KIỂM TOÁN NHÀ NƯỚC

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

Số: 2142/QĐ-KTNN

*Hà Nội, ngày 31 tháng 12 năm 2024*

# QUYẾT ĐỊNH

**Ban hành Quy chế đảm bảo an toàn thông tin mạng của Kiểm toán nhà nước**

## TỔNG KIỂM TOÁN NHÀ NƯỚC

*Căn cứ Luật Kiểm toán nhà nước ngày 24/6/2015; Luật sửa đổi, bổ sung một số điều của Luật Kiểm toán nhà nước ngày 26/11/2019;*

*Căn cứ Luật An toàn thông tin mạng 2015; Luật An ninh mạng 2018;*

*Căn cứ Nghị định số 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 Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 của Chính phủ quy định chi tiết một số điều của Luật An ninh mạng.*

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

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

*Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc;*

*Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16/03/2017 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 Quyết định số 1622/QĐ-TTg ngày 25/10/2017 của Thủ tướng Chính phủ về Phê duyệt Đề án 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 2020, định hướng đến 2025;*

*Theo đề nghị của Cục trưởng Cục Công nghệ thông tin.*

## QUYẾT ĐỊNH:

**Điều 1.** Ban hành kèm theo Quyết định này Quy chế đảm bảo an toàn thông tin mạng của Kiểm toán nhà nước.

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

**Điều 3.** Chánh Văn phòng Kiểm toán nhà nước, Cục trưởng Cục Công nghệ thông tin, Thủ trưởng các đơn vị trực thuộc Kiểm toán nhà nước và các đơn vị, tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

***Nơi nhận:***
- Như Điều 3;
- Lãnh đạo Kiểm toán nhà nước;
- Các đơn vị trực thuộc Kiểm toán nhà nước;
- Lưu: VT, CNTT (02).

**KT. TỔNG KIỂM TOÁN NHÀ NƯỚC**
**PHÓ TỔNG KIỂM TOÁN NHÀ NƯỚC**

KIỂM TOÁN NHÀ NƯỚC

**Bùi Quốc Dũng**

KIỂM TOÁN NHÀ NƯỚC

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

# QUY CHẾ

**Đảm bảo an toàn thông tin mạng của Kiểm toán nhà nước**

*(Kèm theo Quyết định số 2142/QĐ-KTNN ngày 31 / 12/2024 của Tổng Kiểm toán nhà nước)*

## Chương I
## QUY ĐỊNH CHUNG

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

1. Quy chế này quy định về đảm bảo An toàn thông tin mạng của Kiểm toán nhà nước.

2. Quy chế này áp dụng đối với các đơn vị, tổ chức (gọi chung là đơn vị) trực thuộc Kiểm toán nhà nước và cán bộ, công chức, viên chức, người lao động thuộc Kiểm toán nhà nước (gọi chung là công chức); đơn vị, tổ chức, cá nhân khác cung cấp dịch vụ công nghệ thông tin và an toàn thông tin mạng cho các đơn vị trực thuộc Kiểm toán nhà nước hoặc có sử dụng kết nối vào hệ thống mạng của Kiểm toán nhà nước.

### Điều 2. Giải thích từ ngữ

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

1. An toàn thông tin mạng là sự bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy 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. Hệ thống mạng bao gồm dịch vụ kết nối internet, mạng nội bộ, mạng truyền số liệu chuyên dùng.

3. 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.

4. Hệ thống công nghệ thông tin là một tập hợp có cấu trúc các trang thiết bị phần cứng, phần mềm, cơ sở dữ liệu và hệ thống mạng để sản xuất, truyền nhận, thu thập, xử lý, lưu trữ và trao đổi thông tin số phục vụ cho một hoặc nhiều hoạt động kỹ thuật, nghiệp vụ của đơn vị.

