BỘ KẾ HOẠCH VÀ ĐẦU TƯ
TỔNG CỤC THỐNG KÊ

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

Số: 630 /QĐ-TCTK

Hà Nội, ngày 13 tháng 6 năm 2022

QUYẾT ĐỊNH

Ban hành Quy chế quản lý thiết bị công nghệ thông tin và bảo đảm an toàn, an ninh mạng của Tổng cục Thống kê

TỔNG CỤC TRƯỞNG TỔNG CỤC THỐNG KÊ

Căn cứ Luật Công nghệ thông tin ngày 29 tháng 6 năm 2006;

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

Căn cứ Luật An ninh mạng ngày 12 tháng 6 năm 2018;

Căn cứ Nghị định số 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 Quyết định số 10/2020/QĐ-TTg ngày 18 tháng 3 năm 2020 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Tổng cục Thống kê thuộc Bộ Kế hoạch và Đầu tư;

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 2017 của Thủ tướng Chính phủ ban hành Quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

Căn cứ Chỉ thị số 14/CT-TTg ngày 25 tháng 5 năm 2018 của Thủ tướng Chính phủ về việc nâng cao năng lực phòng, chống phần mềm độc hại;

Căn cứ Chỉ thị số 14/CT-TTg ngày 07 tháng 6 năm 2019 của Thủ tướng Chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam;

Căn cứ Quyết định số 1709/QĐ-BKHĐT ngày 24 tháng 12 năm 2021 của Bộ trưởng Bộ Kế hoạch và Đầu tư ban hành Quy chế bảo đảm an toàn thông tin, an ninh mạng máy tính của Bộ Kế hoạch và Đầu tư;

Căn cứ Thông tư số 03/2017/TT-BTTTT ngày 24 tháng 4 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của 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 Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 của Bộ Thông tin và Truyền thông về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc;

Căn cứ Thông tư số 31/2017/TT-BTTTT ngày 15 tháng 11 năm 2017 của Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin;

Theo đề nghị của Cục trưởng Cục Thu thập dữ liệu và Ứng dụng công nghệ thông tin thống kê.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế quản lý thiết bị công nghệ thông tin và bảo đảm an toàn, an ninh mạng của Tổng cục Thống kê.

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày ký.

Điều 3. Cục trưởng Cục Thu thập dữ liệu và Ứng dụng công nghệ thông tin thống kê, Vụ trưởng Vụ Tổ chức cán bộ, Chánh Văn phòng Tổng cục Thống kê, Vụ trưởng Vụ Kế hoạch tài chính, Thủ trưởng các đơn vị thuộc Tổng cục Thống kê chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như điều 3;
- Lãnh đạo Tổng cục;
- Đảng uỷ, Công đoàn cơ quan;
- Lưu: VT, TTDL(05).

KT. TỔNG CỤC TRƯỞNG
PHÓ TỔNG CỤC TRƯỞNG

Nguyễn Trung Tiến

BỘ KẾ HOẠCH VÀ ĐẦU TƯ
TỔNG CỤC THỐNG KÊ

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

QUY CHẾ

Quản lý thiết bị công nghệ thông tin và bảo đảm an toàn, an ninh mạng của Tổng cục Thống kê

(Ban hành kèm theo Quyết định số 630 /QĐ-TCTK ngày 13 / 6 /2022 của Tổng cục trưởng Tổng cục Thống kê)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh, đối tượng áp dụng

1. Phạm vi điều chỉnh: Quy chế này quy định về quản lý thiết bị công nghệ thông tin và bảo đảm an toàn, an ninh mạng của Tổng cục Thống kê.

2. Đối tượng áp dụng

a) Các đơn vị thuộc Tổng cục Thống kê;

b) Công chức, viên chức, người lao động trong ngành Thống kê;

c) Cơ quan, tổ chức, cá nhân có kết nối vào hệ thống mạng của Tổng cục Thống kê;

d) Cơ quan, tổ chức, cá nhân cung cấp dịch vụ công nghệ thông tin và an toàn thông tin mạng (viết gọn là đối tác công nghệ thông tin) cho các đơn vị thuộc Tổng cục Thống kê.

Điều 2. Giải thích thuật ngữ

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

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

2. *Dữ liệu quan trọng* là dữ liệu có thông tin mật; thông tin lưu hành nội bộ của đơn vị hoặc do đơn vị quản lý, nếu lộ lọt ra ngoài sẽ gây ảnh hưởng xấu đến danh tiếng, tài chính và hoạt động của đơn vị; *Hệ thống thông tin quan trọng* (mục b) khoản 2 Điều 9) là hệ thống thông tin có chứa dữ liệu quan trọng.

3. *Thiết bị công nghệ thông tin* bao gồm các thiết bị được Tổng cục Thống kê thực hiện trang bị và mua sắm: máy chủ, thiết bị mạng, thiết bị phục vụ phòng

máy chủ, máy tính để bàn, máy tính xách tay, máy tính bảng.

4. *Hệ thống thông tin* là tập hợp phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên mạng (Theo quy định tại khoản 3 Điều 3 Luật an toàn thông tin mạng 2015).

5. *Người dùng* là người được cấp quyền sử dụng thiết bị công nghệ thông tin (sau đây viết gọn là CNTT), hệ thống thống thông tin theo một vai trò cụ thể để thực hiện các nhiệm vụ của mình.

6. *Người quản trị* là công chức, viên chức, người lao động được giao nhiệm vụ quản trị, vận hành hệ thống CNTT (bao gồm trang thiết bị phần cứng, phần mềm hệ thống, phần mềm ứng dụng, cơ sở dữ liệu, hệ thống mạng, hệ thống an toàn bảo mật,...).

7. *Tài khoản AD nội bộ* là tài khoản thuộc hệ quản trị định danh và xác thực (Active Directory) đồng thời là tài khoản thư điện tử của Tổng cục Thống kê và được cấp phát, quản lý tập trung.

8. *Hệ thống mạng* (còn được gọi là *Mạng máy tính*) là một hệ thống bao gồm ít nhất 2 thiết bị được kết nối với nhau thông qua internet. Mục đích là nhằm chia sẻ thông tin và trao đổi dữ liệu giữa các thiết bị trong cùng hệ thống.

9. *Đơn vị quản lý nhà nước về công nghệ thông tin* (còn được gọi là *đơn vị quản lý hệ thống thông tin*) là đơn vị chuyên trách về công nghệ thông tin của cơ quan, đơn vị hoặc đơn vị chuyên trách về công nghệ thông tin của chủ quản hệ thống thông tin do chủ quản hệ thống thông tin chỉ định. Tại Tổng cục Thống kê, *Đơn vị quản lý nhà nước về công nghệ thông tin* là Cục Thu thập dữ liệu và Ứng dụng công nghệ thông tin thống kê.

10. *Đơn vị vận hành hệ thống* là cơ quan, tổ chức được chủ quản hệ thống thông tin giao nhiệm vụ vận hành hệ thống thông tin. Tại Tổng cục Thống kê, *Đơn vị vận hành hệ thống* là Cục Thu thập dữ liệu và Ứng dụng công nghệ thông tin thống kê (Trung tâm tin học thống kê khu vực I, II, III). Tại Cục Thống kê, *Đơn vị vận hành hệ thống* là Phòng có biên chế chuyên trách công nghệ thông tin.

