống phải được cấu hình chức năng xác thực người dùng khi quản trị thiết bị trực tiếp hoặc từ xa.	x	x	x
2. Thiết lập cấu hình chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị thiết bị từ xa.	x	x	x
3. Không cho phép quản trị, cấu hình thiết bị trực tiếp từ các mạng bên ngoài, trường hợp bắt buộc phải quản trị thiết bị từ xa phải thực hiện gián tiếp thông qua các máy quản trị trong hệ thống và sử dụng kết nối mạng an toàn.	x	x	x
4. Hạn chế được số lần đăng nhập sai khi quản trị hoặc kết nối quản trị từ xa theo địa chỉ mạng.	xx	xx	x
5. Phân quyền truy cập, quản trị thiết bị đối với các tài khoản quản trị có quyền hạn khác nhau.	xx	xx	x

Yêu cầu an toàn	Mạng TSLCD cấp II	Mạng TSDLCD cấp I	Mạng DNVT
6. Cấu hình tối ưu, tăng cường bảo mật cho hệ thống thiết bị hệ thống trước khi đưa vào sử dụng, tối thiểu đáp ứng các yêu cầu tại Mục II hướng dẫn này.	xx	x	x
III. Kiểm tra, đánh giá			
1. Định kỳ 12 tháng thực hiện kiểm tra, đánh giá an toàn thông tin cho thiết bị hệ thống phục vụ kết nối hệ thống với mạng TSLCD.	x		
2. Định kỳ 06 tháng thực hiện kiểm tra, đánh giá an toàn thông tin cho thiết bị hệ thống phục vụ kết nối hệ thống với mạng TSLCD.		x	x
3. Thiết bị hệ thống phải được kiểm tra thiết lập cấu hình an toàn thông tin đáp ứng các yêu cầu tại Mục II phụ lục này, trước khi đưa vào sử dụng.	x	x	x
4. Thiết bị hệ thống phải được kiểm tra, đánh giá và xử lý điểm yếu an toàn thông tin trước khi đưa vào sử dụng.	xx	x	x
IV. Quản lý vận hành			
4.1. Quản lý an toàn mạng			
1. Xây dựng chính sách/quy trình thực hiện quản lý an toàn hạ tầng mạng đáp ứng yêu cầu tại mục 6.1.5.1 TCVN:11930.	x		
2. Xây dựng chính sách/quy trình thực hiện quản lý an toàn hạ tầng mạng đáp	xx	x	x

Yêu cầu an toàn	Mạng TSLCD cấp II	Mạng TSDLCD cấp I	Mạng DNVT
ứng yêu cầu tại mục 7.1.5.1 TCVN:11930.			
3. Xây dựng chính sách/quy trình thực hiện quản lý an toàn hạ tầng mạng đáp ứng yêu cầu tại mục 9.1.5.1 TCVN:11930.	XX	XX	
4.2. Quản lý an toàn thiết bị đầu cuối			
1. Xây dựng chính sách/quy trình thực hiện quản lý an toàn thiết bị đầu cuối đáp ứng yêu cầu tại mục 7.1.5.4 TCVN:11930.	X		
2. Xây dựng chính sách/quy trình thực hiện quản lý an toàn thiết bị đầu cuối đáp ứng yêu cầu tại mục 8.1.5.4 TCVN:11930.	XX	X	
3. Xây dựng chính sách/quy trình thực hiện quản lý an toàn thiết bị đầu cuối đáp ứng yêu cầu tại mục 9.1.5.1 TCVN:11930.	XX	XX	
4.3. Quản lý phòng chống phần mềm độc hại			
1. Xây dựng chính sách/quy trình thực hiện quản lý phòng chống phần mềm độc hại đáp ứng yêu cầu tại mục 7.1.5.5 TCVN:11930.	X		
2. Xây dựng chính sách/quy trình thực hiện quản lý phòng chống phần mềm độc hại đáp ứng yêu cầu tại mục 9.1.5.5 TCVN:11930.	XX	XX	

Yêu cầu an toàn	Mạng TSLCD cấp II	Mạng TSDLCD cấp I	Mạng DNVT
4.4. Quản lý giám sát an toàn hệ thống thông tin			
1. Xây dựng chính sách/quy trình thực hiện quản lý giám sát an toàn hệ thống thông tin đáp ứng yêu cầu tại mục 7.1.5.6 TCVN:11930.	x		x
2. Xây dựng chính sách/quy trình thực hiện quản lý giám sát an toàn hệ thống thông tin đáp ứng yêu cầu tại mục 7.1.5.1 TCVN:11930.	xx	xx	xx
4.5. Quản lý Quản lý điểm yếu an toàn thông tin			
1. Xây dựng chính sách/quy trình thực hiện quản lý điểm yếu an toàn thông tin ứng yêu cầu tại mục 7.1.5.7 TCVN:11930.	xx	x	x
2. Xây dựng chính sách/quy trình thực hiện quản lý điểm yếu an toàn thông tin đáp ứng yêu cầu tại mục 9.1.5.7 TCVN:11930.	xx	xx	xx
4.6. Quản lý sự cố an toàn thông tin			
1. Xây dựng chính sách/quy trình thực hiện quản lý điểm yếu an toàn thông tin ứng yêu cầu tại mục 6.1.5.4 TCVN:11930.	x		
2. Xây dựng chính sách/quy trình thực hiện quản lý điểm yếu an toàn thông tin ứng yêu cầu tại mục 7.1.5.8 TCVN:11930.	xx	x	x

Yêu cầu an toàn	Mạng TSLCD cấp II	Mạng TSDLCD cấp I	Mạng DNVT
3. Xây dựng chính sách/quy trình thực hiện quản lý điểm yếu an toàn thông tin đáp ứng yêu cầu tại mục 9.1.5.8 TCVN:11930.	xx	xx	xx
4.7. Quản lý an toàn người sử dụng đầu cuối			
1. Xây dựng chính sách/quy trình thực hiện quản lý người sử dụng đầu cuối đáp ứng yêu cầu tại mục 6.1.5.5 TCVN:11930.	x		
2. Xây dựng chính sách/quy trình thực hiện quản lý người sử dụng đầu cuối đáp ứng yêu cầu tại mục 7.1.5.7 TCVN:11930.	xx	x	
3. Xây dựng chính sách/quy trình thực hiện quản lý người sử dụng đầu cuối đáp ứng yêu cầu tại mục 9.1.5.9 TCVN:11930.	xx	xx	