5. Mạng nội bộ (LAN) là tập hợp các trang thiết bị công nghệ thông tin được kết nối với nhau thông qua các bộ chuyển mạch, bộ định tuyến, bộ điểm truy cập và các máy chủ, thiết bị quản lý mạng, phần mềm quản lý mạng, thiết bị an toàn hệ thống

mạng trong phạm vi quản lý của Kiểm toán nhà nước. Mạng nội bộ bao gồm mạng nội bộ có dây và mạng nội bộ không dây (Wifi).

6. Mạng truyền số liệu chuyên dùng là mạng kết nối các cơ quan Đảng, Nhà nước, được tổ chức, quản lý thống nhất, bảo đảm chất lượng, an toàn, bảo mật thông tin để trao đổi, chia sẻ dữ liệu giữa các cơ quan Đảng, Nhà nước.

7. Vùng mạng internet là vùng mạng được thiết kế để kết nối hệ thống mạng Trung tâm dữ liệu ra các mạng bên ngoài và mạng internet.

8. Vùng mạng lõi là vùng mạng làm nhiệm vụ kết nối tất cả các vùng mạng với nhau, nó có vai trò trung chuyển lưu lượng giữa các vùng.

9. Vùng mạng quản trị là vùng mạng tập trung các máy chủ quản trị, giám sát hệ thống.

10. Vùng máy chủ nội bộ là nơi đặt các máy chủ ứng dụng, cơ sở dữ liệu không trực tiếp cung cấp dịch vụ cho mạng internet.

11. Trung tâm dữ liệu của Kiểm toán nhà nước bao gồm hệ thống máy chủ, thiết bị chuyển mạch, thiết bị định tuyến, thiết bị lưu trữ, thiết bị đảm bảo an toàn thông tin mạng, thiết bị ngoại vi, thiết bị phụ trợ, đường truyền kết nối internet và thiết bị phòng cháy, chữa cháy, chống sét và các thiết bị khác. Kiểm toán nhà nước có 02 Trung tâm dữ liệu là Trung tâm dữ liệu chính và Trung tâm dữ liệu dự phòng.

12. 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.

13. Trang thiết bị công nghệ thông tin cá nhân bao gồm máy tính để bàn, máy tính xách tay, thiết bị số (máy tính bảng, điện thoại thông minh), các sản phẩm mật mã (gồm: thiết bị ký số, thiết bị lưu tham số mật mã - Token, máy mã thoại VoiIP có hình, máy tính chuyên dụng đa giao diện, thiết bị mã thoại và Fax IP, thiết bị bảo mật mạng BMM-100 cho Hội nghị truyền hình) được cấp phát do công chức thuộc Kiểm toán nhà nước quản lý, sử dụng hoặc của người dùng khác truy cập vào hệ thống mạng của Kiểm toán nhà nước.

14. Đơn vị quản lý là đơn vị được Tổng Kiểm toán nhà nước giao trực tiếp xây dựng, quản lý, vận hành, khai thác, sửa chữa, nâng cấp, bảo trì hệ thống thông tin.

15. Tài khoản định danh là tài khoản bao gồm tên đăng nhập (user name), mật khẩu (password) và các thông tin khác nhằm xác định duy nhất người dùng hoặc tổ chức trong hệ thống công nghệ thông tin của Kiểm toán nhà nước để khai thác và sử dụng hệ thống công nghệ thông tin của Kiểm toán nhà nước.

16. Tài khoản định danh cá nhân là tài khoản định danh được cấp cho người dùng là công chức của Kiểm toán nhà nước.

17. Tài khoản quản trị hệ thống là tài khoản có đặc quyền cao nhất trong hệ

thống để có thể kiểm soát và xử lý lỗi dễ dàng khi hệ thống gặp lỗi; là tài khoản có quyền truy cập đầy đủ tài nguyên của các hệ thống công nghệ thông tin của KTNN bao gồm các thành phần như: Máy chủ, thiết bị an ninh bảo mật, thiết bị lưu trữ, các thiết bị mạng, cơ sở dữ liệu, thiết bị giám sát , thiết bị phụ trợ khác (ví dụ tài khoản Administrator của máy chủ Windows; tài khoản root của máy chủ UNIX; tài khoản DBA của hệ thống CSDL Oracle;..) được dùng để quản trị, vận hành, giám sát, sao lưu phục hồi dữ liệu, xử lý sự cố nhằm duy trì hoạt động an toàn, ổn định của hệ thống Công nghệ thông tin.