11. *Đơn vị chuyên trách về an toàn thông tin* là đơn vị có chức năng, nhiệm vụ bảo đảm an toàn thông tin, có trách nhiệm thực thi nhiệm vụ bảo đảm an toàn thông tin và ứng cứu sự cố an toàn thông tin mạng. Tại Tổng cục Thống kê, *Đơn vị chuyên trách về an toàn thông tin* là Cục Thu thập dữ liệu và Ứng dụng công nghệ thông tin thống kê. Tại Cục Thống kê, *Đơn vị chuyên trách về an toàn thông tin* là Phòng có biên chế chuyên trách công nghệ thông tin.

Điều 3. Nguyên tắc bảo đảm an toàn, an ninh thông tin mạng

1. Bảo đảm an toàn, an ninh thông tin mạng là yêu cầu bắt buộc, thường xuyên, liên tục, có tính xuyên suốt quá trình thiết kế, xây dựng, vận hành, nâng cấp, hủy bỏ hệ thống thông tin. Bảo đảm an toàn, an ninh thông tin mạng tuân thủ các nguyên tắc chung quy định tại Điều 4 Luật An toàn thông tin mạng và Điều 4

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.

2. Công chức, viên chức và người lao động trong các đơn vị thuộc Tổng cục Thống kê có trách nhiệm bảo đảm an toàn, an ninh thông tin mạng trong phạm vi xử lý công việc của mình theo quy định của Nhà nước và của Quy chế này.

3. Xử lý sự cố an toàn thông tin mạng phải phù hợp với trách nhiệm, quyền hạn và bảo đảm lợi ích hợp pháp của cơ quan, đơn vị, cá nhân liên quan và theo quy định của pháp luật.

Điều 4. Các hành vi bị nghiêm cấm

1. Các hành vi bị nghiêm cấm quy định tại Điều 12 Luật Công nghệ thông tin, Điều 7 Luật An toàn thông tin mạng và Điều 8 Luật An ninh mạng.

2. Tự ý đấu nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập mạng không dây của cá nhân vào mạng nội bộ khi chưa có sự hướng dẫn hoặc đồng ý của đơn vị quản lý hệ thống thông tin.

3. Thay đổi, gỡ bỏ biện pháp an toàn thông tin cài đặt trên thiết bị CNTT phục vụ công việc, thay thế, lắp mới, tráo đổi thành phần của máy vi tính phục vụ công việc khi chưa có sự hướng dẫn hoặc đồng ý của đơn vị quản lý hệ thống thông tin.

4. Tạo ra, cài đặt, phát tán phần mềm độc hại gây ảnh hưởng đến hoạt động của hệ thống thông tin.

5. Cản trở hoạt động cung cấp dịch vụ của hệ thống thông tin; ngăn chặn việc truy cập đến thông tin của cơ quan, cá nhân khác trên môi trường mạng, trừ trường hợp pháp luật cho phép.

6. Trộm cắp, sử dụng mật khẩu, khóa mật mã và thông tin của cơ quan, cá nhân khác trên môi trường mạng.

7. Không sử dụng thiết bị lưu trữ, ổ cứng di động, USB kết nối vào máy tính của Ngành khi chưa dò, quét bằng phần mềm phòng chống mã độc (phần mềm diệt virus).

8. Cung cấp, đăng tải, truyền đưa thông tin có nội dung quy định tại các khoản 1, 2, 3, 4 và 5 Điều 16 của Luật An ninh mạng năm 2018 và thông tin khác có nội dung xâm phạm an ninh quốc gia trên Trang thông tin điện tử, cổng thông tin điện tử hoặc chuyên trang trên mạng xã hội của đơn vị, tổ chức, cá nhân.

9. Các hành vi khác làm mất an toàn, bí mật thông tin của cơ quan, cá nhân khác được trao đổi, truyền đưa, lưu trữ trên môi trường mạng.

Chương II
QUẢN LÝ THIẾT BỊ CÔNG NGHỆ THÔNG TIN

Điều 5. Quy định chung về quản lý thiết bị công nghệ thông tin

1. Thiết bị CNTT được quản lý, vận hành theo thiết kế hệ thống đã được phê duyệt của Tổng cục Thống kê và nội quy vận hành (nếu có). Các thiết bị như máy chủ, thiết bị mạng, thiết bị lưu trữ chỉ được bổ sung, sửa chữa, thay đổi chức năng theo phê duyệt của cấp có thẩm quyền.

2. Xử lý khi phát sinh sự cố thiết bị

a) Trường hợp thiết bị còn thời gian bảo hành: đơn vị quản lý, vận hành yêu cầu đơn vị cung cấp sửa chữa khắc phục sự cố;

b) Trường hợp thiết bị đã hết thời gian bảo hành: đơn vị quản lý, vận hành thực hiện khắc phục đối với những thiết bị đã được giao thực hiện trong kế hoạch công nghệ thông tin hằng năm; xây dựng phương án sửa chữa thay thế, khắc phục sự cố với thiết bị chưa được giao trong kế hoạch công nghệ thông tin hằng năm trình cấp có thẩm quyền phê duyệt;

c) Thiết bị công nghệ thông tin có lưu trữ dữ liệu của Ngành khi thay đổi mục đích sử dụng hoặc thanh lý, đơn vị sử dụng phải tổ chức sao lưu và thực hiện xóa, tiêu hủy dữ liệu trên thiết bị.

3. Khi mang thiết bị CNTT ra ngoài trụ sở làm việc phải được sự đồng ý bằng văn bản của Lãnh đạo đơn vị quản lý, sử dụng thiết bị trừ trường hợp khẩn cấp như thiên tai, hoả hoạn.

4. Thiết bị CNTT phải được đơn vị chuyên trách về an toàn, an ninh của đơn vị chủ quản hệ thống thông tin kiểm tra, đánh giá yêu cầu kỹ thuật về đảm bảo an toàn thông tin trước khi mua sắm đầu tư hoặc thuê dịch vụ;

5. Hằng năm đơn vị quản lý hệ thống thông tin xây dựng kế hoạch bảo trì thiết bị CNTT trình cấp có thẩm quyền phê duyệt;

6. Đơn vị vận hành hệ thống thông tin thực hiện báo cáo tình hình sử dụng thiết bị CNTT hàng năm theo hướng dẫn của đơn vị chuyên trách về công nghệ thông tin.

Điều 6. Quản lý, vận hành máy chủ

1. Vị trí đặt máy chủ

a) Máy chủ tại Trung tâm máy chủ/trung tâm dữ liệu phải được đặt trong môi trường vật lý bảo đảm theo quy định về an toàn, an ninh tại Điều 12 Quy chế này;

b) Máy chủ tại các Cục Thống kê tỉnh, thành phố trực thuộc Trung ương (viết tắt là Cục Thống kê), đơn vị sự nghiệp thuộc Tổng cục Thống kê phải được đặt trong môi trường bảo đảm tiêu chuẩn kỹ thuật của Phòng máy chủ quy định

tại Điều 12 Quy chế này.

2. Phần mềm trên máy chủ

a) Phần mềm cài đặt trên máy chủ phải có trong thiết kế hệ thống, hoặc được sự phê duyệt của đơn vị quản lý hệ thống thông tin và đơn vị vận hành hệ thống thông tin;

b) Máy chủ phải được cài đặt phần mềm phòng chống mã độc có bản quyền và được quản lý thống nhất, tập trung.

