CỤC THỐNG KÊ
CHI CỤC THỐNG KÊ TỈNH VĨNH PHÚC

Số: 25 /QĐ-CCTK

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

Vĩnh Phúc, ngày 16 tháng 4 năm 2025

QUYẾT ĐỊNH

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

CHI CỤC TRƯỞNG CHI CỤC THỐNG KÊ TỈNH VĨNH PHÚC

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 Nghị định số 13/2023/NĐ-CP ngày 17 tháng 4 năm 2023 của Chính phủ về bảo vệ dữ liệu cá nhân;

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 630/QĐ-TCTK ngày 13 tháng 6 năm 2022 của Tổng cục Thống kê 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;

Căn cứ Quyết định số 1103/QĐ-TCTK ngày 25 tháng 11 năm 2021 của Tổng cục Thống kê ban hành Quy chế quản lý, sử dụng hệ thống thư điện tử của Tổng cục Thống kê;

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;

Căn cứ Quyết định số 956/QĐ-BTC ngày 05 tháng 3 năm 2025 của Bộ trưởng Bộ Tài chính quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Chi cục Thống kê cấp tỉnh thuộc Cục Thống kê;

Theo đề nghị của Trưởng phòng Thống kê Tổng hợp.

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 thông tin, an ninh mạng của Chi cục Thống kê tỉnh Vĩnh Phúc.

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

Điều 3. Trưởng phòng Thống kê Tổng hợp; Trưởng các phòng tham mưu; Đội trưởng các Đội Thống kê thuộc Chi cục Thống kê và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- LĐ Chi cục;
- Lưu: VT, TKTH.

CHI CỤC TRƯỞNG

CỘNG HÒA X.H.C.N VIỆT NAM
CHI CỤC THỐNG KÊ TỈNH VĨNH PHÚC
CỤC THỐNG KÊ

Nguyễn Hồng Phong

CỤC THỐNG KÊ
CHI CỤC THỐNG KÊ TỈNH VĨNH PHÚC

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 đảm bảo an toàn thông tin, an ninh mạng của Chi cục Thống kê tỉnh Vĩnh Phúc

(Ban hành theo Quyết định số 25/QĐ-CCTK ngày 16 tháng 4 năm 2025 của Chi cục Thống kê tỉnh Vĩnh Phúc)

Chương I
QUI ĐỊNH CHUNG

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

1. Phạm vi điều chỉnh: Quy chế này quy định về việc quản lý, sử dụng trang thiết bị công nghệ thông tin (CNTT) và bảo đảm an toàn thông tin, an ninh mạng (ATTT, ANM) của Chi cục Thống kê tỉnh Vĩnh Phúc.

2. Đối tượng áp dụng

a) Các đơn vị thuộc Chi cục Thống kê tỉnh Vĩnh Phúc;

b) Công chức, người lao động trong ngành Thống kê tỉnh Vĩnh Phúc.

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.

3. *Thiết bị CNTT* bao gồm các thiết bị được cấp trên hoặc địa phương hoặc Chi cục hoặc các đơn vị thuộc Chi cục trang bị hoặc tự trang bị gồm: máy chủ; máy tính để bàn, máy tính xách tay, máy tính bảng, smartphone, smartwatch; máy in, máy quét; thiết bị mạng; thiết bị phục vụ phòng máy chủ...

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. *Hệ thống thông tin quan trọng* là hệ thống thông tin có chứa dữ liệu quan trọng.

5. *Người dùng* là người được cấp quyền sử dụng thiết bị CNTT, hệ thống thông tin theo một vai trò cụ thể để thực hiện các nhiệm vụ được giao.

6. *Người quản trị* là công 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 được Cục Thống kê được cấp phát, quản lý tập trung.

8. *Hệ thống mạng* là một hệ thống 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.

Điều 3. Nguyên tắc bảo đảm ATTT, ANM

1. Bảo đảm ATTT, ANM 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. Tuân thủ các nguyên tắc chung quy định tại Điều 4 Luật ATTT 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 và người lao động trong các đơn vị thuộc Chi cục Thống kê tỉnh Vĩnh Phúc có trách nhiệm bảo đảm ATTT, ANM 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 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 năm 2006; Điều 7 Luật An toàn thông tin mạng năm 2015; Điều 8 Luật An ninh mạng năm 2018; Điều 8 Nghị định số 13/2023/NĐ-CP của Chính phủ về bảo vệ dữ liệu cá nhân và Điều 4 Quy chế Quản lý, sử dụng hệ thống thư điện tử của Tổng cục Thống kê được ban hành theo Quyết định số 1103/QĐ-TCTK.