18. Mật mã là những quy tắc, quy ước riêng dùng để thay đổi hình thức biểu hiện thông tin nhằm bảo đảm bí mật, xác thực, toàn vẹn của nội dung thông tin.

19. Mã hóa là quá trình chuyển đổi dữ liệu này sang một dữ liệu khác với ý nghĩa khác với dữ liệu ban đầu. Mục đích nhằm chỉ cho phép một số người, đối tượng nhất định đọc, hiểu được dữ liệu ban đầu thông qua quá trình giải mã dữ liệu sau khi đã được biến đổi.

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

1. Đảm bảo an toàn thông tin mạng là yêu cầu bắt buộc, thường xuyên, liên tục, có tính xuyên suốt quá trình, đồng bộ từ khi thiết kế, xây dựng, vận hành, nâng cấp và hủy bỏ (dừng hoạt động) hệ thống thông tin. Đảm bảo an toàn thông tin mạng phải tuân thủ các nguyên tắc chung, được quy định tại Điều 4 Luật An toàn thông tin mạng và Điều 4 Nghị định số 85/2016/NĐ-CP ngày 01/07/2016 của Chính phủ về đảm bảo an toàn thông tin theo cấp độ (gọi tắt là Nghị định 85).

2. Các đơn vị được giao quản lý, sử dụng hệ thống thông tin có trách nhiệm đảm bảo an toàn thông tin mạng đối với hệ thống thông tin của đơn vị mình quản lý và sử dụng; bố trí nhân sự để sẵn sàng xử lý sự cố an toàn thông tin mạng đối với các hệ thống thông tin do đơn vị mình quản lý.

3. Công chức thuộc Kiểm toán nhà nước có trách nhiệm đảm bảo an toàn thông tin mạng trong phạm vi xử lý công việc của mình và các thiết bị công nghệ thông tin, phần mềm được giao quản lý, sử dụng theo quy định của Nhà nước và của Kiểm toán nhà nước.

4. Các đơn vị, tổ chức, cá nhân khác có liên quan khi đến làm việc hoặc truy cập vào hệ thống mạng của Kiểm toán nhà nước phải tuân thủ các quy định tại Quy chế này.

5. Việc xử lý sự cố an toàn thông tin mạng phải bảo đảm quyền và lợi ích hợp pháp của cơ quan, đơn vị, cá nhân liên quan và theo quy định của pháp luật, 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, cơ quan.

6. 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.

**Điều 4. Các hành vi bị nghiêm cấm**

1. Các hành vi bị nghiêm cấm quy định tại Điều 7 Luật An toàn thông tin mạng năm 2015 và Điều 8 Luật An ninh mạng năm 2018.

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 hệ thống mạng Kiểm toán nhà nước.

3. Tự ý thay đổi, gỡ bỏ biện pháp an toàn thông tin (như phần mềm phòng chống mã độc - virus) cài đặt trên thiết bị công nghệ thông tin phục vụ công việc.

4. 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.

5. Bẻ khóa, sử dụng trái phép mật khẩu, khóa mật mã và thông tin của cơ quan, cá nhân khác trên môi trường mạng.

6. Các hành vi khác làm mất an toàn thông tin của tổ chức, cá nhân khi trao đổi, truyền đưa, lưu trữ trên môi trường mạng.

7. Truyền bá tư tưởng, văn hóa mang tính kích động, chống phá các chủ trương, đường lối của Đảng, chính sách, pháp luật của Nhà nước.