3. Vận hành máy chủ

Đơn vị được giao nhiệm vụ vận hành máy chủ, thực hiện:

a) Giám sát máy chủ vận hành thông suốt, liên tục 24/7;

b) Xây dựng và tổ chức thực hiện kế hoạch bảo trì máy chủ không ảnh hưởng đến quá trình vận hành hệ thống;

c) Thực hiện quy định về bảo đảm an toàn, an ninh mạng, ghi nhật ký vận hành máy chủ, cập nhật hệ điều hành;

d) Thiết lập chế độ sao lưu dữ liệu định kỳ.

Điều 7. Quản lý, sử dụng máy vi tính

1. Thiết lập thông tin máy vi tính

a) Máy vi tính kết nối vào mạng nội bộ của Tổng cục Thống kê phải thực hiện kết nối hệ thống định danh (join domain) của Tổng cục Thống kê, đặt tên theo quy định tại điểm b khoản này;

b) Máy vi tính được đặt tên theo quy tắc: <tên viết tắt đơn vị><-><họ tên viết tắt>; tên viết tắt đặt theo quy định tại Điều 5 Quy chế quản lý, sử dụng thư điện tử của Tổng cục Thống kê do Tổng cục trưởng ban hành theo Quyết định số 1103/QĐ-TCTK ngày 25 tháng 11 năm 2021. Trường hợp cá nhân có nhiều hơn 01 máy vi tính, sử dụng số thứ tự ở cuối tên để đặt tên máy vi tính;

c) Đơn vị vận hành hệ thống thông tin có trách nhiệm hỗ trợ người dùng thực hiện điểm a, b khoản này.

2. Quy định về sử dụng máy vi tính

a) Người sử dụng máy vi tính không được tự ý: thay đổi các cài đặt mà đơn vị chuyên trách đã cài; gỡ bỏ phần mềm phòng chống virus; thay đổi hiện trạng cấu hình của máy vi tính khi chưa được sự đồng ý của đơn vị (bộ phận) chuyên trách về an toàn, an ninh mạng;

b) Người sử dụng máy vi tính có trách nhiệm bảo quản, sử dụng đúng mục đích;

c) Kịp thời báo cáo với cán bộ phụ trách về CNTT của đơn vị khi máy vi tính gặp sự cố.

Điều 8. Thiết bị mạng và thiết bị phát sóng không dây (Wifi)

1. Thiết bị mạng, hệ thống lưu trữ

a) Vị trí đặt thiết bị mạng, hệ thống lưu trữ

Thiết bị mạng, hệ thống lưu trữ được đặt trong môi trường vật lý theo tiêu chuẩn Phòng máy chủ hoặc Trung tâm máy chủ/trung tâm dữ liệu được quy định tại Điều 12 Quy chế này.

b) Vận hành thiết bị mạng, hệ thống lưu trữ

Thiết bị mạng, hệ thống lưu trữ được vận hành theo tiêu chuẩn được khuyến cáo của nhà sản xuất, bảo đảm vận hành thông suốt liên tục 24/7, giám sát theo quy định về giám sát an toàn, an ninh mạng của Tổng cục Thống kê tại Điều 19 Quy chế này;

Tất cả các cài đặt, cấu hình ứng dụng, chính sách về định tuyến, bảo mật đều phải có trong thiết kế hệ thống, có sự cho phép của đơn vị quản lý;

Trường hợp cần thay đổi, phải báo cáo đơn vị chuyên trách an toàn, an ninh mạng của Tổng cục Thống kê và phải thực hiện sao lưu cấu hình của thiết bị mạng;

Tất cả thiết bị lưu trữ di động chỉ được kết nối vào hệ thống mạng Tổng cục Thống kê khi có sự kiểm tra, giám sát của đơn vị chuyên trách về an toàn, an ninh mạng của Tổng cục Thống kê.

2. Thiết bị phát sóng không dây (Wifi)

a) Khuyến khích các đơn vị triển khai đồng bộ thiết bị phát sóng không dây (Wifi) tập trung, thiết lập tài khoản người dùng theo 2 đối tượng: (i) người dùng sử dụng tài khoản AD nội bộ được truy cập mạng nội bộ; (ii) người dùng bên ngoài không được truy cập mạng nội bộ (chỉ kết nối Internet);

b) Đơn vị chưa triển khai thiết bị phát sóng không dây (Wifi) tập trung, sử dụng thiết bị phát sóng không dây (Wifi) có thiết lập chế độ xác thực tài khoản, không kết nối vào mạng nội bộ;

c) Không tự ý lắp đặt các thiết bị phát sóng không dây (Wifi) không rõ nguồn gốc gây nguy cơ mất an toàn, an ninh mạng.

Chương III

QUY ĐỊNH BẢO ĐẢM AN TOÀN, AN NINH THÔNG TIN

Điều 9. Bảo đảm an toàn thông tin trong việc quản lý công chức, viên chức và người lao động

1. Phân công nhiệm vụ

a) Xác định trách nhiệm trong việc bảo đảm an toàn thông tin mạng của vị

trí phân công công việc;

b) Đảm bảo người được phân công làm việc tại các vị trí có tiếp xúc với thông tin, dữ liệu quan trọng phải qua bước đánh giá, thẩm tra nhân thân và lý lịch tư pháp;

c) Yêu cầu người được phân công quản lý dữ liệu quan trọng hoặc quản lý thông tin hệ thống bảo mật phải cam kết bảo mật thông tin bằng văn bản riêng hoặc cam kết trong hợp đồng làm việc, hợp đồng lao động, bao gồm các điều khoản về trách nhiệm của cá nhân sau khi thôi việc tại đơn vị.

2. Sử dụng nguồn nhân lực

Các đơn vị có trách nhiệm:

a) Sau khi tuyển dụng, tiếp nhận nhân sự mới, đơn vị phải có trách nhiệm phổ biến cho nhân sự mới các quy định về bảo đảm an toàn, an ninh thông tin tại đơn vị; đối với các vị trí tiếp xúc, quản lý các thông tin, dữ liệu quan trọng hoặc quản trị các hệ thống thông tin quan trọng, đơn vị phải yêu cầu nhân sự mới cam kết bảo mật thông tin bằng văn bản hoặc cam kết trong hợp đồng làm việc, hợp đồng lao động;

b) Có biện pháp quản lý tài khoản người dùng của công chức, viên chức và người lao động trên các hệ thống thông tin quan trọng;

c) Thường xuyên rà soát, kiểm tra quyền truy cập vào các hệ thống thông tin đối với tất cả công chức, viên chức và người lao động đảm bảo quyền truy cập phù hợp với nhiệm vụ được giao;

d) Phải thường xuyên tổ chức quán triệt các quy định về an toàn, an ninh thông tin, nhằm nâng cao nhận thức về trách nhiệm bảo đảm an toàn, an ninh thông tin của từng cá nhân trong đơn vị;

đ) Thực hiện đúng quy trình cấp mới, quản lý và thu hồi tài khoản, phân quyền truy cập các hệ thống thông tin và tất cả các tài sản liên quan đến hệ thống thông tin đối với các cá nhân do đơn vị quản lý.