2. Để lộ lọt, cung cấp, truyền đưa, phổ biến thông tin cá nhân của bản thân; của người thân, người quen hoặc đối tượng cung cấp thông tin cho hoạt động thống kê mà mình có được qua mạng xã hội như Facebook, Zalo, Twitter, Tiktok, Instagram... hoặc cung cấp cho đối tượng khác trái quy định của Luật Thống kê.

3. Cung cấp, truyền đưa, phổ biến thông tin nội bộ, tài liệu quan trọng của cơ quan, tổ chức; chia sẻ dự thảo các văn bản nhạy cảm thuộc lĩnh vực thanh kiểm tra; tổ chức, quản lý cán bộ công chức... qua mạng xã hội như Facebook, Zalo, Twitter, Tiktok, Instagram...

4. Truyền đưa các văn bản, tài liệu thuộc danh mục bí mật của Nhà nước trên môi trường mạng; thông tin ngoài chức năng, nhiệm vụ được phân công; truyền đưa thông tin nhằm địa chỉ người nhận hoặc đến đối tượng không có chức năng, nhiệm vụ liên quan đến thông tin đó; tiết lộ bí mật cá nhân, bí mật

công tác và những thông tin bí mật khác được pháp luật bảo vệ.

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

6. Thay đổi, gỡ bỏ biện pháp bảo đảm ATTT cài trên thiết bị CNTT phục vụ công việc; thay thế, lắp mới, tráo đổi thiết bị của máy tính được cơ quan trang bị khi chưa có sự hướng dẫn hoặc đồng ý của đơn vị quản lý hệ thống thông tin.

7. Các hành động gây ảnh hưởng đến hoạt động của hệ thống thông tin, ATTT, ANM bao gồm:

a) Tạo ra, cài đặt hoặc phát tán virus, phần mềm độc hại;

b) Tải, cài đặt và sử dụng các phần mềm không rõ nguồn gốc, kênh phát hành không chính thống, tính năng, tác dụng không phục vụ yêu cầu công việc;

c) Không cài phần mềm diệt virus Kaspersky do Ngành trang bị;

d) Không thay đổi mật khẩu ban đầu các tài khoản được Ngành cung cấp phục vụ công việc gây ra nguy cơ mất an toàn cho hệ thống;

e) Không nâng cao cảnh giác, thiếu trách nhiệm với hành động like, share, post... tin tức, hình ảnh, âm thanh, bài viết của đối tượng xấu;

f) Vô tình hoặc cố ý không kiểm tra kỹ nguồn gốc thông tin, địa chỉ truy cập để truy cập vào các đường link giả mạo, trang web có địa chỉ không rõ ràng, thiếu lành mạnh, lừa đảo;

g) Buôn bán hàng hóa, dịch vụ, chứng khoán trong giờ làm việc; đánh bài bạc, trò chơi điện tử không lành mạnh trên môi trường mạng; xem các video trên mạng xã hội trong giờ làm việc làm tắc ngẽn đường truyền mạng của Cơ quan;

h) Tạo lập các kênh, tài khoản mạng xã hội không chính danh, sử dụng thông tin đăng ký không chính chủ gây khó khăn cho cơ quan nhà nước trong quá trình quản lý, kiểm tra, xác minh...

8. Phát tán tin rác, thư rác; thông tin có nội dung văn hóa phẩm đồi trụy; chống phá nhà nước, kích động bạo lực và chiến tranh, gây chia rẽ khối đại đoàn kết toàn dân tộc và các đơn thư khiếu nại, tố cáo, bôi nhọ tổ chức, cá nhân, gây chia rẽ nội bộ.

9. Sử dụng thư điện tử công vụ và các tài khoản của Ngành cung cấp để đăng ký các dịch vụ trực tuyến trên Internet cho mục đích cá nhân như: đăng ký tài khoản mạng xã hội, website thương mại, diễn đàn công cộng.

10. Trộm cắp, chiếm đoạt, sử dụng trái phép tài khoản, mật khẩu, khóa mật mã và thông tin của cơ quan, tổ chức, cá nhân khác trên môi trường mạng.