8. Khai thác, lưu trữ các chương trình giải trí không lành mạnh, các thông tin có nội dung xấu.

9. Sử dụng hệ thống mạng Kiểm toán nhà nước vào các mục đích trái với quy định của Kiểm toán nhà nước và pháp luật.

## Chương II
## QUY ĐỊNH ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG

**Điều 5. Đảm bảo an toàn thông tin mạng của Kiểm toán nhà nước**

1. Đảm bảo an toàn Trung tâm dữ liệu

a) Cục Công nghệ thông tin là đơn vị quản lý, vận hành Trung tâm dữ liệu của Kiểm toán nhà nước.

b) Trung tâm dữ liệu là khu vực hạn chế tiếp cận, chỉ những cá nhân có quyền, nhiệm vụ theo quy định mới được phép vào Trung tâm dữ liệu. Cục Công nghệ thông tin có trách nhiệm kiểm soát ra/vào Trung tâm dữ liệu, ghi nhật ký ra/vào Trung tâm dữ liệu.

2. Đảm bảo an toàn thông tin hệ thống mạng

a) Cục Công nghệ thông tin là đơn vị quản lý, vận hành mạng nội bộ, mạng

truyền số liệu chuyên dùng và dịch vụ internet của Kiểm toán nhà nước.

b) Cục Công nghệ thông tin có trách nhiệm triển khai biện pháp kỹ thuật giám sát kết nối mạng internet của thiết bị công nghệ thông tin, phát hiện và ngăn chặn các hành vi xâm nhập từ mạng internet.

c) Hệ thống mạng nội bộ phải được thiết kế phân vùng theo chức năng cơ bản (theo các chính sách an toàn thông tin riêng), bao gồm: vùng mạng internet, vùng mạng lõi, vùng mạng quản trị, vùng máy chủ nội bộ. 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.

d) Đơn vị thuộc Kiểm toán nhà nước có trách nhiệm tự quản lý, vận hành dịch vụ internet và bảo đảm an toàn thông tin đối với hệ thống mạng nội bộ và các thiết bị tại đơn vị; Thủ trưởng các đơn vị trực thuộc Kiểm toán nhà nước có quyền yêu cầu khóa quyền truy cập của tài khoản định danh thuộc đơn vị mình quản lý trong trường hợp tài khoản đó vi phạm quy định về đảm bảo an toàn thông tin mạng, áp dụng các biện pháp bảo vệ thông tin của đơn vị.

e) Khi phát hiện nguy cơ mất an toàn thông tin (cảnh báo từ phần mềm phòng chống mã độc, máy tính hoạt động chậm bất thường, mất dữ liệu, dấu hiệu phần mềm, ứng dụng lạ), đơn vị và cá nhân phải tắt thiết bị công nghệ thông tin, kịp thời thông báo với Cục Công nghệ thông tin để được hỗ trợ xử lý.

3. Đảm bảo an toàn trong quản lý hệ thống thông tin

a) Đơn vị vận hành hệ thống thông tin chịu trách nhiệm đảm bảo an toàn thông tin cho các hệ thống thông tin theo quy định tại các Điều 22, 23 và 24 của Luật An toàn thông tin mạng năm 2015.

b) Cục Công nghệ thông tin đảm bảo an toàn thông tin cho các hệ thống thông tin dùng chung và cho ý kiến về phương án bảo đảm an toàn cho các hệ thống thông tin trong phạm vi quản lý của Kiểm toán nhà nước.

c) Khi xây dựng mới hoặc nâng cấp hệ thống thông tin, đơn vị quản lý cần phải phối hợp với Cục Công nghệ thông tin để xây dựng phương án bảo đảm an toàn thông tin: rà soát cấp độ an toàn của hệ thống và thực hiện điều chỉnh, bổ sung hoặc thay mới hồ sơ đề xuất cấp độ trong trường hợp cần thiết; kiểm tra đánh giá về an toàn thông tin trước khi vận hành chính thức; giám sát an toàn thông tin cho hệ thống sau khi triển khai.