3. Chấm dứt hoặc thay đổi công việc

Khi công chức, viên chức và người lao động chấm dứt hoặc thay đổi công việc, cơ quan, đơn vị phải:

a) Xác định rõ trách nhiệm của công chức, viên chức, người lao động và các bên liên quan trong quản lý, sử dụng các tài sản công nghệ thông tin được giao;

b) Lập biên bản bàn giao tài sản công nghệ thông tin;

c) Thay đổi hoặc thu hồi quyền truy cập các hệ thống thông tin.

Điều 10. Xác định cấp độ và phương án bảo đảm an toàn hệ thống thông tin

1. Việc xác định cấp độ hệ thống thông tin và xây dựng phương án bảo vệ

hệ thống thông tin theo cấp độ phục vụ mục đích đánh giá an toàn thông tin và bảo đảm an toàn thông tin cho các hệ thống thông tin. Nguyên tắc bảo đảm an toàn thông tin theo cấp độ và nguyên tắc xác định cấp độ căn cứ trên các nguyên tắc quy định tại Điều 4, Điều 5 Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về việc bảo đảm an toàn an toàn hệ thống thông tin theo cấp độ.

2. Thẩm quyền xác định cấp độ an toàn hệ thống thông tin

a) Đơn vị chủ trì triển khai hệ thống thông tin lập hồ sơ đề xuất cấp độ an toàn hệ thống thông tin do Tổng cục Thống kê quản lý, vận hành;

b) Thẩm quyền thẩm định và phê duyệt hồ sơ cấp độ hệ thống thông tin theo quy định của Bộ Thông tin và Truyền thông.

3. Trình tự, thủ tục xác định cấp độ hệ thống thông tin

a) Nội dung của hồ sơ đề xuất cấp độ hệ thống thông tin theo quy định tại Điều 15 Nghị định 85/2016/NĐ-CP;

b) Trình tự, thủ tục xác định cấp độ hệ thống thông tin theo quy định tại Điều 13, Điều 14 Nghị định 85/2016/NĐ-CP và hướng dẫn của Bộ Thông tin và Truyền thông.

4. Phương án bảo đảm an toàn hệ thống thông tin

a) Đơn vị chuyên trách về an toàn thông tin tổ chức triển khai phương án bảo đảm an toàn hệ thống thông tin sau khi hồ sơ đề xuất cấp độ hoặc phương án bảo đảm an toàn hệ thống thông tin được phê duyệt;

b) Đơn vị quản lý nhà nước về công nghệ thông tin xây dựng kế hoạch và tổ chức giám sát việc triển khai các phương án bảo đảm an toàn hệ thống thông tin đã được phê duyệt.

Điều 11. Bảo đảm an toàn, an ninh thông tin đối với hệ thống mạng

1. Hệ thống mạng nội bộ (LAN), hệ thống mạng diện rộng (WAN)

a) Hệ thống mạng LAN phải được thiết kế phân vùng theo chức năng cơ bản, tuân thủ Kiến trúc hạ tầng mạng của Tổng cục Thống kê, bao gồm: vùng mạng người dùng; vùng mạng kết nối hệ thống ra bên ngoài Internet và các mạng khác; vùng mạng máy chủ công cộng; vùng mạng máy chủ nội bộ; vùng mạng máy chủ cơ sở dữ liệu, vùng mạng máy chủ quản trị. Dữ liệu trao đổi giữa các vùng mạng phải được quản lý, giám sát bởi hệ thống các thiết bị mạng, thiết bị bảo mật;

b) Các đơn vị sử dụng hệ thống mạng WAN của Tổng cục Thống kê có trách nhiệm bảo đảm an toàn thông tin đối với hệ thống mạng nội bộ và các thiết bị của mình khi thực hiện kết nối vào mạng WAN; Thông báo sự cố hoặc các hành vi phá hoại, xâm nhập về đơn vị quản lý CNTT của Tổng cục Thống kê để xử lý;

c) Sao lưu cấu hình thiết bị kết nối mạng LAN, mạng WAN khi có thay đổi.

2. Máy vi tính kết nối mạng

a) Phải được thiết lập phương thức xác thực an toàn;

b) Phải được cài đặt phần mềm phòng chống mã độc tập trung do đơn vị chuyên trách về an toàn, an ninh thông tin triển khai;

c) Phải được cấu hình nhằm vô hiệu hóa tính năng tự động thực thi (autoplay) các tệp tin trên các thiết bị lưu trữ di động;

d) Truy cập mạng, ứng dụng nội bộ từ Internet phải thực hiện xác thực đa yếu tố hoặc qua mạng riêng ảo VPN.

Điều 12. Bảo đảm an toàn, an ninh thông tin tại Trung tâm máy chủ/trung tâm dữ liệu, Phòng máy chủ

1. Các thiết bị kết nối mạng, thiết bị bảo mật quan trọng như tường lửa, thiết bị định tuyến, hệ thống máy chủ, hệ thống lưu trữ... phải được đặt trong Trung tâm máy chủ/trung tâm dữ liệu và phải được thiết lập cơ chế bảo vệ, theo dõi phát hiện xâm nhập và biện pháp kiểm soát truy cập, kết nối vật lý phù hợp với từng khu vực: máy chủ và hệ thống lưu trữ; tủ mạng và đầu nối; thiết bị nguồn điện và dự phòng điện khẩn cấp; vận hành, kiểm soát, quản trị hệ thống.

2. Trung tâm máy chủ/trung tâm dữ liệu phải được trang bị hệ thống lưu điện đủ công suất và duy trì thời gian hoạt động của các máy chủ khi có sự cố mất điện; hệ thống làm mát điều hòa không khí, độ ẩm để bảo đảm môi trường vận hành; hệ thống cảnh báo cháy, hệ thống chữa cháy tự động, thiết bị phòng cháy, chữa cháy khẩn cấp; hệ thống cảnh báo hệ thống nguồn điện; hệ thống chống sét lan truyền. Các hệ thống này phải được thiết lập chế độ cảnh báo phù hợp. Môi trường vật lý Trung tâm máy chủ/trung tâm dữ liệu bảo đảm tuân theo tiêu chuẩn quốc gia TCVN 9250:2021 về Trung tâm máy chủ – yêu cầu hạ tầng kỹ thuật viễn thông.

3. Phòng máy chủ phải được trang bị hệ thống lưu điện, hệ thống làm mát điều hòa không khí, bình cứu hỏa. Khuyến khích trang bị môi trường vật lý Phòng máy chủ theo tiêu chuẩn quốc gia TCVN 9250:2021.

4. Chỉ những cá nhân có quyền, nhiệm vụ theo quy định của thủ trưởng đơn vị được giao quản lý Trung tâm máy chủ/trung tâm dữ liệu được phép vào, ra Trung tâm máy chủ. Việc vào, ra Trung tâm máy chủ/trung tâm dữ liệu phải được kiểm soát bằng thiết bị bảo vệ (quẹt thẻ, vân tay, sinh trắc học, ...).

5. Đối với phần mềm thương mại tại Trung tâm máy chủ/trung tâm dữ liệu yêu cầu phải có bản quyền.

6. Toàn bộ thiết bị trong Trung tâm máy chủ/trung tâm dữ liệu phải được lắp đặt, cài đặt, cấu hình theo thiết kế được phê duyệt, được bảo trì, bảo dưỡng định kỳ để bảo đảm tính ổn định, sẵn sàng, an toàn trong vận hành.