11. Sử dụng thiết bị lưu trữ, ổ cứng di động, USB cắm vào máy tính của Cơ quan khi chưa kiểm tra, quét virus, phần mềm độc hại bằng phần mềm phòng chống virus được Ngành trang bị (Kaspersky).

12. 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 hoặc trang mạng xã hội của đơn vị, tổ chức, cá nhân.

13. 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 CNTT

1. Thiết bị CNTT được quản lý, vận hành theo thiết kế hệ thống của Cục Thống kê. 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 trong khả năng có thể sửa chữa, khắc phục. Đối với thiết bị ngoài khả năng sửa chữa, khắc phục thông báo cho đơn vị sử dụng làm giấy báo hỏng đề nghị sửa chữa, khắc phục gửi Phòng Tổ chức - Hành chính trình cấp có thẩm quyền phê duyệt theo quy định.

c) Thiết bị CNTT 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, hỏa hoạn.

4. Hàng 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.

5. 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 cấp trên.

Điều 6. Quản lý, vận hành máy chủ

1. Vị trí lắp đặt máy chủ

Máy chủ tại Chi cục Thống kê tỉnh Vĩnh Phúc phải được đặt trong môi trường bảo đảm tiêu chuẩn kỹ thuật của phòng máy chủ quy định tại điều 11 Quy chế này.

2. Phần mềm trên máy chủ

Máy chủ được cài đặt các phần mềm và được quản lý thống nhất, tập

trung bởi Cục Thống kê (Trung tâm Xử lý và Tích hợp dữ liệu thống kê).

3. Vận hành máy chủ

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

b) Thực hiện quy định về đảm bảo ATTT, ANM.

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 CTK phải thực hiện kết nối hệ thống định danh (join domain) của CTK, 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 của người sử dụng.

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 chuyên trách về CNTT;

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

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

Điều 8. Thiết bị mạng, thiết bị lưu trữ

1. Không được tự ý kết nối thiết bị lưu trữ di động vào hệ thống máy tính cơ quan. Tất cả thiết bị lưu trữ di động (USB, ổ cứng di động...) chỉ được kết nối khi có sự kiểm tra, giám sát của đơn vị phụ trách về CNTT.

2. Không tự ý lắp đặt các thiết bị phát sóng Wifi không rõ nguồn gốc vào mạng cơ qun gây nguy cơ mất ATTT, ANM.

Chương III
QUY ĐỊNH BẢO ĐẢM ATTT, ANM

Điều 9. Bảo đảm ATTT trong việc quản lý công chức, người lao động

1. Yêu cầu người được phân công quản lý dữ liệu (Văn bản điều hành và hồ sơ công việc, nhân sự, tài chính kế toán, thi đua khen thưởng, các cuộc điều tra...) và người quản lý hệ thống thông tin phải cam kết trách nhiệm của cá nhân trong việc bảo quản, bảo mật bảo đảm ATTT, ANM; khai thác, sử dụng thông tin, dữ liệu an toàn, hiệu quả.

2. Sử dụng nguồn nhân lực

Các đơn vị có trách nhiệm:

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

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

c) 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, người lao động chấm dứt hoặc thay đổi công việc, cơ quan, đơn vị phải:

a) Giao nhận, lập biên bản bàn giao toàn bộ tài sản, dữ liệu CNTT có liên quan; yêu cầu người bàn giao cam kết không xóa bỏ, tiêu hủy, hủy hoại tài sản và dữ liệu; cất dấu, che đạy, chuyển tài sản, dữ liệu CNTT đi trái quy định.

b) Báo cáo cấp trên thay đổi hoặc thu hồi quyền truy cập các hệ thống thông tin.

Điều 10. Bảo đảm an toàn, an ninh thông tin đối với hệ thống mạng

1. Hệ thống mạng nội bộ (LAN)

Được quản lý, giám sát bởi hệ thống các thiết bị mạng, thiết bị bảo mật.

2. Máy vi tính kết nối mạng

a) Phải được xác thực an toàn;

b) Phải được cài đặt phần mềm phòng chống virus, mã độc tập trung do Cục Thống kê trang bị (Kaspersky);

Điều 11. Bảo đảm an toàn, an ninh thông tin tại 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... phải được đặt trong phòng máy chủ và phải được thiết lập cơ chế bảo vệ, theo dõi phát hiện xâm nhập và biện pháp kiểm soát truy cập theo thiết kế hệ thống của Cục Thống kê.