4. Đảm bảo an toàn trong vận hành hệ thống thông tin

a) Đơn vị vận hành hệ thống thông tin phải thực hiện các quy định về đảm bảo an toàn thông tin theo Điều 22, Nghị định số 85.

b) Đơn vị vận hành hệ thống thông tin thường xuyên kiểm tra, đánh giá, giám sát an toàn hệ thống thông tin; lưu trữ đầy đủ thông tin nhật ký hệ thống thông tin để

phục vụ quản lý, kiểm soát và truy vết khi có sự cố.

5. Đảm bảo an toàn thông tin trong quản lý và sử dụng tài khoản truy cập các hệ thống

a) Công chức có trách nhiệm bảo vệ thông tin tài khoản được cấp, không tiết lộ mật khẩu, không khuyến khích để chế độ lưu mật khẩu tự động hoặc đưa cho người khác phương tiện xác thực tài khoản của mình ngoại trừ các trường hợp: cần xử lý công việc khẩn cấp của đơn vị; đổi ngay mật khẩu sau khi nhận bàn giao lần đầu từ Cục Công nghệ thông tin hoặc có thông báo về sự cố an toàn thông tin, điểm yếu liên quan đến khả năng lộ mật khẩu từ Cục Công nghệ thông tin.

b) Đối với công chức thay đổi vị trí công tác, chuyển công tác, thôi việc hoặc nghỉ hưu, Vụ Tổ chức cán bộ có trách nhiệm cập nhật thông tin lên phần mềm Quản lý cán bộ để hệ thống tự động khóa/thu hồi tài khoản định danh.

c) Thủ trưởng các đơn vị trực thuộc Kiểm toán nhà nước có quyền yêu cầu khóa quyền truy cập của tài khoản định danh thuộc đơn vị mình quản lý trong trường hợp tài khoản đó vi phạm kỷ luật, áp dụng các biện pháp bảo vệ thông tin của đơn vị; khi phát hiện sự cố hoặc các hành vi phá hoại, xâm nhập cần thông báo kịp thời cho Cục Công nghệ thông tin để xử lý.

d) Cục Công nghệ thông tin có quyền khóa quyền truy cập của tài khoản định danh, tài khoản quản trị hệ thống trong trường hợp tài khoản đó có dấu hiệu mất an toàn thông tin hoặc thực hiện các hành vi tấn công vào hệ thống.

e) Tài khoản quản trị hệ thống phải tách biệt với tài khoản truy nhập của người sử dụng thông thường (không dùng tài khoản định danh cá nhân làm tài khoản quản trị hệ thống). Tài khoản quản trị hệ thống phải được giao đích danh cá nhân làm công tác quản trị và không dùng chung tài khoản quản trị hệ thống.

f) Công chức được giao quản trị hệ thống khi thay đổi vị trí công tác, chuyển công tác, thôi việc hoặc nghỉ hưu, thì công chức đó phải có trách nhiệm bàn giao lại tài khoản quản trị hệ thống cho Lãnh đạo phòng quản lý trực tiếp.

6. Đảm bảo an toàn đối với thiết bị công nghệ thông tin được cơ quan cấp phát

a) Các đơn vị và công chức có trách nhiệm quản lý, bảo quản các trang thiết bị công nghệ thông tin được giao quản lý, thiết bị mạng nội bộ và thiết bị công nghệ thông tin dùng chung lắp đặt tại phòng làm việc của đơn vị.

b) Công chức chịu trách nhiệm đảm bảo an toàn thông tin, tránh bị lộ lọt dữ liệu khi thực hiện bảo hành, bảo dưỡng, sửa chữa hoặc bảo trì thiết bị được giao quản lý.

c) Khi ngừng sử dụng thiết bị công nghệ thông tin, công chức phải thực hiện xóa toàn bộ dữ liệu nghiệp vụ được lưu trữ trên thiết bị trước khi bàn giao lại cho đơn vị quản lý. Cục Công nghệ thông tin có trách nhiệm hướng dẫn các công chức xóa dữ liệu trước khi bàn giao thiết bị cho đơn vị quản lý (nếu có yêu cầu).