7. Các vùng mạng, máy chủ trong Trung tâm máy chủ/trung tâm dữ liệu phải được kiểm soát bởi tường lửa, các thiết bị, phầm mềm bảo mật. Mọi truy cập vào

ra giữa các vùng mạng, máy chủ phải có hệ thống theo dõi, giám sát và phát hiện xâm nhập.

8. Các máy chủ phải được cài đặt phần mềm phòng chống mã độc và được quản lý thống nhất, tập trung.

9. Đơn vị vận hành hệ thống thông tin có trách nhiệm xây dựng nội quy hoặc hướng dẫn làm việc khu vực này, bao gồm các nội dung chính: quản lý việc mang thiết bị vào, ra Trung tâm máy chủ/trung tâm dữ liệu; sổ nhật ký ghi quá trình vào, ra Trung tâm máy chủ/trung tâm dữ liệu; quy định mang thiết bị vào, ra Trung tâm máy chủ/trung tâm dữ liệu; quy định các công việc định kỳ thực hiện.

Điều 13. Quản lý tài khoản truy cập

1. Tài khoản quản trị hệ thống (mạng máy tính, hệ điều hành, thiết bị kết nối mạng, phần mềm, ứng dụng, cơ sở dữ liệu, hệ thống thông tin) thiết lập tách biệt với tài khoản truy cập của người sử dụng thông thường. Tài khoản hệ thống được giao đích danh cá nhân làm công tác quản trị.

2. Tài khoản người dùng

a) Mỗi công chức, viên chức, người lao động ngành Thống kê được cấp một tài khoản AD nội bộ;

b) Tài khoản nội bộ được xác thực khi truy cập máy vi tính, truy cập khai thác tài nguyên mạng LAN, mạng WAN và các phần mềm nội bộ. Đối với những phần mềm ứng dụng chưa cấu hình sử dụng tài khoản AD nội bộ, tài khoản được khuyến khích đặt tên trùng nhưng khác mật khẩu với tài khoản AD nội bộ;

c) Đối với những tài khoản của người ngoài Ngành Thống kê (tài khoản Guest đối với khách đến làm việc tại cơ quan Tổng cục; tài khoản đối tác đang trong quá trình triển khai công việc; tài khoản điều tra viên,...) không được kết nối trực tiếp vào hệ thống mạng nội bộ;

d) Việc đăng ký mới, thay đổi, thu hồi tài khoản AD nội bộ thực hiện theo Điều 7 Quy chế quản lý, sử dụng thư điện tử của Tổng cục Thống kê do Tổng cục trưởng ban hành theo Quyết định số 1103/QĐ-TCTK ngày 25 tháng 11 năm 2021.

3. Mật khẩu tài khoản truy cập hệ thống thông tin, mạng máy tính phải thực hiện theo khoản 1, Điều 6 Quy chế quản lý, sử dụng thư điện tử của Tổng cục Thống kê do Tổng cục trưởng ban hành ngày 25 tháng 11 năm 2021.

4. Đơn vị chuyên trách về an toàn, an ninh thông tin mạng thực hiện đóng quyền truy cập của tài khoản truy cập hệ thống thông tin trong trường hợp:

a) Đóng tạm thời khi phát hiện tài khoản thực hiện các hành vi tấn công hoặc để xảy ra vấn đề mất an toàn, an ninh thông tin mạng;

b) Đóng vĩnh viễn với những tài khoản nội bộ thực hiện theo Điều 8 Quy chế quản lý, sử dụng thư điện tử của Tổng cục Thống kê do Tổng cục trưởng ban hành ngày 25 tháng 11 năm 2021; những tài khoản khác khi hoàn thành

nhiệm vụ.

Điều 14. Bảo đảm an toàn, an ninh thông tin đối với việc xây dựng, nâng cấp và sử dụng phần mềm ứng dụng

1. Yêu cầu về bảo đảm an toàn, an ninh thông tin phải được đưa vào tất cả các công đoạn thiết kế, xây dựng, triển khai và vận hành, sử dụng phần mềm ứng dụng.

2. Phần mềm ứng dụng phải đáp ứng các yêu cầu sau: phần mềm nội bộ mới đưa vào sử dụng thực hiện xác thực tài khoản quy định tại mục a) khoản 2 Điều 13; giới hạn số lần đăng nhập sai liên tiếp tối đa là 15 lần; giới hạn thời gian để chờ đóng phiên kết nối; mã hóa thông tin xác thực trên hệ thống; không được để chế độ đăng nhập tự động.

3. Phần mềm ứng dụng phải được kiểm tra phát hiện và khắc phục các điểm yếu về an toàn, an ninh thông tin mạng trước khi đưa vào sử dụng. Đơn vị chủ trì xây dựng phần mềm thực hiện cập nhật, khắc phục các điểm yếu bảo mật khi phát hiện trong quá trình sử dụng.

4. Cá nhân chỉ sử dụng phần mềm do bộ phận chuyên trách về công nghệ thông tin của đơn vị cài đặt trên máy tính, thiết bị kết nối mạng máy tính được cấp; không được tự ý thay đổi các phần mềm theo quy định tại điểm a khoản 2 Điều 7.

5. Thiết lập, phân quyền truy cập, quản trị, sử dụng tài nguyên khác nhau của phần mềm ứng dụng với người sử dụng/nhóm người sử dụng có chức năng, yêu cầu nghiệp vụ khác nhau; đóng các cổng giao tiếp không sử dụng.

6. Chỉ cho phép sử dụng các giao thức mạng có hỗ trợ chức năng mã hóa thông tin (SSH, SSL, VPN hoặc tương đương) khi truy cập, quản trị phần mềm, ứng dụng từ xa trên môi trường mạng; phải đặt mã nguồn trong môi trường an toàn do bộ phận chuyên trách công nghệ thông tin quản lý.

7. Các ứng dụng dùng chung, hệ thống thông tin, cơ sở dữ liệu trước khi nâng cấp, sửa chữa, bảo trì, xử lý sự cố phải thực hiện sao lưu.

8. Thường xuyên cập nhật, vá lỗi bảo mật phần mềm, ứng dụng trên các máy chủ, máy vi tính cá nhân, thiết bị kết nối mạng đang hoạt động thuộc hệ thống mạng nội bộ.

9. Phần mềm ứng dụng chuyên ngành cài đặt trên máy chủ phải được duy trì trong mạng nội bộ tối thiểu 05 năm tính từ lần xây dựng, nâng cấp cuối cùng.

Điều 15. Bảo đảm an toàn, an ninh thông tin đối với dữ liệu

1. Đơn vị vận hành hệ thống thông tin phải thiết lập phương án bảo đảm tính bí mật, nguyên vẹn và khả dụng của thông tin, dữ liệu; mã hóa thông tin, dữ liệu khi lưu trữ trên hệ thống/thiết bị lưu trữ dữ liệu di động.

2. Tập tin cấu hình hệ thống, ảnh sao lưu hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ phải được sao lưu dự phòng định kỳ và lưu trữ độc lập với hệ thống lưu trữ trên các máy chủ dịch vụ.

3. Mỗi đơn vị cần bố trí máy vi tính, máy in riêng không kết nối mạng, đặt mật khẩu, mã hóa dữ liệu và các biện pháp bảo mật khác bảo đảm an toàn, an ninh thông tin để soạn thảo tài liệu mật.