2. Phòng máy chủ phải được trang bị hệ thống lưu điện, hệ thống làm mát điều hòa không khí, bình cứu hỏa.

3. Chỉ những cá nhân có quyền, nhiệm vụ theo quy định của thủ trưởng đơn vị được giao quản lý phòng máy chủ được phép vào, ra.

Điều 12. Quản lý tài khoản truy cập

a) Mỗi công chức, người lao động ngành Thống kê tỉnh Vĩnh Phúc được cấp một tài khoản AD nội bộ, đồng thời là địa chỉ email công vụ;

b) Tài khoản nội bộ được xác thực khi truy cập máy vi tính, các hệ thống CNTT của ngành như quản lý điều hành, chuyên môn nghiệp vụ;

c) 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 Cục Thống kê.

3. Mật khẩu tài khoản truy cập hệ thống thông tin phải thực hiện đổi ngay sau lần đầu tiên đăng nhập vào hệ thống; định kỳ đổi mật khẩu; đổi ngay khi nghi ngờ mật khẩu bị lộ, lọt, chiếm quyền điều khiển.

4. Đơn vị chuyên trách về ATTT, ANM thực hiện đề nghị đóng tài khoản truy cập hệ thống thông tin trong trường hợp:

a) Đề nghị đóng tạm thời khi phát hiện tài khoản thực hiện các hành vi tấn công hoặc để xảy ra vấn đề mất ATTT, ANM;

b) Đóng vĩnh viễn với những tài khoản nghỉ hưu, chuyển công tác.

Điều 13. Phòng chống mã độc

1. Trách nhiệm của đơn vị quản lý CNTT

a) Theo dõi và vận hành các giải pháp phòng chống mã độc (được cấp bởi Cục Thống kê và tự cơ quan trang bị) và đảm bảo các giải pháp này vận hành liên tục;

b) Tiếp nhận thông báo về sự cố liên quan đến mã độc từ các đơn vị quản lý nhà nước về CNTT; 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 công chức, người lao động trong việc bảo vệ chống lại mã độc:

a) Không sử dụng phần mềm trái phép;

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

c) 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 CNTT hỗ trợ thực hiện;

d) 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.

Điều 14. 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 mất ATTT, ANM cần nhanh chóng báo cho Đơn vị chuyên trách về CNTT.

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 CTK để khắc phục, xử lý kịp thời.

Chương IV
ĐIỀU KHOẢN THI HÀNH

Điều 15. Tổ chức thực hiện

Phòng Thống kê Tổng hợp và Tổ chức - Hành chính có nhiệm vụ:

- Phòng Thống kê tổng hợp là đơn vị quản lý, vận hành hệ thống thông tin, an toàn thông tin tại Chi cục.

- Nghiên cứu, tham mưu, giúp việc và đề xuất với lãnh đạo các biện pháp nhằm phát huy tốt việc quản lý thiết bị CNTT và bảo đảm ATTT, ANM của Chi vục Thống kê tỉnh Vĩnh Phúc.

- Triển khai, hướng dẫn, theo dõi và kiểm tra, kiểm soát việc thực hiện Quy chế này, kịp thời báo cáo Lãnh đạo Chi cục các vấn đề phát sinh nhằm đảm bảo hệ thống mạng hoạt động ổn định, thông suốt, an toàn và hiệu quả.

Các Phòng tham mưu khác và các Đội Thống kê: Tổ chức phổ biến Quy chế đến công chức, người lao động thuộc đơn vị; thực hiện công tác quản lý thiết bị công nghệ thông tin và đảm bảo an toàn thông tin, an ninh mạng; chịu trách nhiệm đảm bảo an toàn, an ninh mạng, khi xảy tra sự cố cần thông báo kịp thời với Phòng Thống kê Tổng hợp để có phương án xử lý. Trong quá trình tổ chức thực hiện, nếu có phát sinh vướng mắc cần kịp thời báo cáo Lãnh đạo Chi cục xem xét, sửa đổi, bổ sung cho phù hợp.

Điều 16. Xử lý vi phạm

Các hành vi vi phạm quy định tại Quy chế này, tùy theo tính chất, mức độ vi phạm sẽ bị nhắc nhở, xử lý theo các quy định của pháp luật và/hoặc Quy chế hoạt động của Cơ quan./.