4. Các đơn vị thuộc Tổng cục Thống kê phải thường xuyên kiểm tra, giám sát các hoạt động chia sẻ, gửi, nhận thông tin, dữ liệu trong hoạt động nội bộ của mình; việc chia sẻ, gửi, nhận thông tin trên môi trường mạng cần phải sử dụng mật khẩu để bảo vệ thông tin.

5. Đối với hoạt động trao đổi thông tin, dữ liệu với bên ngoài, tập thể cá nhân thực hiện trao đổi thông tin, dữ liệu ra bên ngoài phải có biện pháp bảo mật thông tin, dữ liệu được trao đổi. Giao dịch trực tuyến phải được truyền đầy đủ, đúng địa chỉ, tránh bị sửa đổi, tiết lộ hoặc nhân bản một cách trái phép; sử dụng các cơ chế xác thực mạnh, sử dụng các giao thức truyền thông an toàn.

Điều 16. Bảo đảm an toàn, an ninh thông tin khi tiếp nhận, phát triển, vận hành và bảo trì hệ thống thông tin

1. Khi thực hiện nâng cấp, mở rộng, thay thế một phần hệ thống thông tin, đơn vị vận hành hệ thống thông tin phải rà soát cấp độ, phương án bảo đảm an toàn của hệ thống thông tin và thực hiện điều chỉnh, bổ sung hoặc thay mới hồ sơ đề xuất cấp độ trong trường hợp cần thiết; triển khai phương án bảo đảm an toàn hệ thống thông tin đáp ứng yêu cầu cơ bản trong tiêu chuẩn, quy chuẩn kỹ thuật về bảo đảm an toàn hệ thống thông tin theo cấp độ.

2. Khi tiếp nhận, phát triển, nâng cấp, bảo trì hệ thống thông tin, đơn vị vận hành hệ thống thông tin phải tiến hành phân tích, xác định rủi ro có thể xảy ra, đánh giá phạm vi tác động và phải chuẩn bị các biện pháp hạn chế, loại trừ các rủi ro này và yêu cầu các bên cung cấp, thi công, các cá nhân liên quan thực hiện.

3. Đơn vị tiếp nhận hệ thống thông tin phải thực hiện công tác bảo đảm an toàn, an ninh thông tin mạng, tránh lộ, lọt mã nguồn và dữ liệu, tài liệu thiết kế, quản trị hệ thống mà đối tác đang xử lý ra bên ngoài khi xây dựng, nâng cấp.

Điều 17. Phòng chống mã độc

1. Trách nhiệm của các đơn vị quản lý nhà nước về CNTT trong việc bảo vệ chống lại mã độc:

a) Xây dựng, quản lý, theo dõi các giải pháp phòng chống mã độc và đảm bảo các giải pháp này vận hành liên tục;

b) Theo dõi và phát hiện sớm nguồn phát tán mã độc để kịp thời xử lý. Báo cáo lãnh đạo Tổng cục Thống kê khi các giải pháp phòng chống mã độc không hoạt động hoặc hoạt động không đúng chức năng và khi xảy ra sự cố liên quan đến mã độc;

c) Chủ trì, phối hợp với các đơn vị có liên quan trong việc xử lý các sự cố liên quan đến mã độc.

2. Trách nhiệm của các đơn vị vận hành hệ thống mạng máy tính trong việc bảo vệ chống lại mã độc:

a) Triển khai các giải pháp phòng chống mã độc; cài đặt chương trình tìm, phát hiện, diệt mã độc trong hệ thống mạng máy tính thuộc TCTK;

b) Tiếp nhận thông báo về sự cố liên quan đến mã độc từ các đơn vị; Xác định nguyên nhân và đề ra biện pháp xử lý mã độc;

c) Thực hiện các biện pháp xử lý sự cố liên quan đến mã độc trên máy trạm và máy chủ;

d) Khôi phục hoạt động hệ thống sau khi xử lý sự cố liên quan đến mã độc.

3. Trách nhiệm của công chức, viên chức, người lao động trong việc bảo vệ chống lại mã độc:

a) Không được sử dụng phần mềm trái phép;

b) Không lưu trữ dữ liệu, dữ liệu quan trọng của cơ quan trên các thiết bị di động thông minh (điện thoại thông minh Smartphone, máy tính bảng, thiết bị thu phát media...);

c) Không mang các thiết bị di động thông minh vào các cuộc họp có nội dung bí mật, hạn chế đến mức thấp nhất việc sử dụng các thiết bị di động thông minh và dịch vụ trực tuyến của cá nhân tại nơi làm việc, thực hiện theo khoản 2 Điều 6 Nghị định số 26/2020/NĐ-CP của Chính phủ ban hành ngày 28 tháng 02 năm 2020 về việc Quy định chi tiết một số điều của Luật bảo vệ bí mật nhà nước;

d) Không mở tệp hoặc truy cập đường dẫn có nghi ngờ chứa mã độc; không cố mở hoặc thực hiện các tệp, phần mềm đã bị các phần mềm phòng chống mã độc khóa hoặc cảnh báo. Trong trường hợp cần thiết, đề nghị bộ phận kỹ thuật hỗ trợ thực hiện;

đ) Để chế độ tự động kiểm tra, quét phát hiện mã độc trên các chương trình quét mã độc để quét máy tính và các phương tiện xử lý thông tin để phát hiện, ngăn chặn mã độc. Hàng tuần kiểm tra sự hoạt động của chương trình quét mã độc.

Điều 18. Quản lý sao lưu dự phòng và ghi nhật ký hoạt động của hệ thống thông tin

1. Quản lý sao lưu dự phòng (Backup)

Chủ quản hệ thống thông tin hoặc đơn vị được ủy quyền quản lý trực tiếp hệ thống thông tin thực hiện quản lý sao lưu dự phòng bảo đảm an toàn dữ liệu sau:

a) Lập danh sách hệ thống thông tin theo mức độ quan trọng cần được sao lưu, kèm theo thời gian lưu trữ, định kỳ sao lưu, phương pháp sao lưu và thời gian kiểm tra phục hồi hệ thống từ dữ liệu sao lưu;

b) Dữ liệu của các hệ thống thông tin từ mức độ 2 trở lên phải có phương án tự động sao lưu phù hợp với tần suất thay đổi của dữ liệu và bảo đảm nguyên tắc dữ liệu phát sinh phải được sao lưu trong vòng 24 giờ. Dữ liệu sao lưu phải được lưu trữ ra phương tiện lưu trữ ngoài (như đĩa quang, ổ cứng di động hoặc phương tiện lưu trữ khác) và cất giữ, bảo quản an toàn tách rời với khu vực lắp đặt hệ thống thông tin nguồn;

c) Đối với hệ thống thông tin từ mức độ 2 trở lên phải kiểm tra, phục hồi dữ liệu sao lưu từ phương tiện lưu trữ ngoài tối thiểu 3 (ba) tháng một lần.

2. Ghi nhật ký hoạt động (Log) của hệ thống thông tin

Chủ quản hệ thống thông tin hoặc đơn vị được ủy quyền quản lý trực tiếp hệ thống thông tin thực hiện ghi nhật ký hoạt động của hệ thống thông tin như sau:

a) Thực hiện ghi nhật ký và lưu trữ nhật ký về hoạt động của hệ thống thông tin và người sử dụng, các lỗi phát sinh, các sự cố an toàn thông tin. Dữ liệu nhật ký của các hệ thống thông tin từ mức độ 2 trở lên phải được lưu trữ trực tuyến tối thiểu 3 tháng theo hình thức tập trung và sao lưu tối thiểu một năm;

b) Bảo vệ các chức năng ghi nhật ký và thông tin nhật ký, chống giả mạo và truy cập trái phép; bảo đảm người quản trị hệ thống và người sử dụng không thể xóa hay sửa đổi nhật ký hệ thống ghi lại các hoạt động của chính họ;

c) Thực hiện việc đồng bộ thời gian giữa các hệ thống thông tin.

Điều 19. Giám sát, kiểm tra đánh giá an toàn hệ thống

1. Giám sát an toàn thông tin mạng

a) Đơn vị chuyên trách về an toàn thông tin của Tổng cục Thống kê chủ trì tổ chức giám sát an ninh mạng theo quy định;

b) Các hệ thống thông tin bắt buộc phải có chức năng ghi và lưu trữ nhật ký về hoạt động của hệ thống và người sử dụng hệ thống thông tin. Thực hiện việc bảo vệ các chức năng ghi nhật ký và thông tin nhật ký, chống giả mạo, sửa đổi, phá hủy và truy cập trái phép;

c) Nguyên tắc, yêu cầu, nội dung, phương thức, hệ thống kỹ thuật phục vụ công tác giám sát thực hiện theo quy định tại Thông tư số 31/2017/TT-BTTTT ngày 15 tháng 11 năm 2017 của Bộ Thông tin và Truyền thông về Quy định hoạt động giám sát an toàn hệ thống thông tin và theo quy định tại Điều 12 Quy chế bảo đảm an toàn thông tin, an ninh mạng máy tính của Bộ Kế hoạch và Đầu tư ban hành ngày 24 tháng 12 năm 2021;

d) Đơn vị chuyên trách về an toàn thông tin làm đầu mối giám sát an toàn thông tin mạng để tiếp nhận cảnh báo, cung cấp, trao đổi, chia sẻ thông tin với các đơn vị có liên quan.

2. Kiểm tra, đánh giá an toàn thông tin

a) Nội dung kiểm tra, đánh giá:

- Kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn, an ninh thông tin theo cấp độ;

- Đánh giá hiệu quả của biện pháp bảo đảm an toàn, an ninh hệ thống thông tin;

- Đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống;

- Kiểm tra, đánh giá khác do đơn vị vận hành hệ thống thông tin quy định.

b) Hình thức kiểm tra, đánh giá:

- Kiểm tra, đánh giá định kỳ theo kế hoạch của đơn vị vận hành hệ thống thông tin; Kiểm tra thực hiện định kỳ theo phương án bảo đảm an toàn hệ thống thông tin theo cấp độ đã được phê duyệt của đơn vị chuyên trách an toàn, an ninh thông tin, theo khoản 2 Điều 20 Nghị định số: 85/2016/NĐ-CP của Chính Phủ ban hành ngày 01 tháng 7 năm 2016 về việc bảo đảm an toàn hệ thống thông tin theo cấp độ;

- Kiểm tra, đánh giá đột xuất theo yêu cầu của cấp có thẩm quyền;

- Hình thức thực hiện: Tự thực hiện hoặc thuê dịch vụ.

Điều 20. Ứng cứu sự cố an toàn thông tin mạng

1. Các đơn vị, cá nhân khi phát hiện dấu hiệu tấn công hoặc sự cố an toàn, an ninh thông tin mạng cần nhanh chóng báo cho Đơn vị chuyên trách về an toàn thông tin.

2. Khi xảy ra sự cố an toàn, an ninh thông tin mạng thuộc loại hình tấn công mạng, đơn vị vận hành hệ thống thông tin thực hiện báo cáo Đơn vị chuyên trách về an toàn, an ninh thông tin của Tổng cục Thống kê để khắc phục, xử lý kịp thời.

3. Đơn vị chuyên trách về an toàn an ninh mạng xây dựng kịch bản và tổ chức thực hiện ứng cứu sự cố an toàn thông tin mạng theo quy định tại Thông tư số 20/2017/TTBTTT ngày 12 tháng 9 năm 2017 của Bộ Thông tin và Truyền thông về Quy định điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc.

4. Đơn vị chuyên trách về an toàn, an ninh thông tin chủ trì, phối hợp với các đơn vị thuộc TCTK tham gia các cuộc diễn tập quốc gia, quốc tế do Cơ quan điều phối quốc gia, Bộ Thông tin và Truyền thông tổ chức và tổ chức diễn tập ứng cứu sự cố trong phạm vi Tổng cục Thống kê theo tần suất quy định tại điểm b Nhiệm vụ 4 mục II Điều 1 Quyết định số 1622/QĐ-TTg ngày 25/10/2017 của Thủ tướng Chính phủ về việc đẩy mạnh hoạt động của mạng lưới ứng cứu sự cố, tăng cường năng lực cho các cán bộ, bộ phận chuyên trách ứng cứu sự cố an toàn thông tin mạng trên toàn quốc đến năm 2020, định hướng đến 2025.

Điều 21. Đào tạo, bồi dưỡng nghiệp vụ, tuyên truyền, phổ biến nâng cao nhận thức về an toàn, an ninh mạng

1. Vụ Tổ chức cán bộ phối hợp với Cục Thu thập dữ liệu và Ứng dụng công nghệ thông tin thống kê định kỳ rà soát, xây dựng trình lãnh đạo Tổng cục phê duyệt kế hoạch bồi dưỡng nghiệp vụ an toàn, an ninh thông tin cho công chức, viên chức và người lao động của Tổng cục Thống kê.

2. Các đơn vị thuộc Tổng cục Thống kê

a) Tổ chức đào tạo, bồi dưỡng nghiệp vụ về an toàn thông tin cho cán bộ công nghệ thông tin, cán bộ chuyên trách an toàn thông tin mạng và đào tạo cơ bản về an toàn thông tin cho cán bộ quản lý, người sử dụng hệ thống thông tin thuộc đơn vị ngoài các chương trình đào tạo của Tổng cục Thống kê;

b) Thường xuyên tổ chức các hoạt động tuyên truyền, phổ biến nâng cao nhận thức về bảo đảm an toàn, an ninh thông tin mạng đến toàn thể công chức, viên chức và người lao động tại đơn vị.

3. Đơn vị chuyên trách về an toàn, an ninh mạng của Tổng cục Thống kê xây dựng kế hoạch tuyên truyền, phổ biến nâng cao nhận thức về an toàn, an ninh thông tin mạng.

Chương IV
TRÁCH NHIỆM CỦA CÁC TỔ CHỨC LIÊN QUAN

Điều 22. Trách nhiệm của các đơn vị thuộc Tổng cục Thống kê

1. Thực hiện đúng các quy định liên quan tại Quy chế này.

2. Thủ trưởng các đơn vị, tổ chức có trách nhiệm phổ biến, quán triệt Quy chế này đến toàn thể công chức, viên chức, người lao động trong đơn vị, nghiêm túc tổ chức thực hiện các quy định tại Quy chế này và chịu trách nhiệm trước Tổng cục trưởng trong công tác bảo đảm an toàn thông tin, an ninh mạng máy tính tại đơn vị mình.

3. Phối hợp, cung cấp thông tin và tạo điều kiện cho đơn vị vận hành hệ thống thông tin triển khai công tác kiểm tra, khắc phục sự cố xảy ra một cách kịp thời, nhanh chóng và đạt hiệu quả.

Điều 23. Trách nhiệm của cá nhân

1. Thực hiện đúng các quy định liên quan tại Quy chế này.

2. Không được tự ý cài đặt các phần mềm trên máy vi tính đã kết nối mạng nội bộ (join domain).

3. Có trách nhiệm bảo mật tài khoản truy cập được cấp, không giao tài khoản, mật khẩu cá nhân cho người khác. Phải tắt máy vi tính trước khi về.

4. Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm mã độc trên máy vi tính (ví dụ: máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống mã độc, mất dữ liệu, ...), người sử dụng phải tắt máy và thông báo trực tiếp cho đơn vị vận hành hệ thống thông tin để được hỗ trợ, xử lý.

5. Thực hiện sao lưu dữ liệu trên máy vi tính.

6. Cá nhân được giao quản lý, vận hành hệ thống, làm nhiệm vụ bảo đảm an toàn, an ninh mạng có trách nhiệm giữ bí mật thông tin về hệ thống thông tin.

Điều 24. Trách nhiệm của Cục Thu thập dữ liệu và Ứng dụng công nghệ thông tin thống kê

1. Thực hiện đúng các quy định liên quan tại Quy chế này.

2. Tham mưu cho Tổng cục trưởng về công tác bảo đảm an toàn thông tin,

an ninh mạng.

3. Thực hiện trách nhiệm của Đơn vị quản lý nhà nước về công nghệ thông tin, Đơn vị chuyên trách về an toàn, an ninh thông tin, Đơn vị vận hành hệ thống của Tổng cục Thống kê, hỗ trợ ứng cứu sự cố hệ thống tại các Cục Thống kê.

4. Tổ chức xây dựng, quản lý vận hành hệ thống mạng, hệ thống giám sát an toàn, an ninh mạng của toàn Ngành Thống kê. Chia sẻ thông tin giám sát an toàn thông tin mạng theo quy định và hướng dẫn của Bộ Kế hoạch và Đầu tư tại Khoản 4 Điều 12 Quy chế bảo đảm an toàn thông tin, an ninh mạng máy tính của Bộ Kế hoạch và Đầu tư ban hành tại Quyết định số 1709/QĐ-BKHĐT ngày 24 tháng 12 năm 2021.

5. Lập kế hoạch, thực hiện kiểm tra, đánh giá an toàn, an ninh thông tin. Chủ trì kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ đối với các đơn vị quản lý, vận hành hệ thống thông tin.

6. Chủ trì phối hợp với các cơ quan quản lý nhà nước trong việc xử lý, ứng cứu sự cố an toàn thông tin, an ninh mạng. Thực hiện nghĩa vụ thành viên của Mạng lưới ứng cứu sự cố an toàn thông tin mạng Bộ Kế hoạch và Đầu tư theo Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 2017 của Thủ tướng Chính phủ về việc ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia.

7. Cấp, hủy tài khoản, quyền truy cập các hệ thống thông tin đối với các cá nhân, đơn vị theo quy định.

8. Xây dựng kê hoạch và tổ chức thực hiện tuyên truyền, phổ biến, tập huấn, nâng cao nhận thức, kỹ năng về an toàn thông tin, an ninh mạng cho cán bộ, công chức, viên chức và người lao động ngành Thống kê.

9. Hằng năm, tổ chức diễn tập ứng cứu sự cố an toàn, an ninh thông tin.

10. Báo cáo cấp có thẩm quyền khi phát hiện hành vi vi phạm pháp luật về an toàn, an ninh mạng.

11. Thông báo cho lực lượng chuyên trách bảo vệ an ninh mạng cấp có thẩm quyền khi phát hiện hành vi vi phạm pháp luật về an ninh mạng sau khi báo cáo và được sự đồng ý của Lãnh đạo Tổng cục.

12. Chủ trì, phối hợp với các đơn vị bảo đảm việc mua sắm tập trung trang thiết bị công nghệ thông tin và các bản quyền phần mềm trong toàn Ngành.

Điều 25. Trách nhiệm của Văn phòng Tổng cục

Phối hợp với Cục Thu thập dữ liệu và Ứng dụng công nghệ thông tin thống kê đảm bảo an toàn, an ninh hệ thống hội nghị trực tuyến và các hệ thống thông tin lĩnh vực văn phòng.

Điều 26. Trách nhiệm của Vụ Tổ chức cán bộ

Phối hợp với Cục Thu thập dữ liệu và Ứng dụng công nghệ thông tin thống kê xây dựng kế hoạch và tổ chức đào tạo, bồi dưỡng nghiệp vụ an toàn, an ninh

thông tin và an toàn, an ninh mạng cho công chức, viên chức và người lao động ngành Thống kê theo Quy chế đào tạo, bồi dưỡng công chức, viên chức Tổng cục Thống kê ban hành ngày 30 tháng 6 năm 2015 của Tổng cục Thống kê.

Điều 27. Trách nhiệm của Vụ Kế hoạch tài chính

1. Căn cứ hồ sơ đề xuất cấp độ an toàn hệ thống thông tin do Tổng cục Thống kê quản lý và vận hành, Vụ Kế hoạch tài chính thực hiện thẩm định dự toán phương án bảo đảm an toàn, an ninh mạng trình Lãnh đạo Tổng cục phê duyệt.

2. Bố trí kinh phí cho các hoạt động bảo đảm an toàn, an ninh mạng của ngành Thống kê phù hợp với dự toán, phân bổ kinh phí Kế hoạch công nghệ thông tin hằng năm của Tổng cục Thống kê.

Chương V
TỔ CHỨC THỰC HIỆN

Điều 28. Khen thưởng và xử lý vi phạm

1. Hằng năm, Cục Thu thập dữ liệu và Ứng dụng công nghệ thông tin thống kê theo dõi, tổng hợp báo cáo các chỉ số an toàn thông tin, an ninh mạng máy tính ngành Thống kê theo quy định tại Điều 20 Quy chế bảo đảm an toàn thông tin, an ninh mạng máy tính của Bộ Kế hoạch và Đầu tư tại Quyết định số 1709/QĐ-BKHĐT ngày 24 tháng 12 năm 2021, để xếp hạng và làm cơ sở để Bộ trưởng Bộ Kế hoạch và Đầu tư khen thưởng theo quy định.

2. Các đơn vị, tổ chức, cá nhân có hành vi vi phạm Quy chế này tùy theo tính chất, mức độ vi phạm mà bị nhắc nhở, xử lý theo quy định của pháp luật hiện hành.

Điều 29. Điều khoản thi hành

1. Cục Thu thập dữ liệu và Ứng dụng công nghệ thông tin thống kê chủ trì, phối hợp với các cơ quan, đơn vị có liên quan tổ chức hướng dẫn, theo dõi và đôn đốc việc thực hiện các quy định của Quy chế này.

2. Trong quá trình thực hiện Quy chế này, nếu có những vấn đề khó khăn, vướng mắc, các đơn vị phản ảnh về Cục Thu thập dữ liệu và Ứng dụng công nghệ thông tin thống kê để tổng hợp, trình Tổng cục trưởng xem xét, quyết định cho phù hợp với điều kiện thực tế và quy định của pháp luật hiện hành./.