7. Quy định về đảm bảo an toàn cho máy tính được cơ quan cấp phát

a) Công chức sử dụng máy tính phải cài đặt và cập nhật thường xuyên phần mềm phòng chống mã độc do Kiểm toán nhà nước trang bị; thực hiện kiểm tra, rà quét bằng phần mềm phòng chống mã độc toàn bộ tập tin trên máy tính đối với trường hợp cài đặt lần đầu.

b) Công chức chỉ được cài đặt các phần mềm trên máy tính của mình theo quy định tại Quy chế sử dụng thiết bị Công nghệ thông tin của Kiểm toán nhà nước.

c) Máy tính khi được chuyển sử dụng từ công chức này sang công chức khác hoặc không tiếp tục sử dụng cho công việc của đơn vị phải thực hiện xóa vĩnh viễn toàn bộ dữ liệu trên ổ cứng. Máy tính khi mang đi bảo hành, bảo dưỡng, sửa chữa, phải tháo ổ cứng hoặc xóa vĩnh viễn dữ liệu ổ cứng (có phương án sao lưu dữ liệu ra thiết bị lưu trữ ngoài của công chức), trường hợp cần sự hỗ trợ có thể liên hệ với bộ phận kỹ thuật của Cục Công nghệ thông tin.

d) Đơn vị cần bố trí máy tính riêng không kết nối mạng hoặc sử dụng máy tính đa giao diện do Ban Cơ yếu cung cấp để soạn thảo, lưu trữ tài liệu bí mật nhà nước.

e) Khi phát hiện nguy cơ mất an toàn thông tin (cảnh báo từ phần mềm phòng chống mã độc, máy tính hoạt động chậm bất thường, mất dữ liệu), đơn vị và công chức phải tắt thiết bị công nghệ thông tin, đồng thời báo cáo lãnh đạo đơn vị và thông báo ngay cho Cục Công nghệ thông tin để được hỗ trợ xử lý.

**Điều 6. Kiểm tra, đánh giá an toàn thông tin mạng**

1. Hệ thống công nghệ thông tin của Kiểm toán nhà nước phải được kiểm tra, đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống định kỳ theo quy định tại điểm c khoản 2 Điều 20 Nghị định số 85/2016/NĐ-CP của Chính phủ và khoản 3 Điều 11, khoản 3 Điều 12 Thông tư số 12/2022/TT- BTTTT ngày 01/7/2016 của Bộ trưởng Bộ Thông tin và Truyền thông về Quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP của Chính phủ; kiểm tra, đánh giá an toàn thông tin mạng theo quy định tại điểm c khoản 2 Điều 24 Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 của Thủ tướng Chính phủ quy định chi tiết một số điều của Luật An ninh mạng.

2. Cục Công nghệ thông tin thực hiện kiểm tra, đánh giá hệ thống thông tin của Kiểm toán nhà nước hàng năm hoặc theo chương trình kiểm tra theo chuyên đề về an toàn thông tin mạng được Tổng Kiểm toán nhà nước phê duyệt.

3. Đơn vị quản lý hệ thống thông tin lựa chọn tổ chức, doanh nghiệp có chức năng hoặc được cấp phép thực hiện kiểm tra, đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống thông tin, theo quy định tại khoản 1 Điều 6 Quy chế này.

**Điều 7. Giám sát an toàn hệ thống thông tin**

1. Các hệ thống thông tin phải được thực hiện giám sát an toàn thông tin trong quá trình hoạt động theo quy định tại Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin (gọi tắt là Thông tư số 31).

2. Cục Công nghệ thông tin thiết lập hệ thống kết nối, chia sẻ thông tin giám sát giữa hệ thống thông tin của Kiểm toán nhà nước với Trung tâm giám sát không gian mạng quốc gia thuộc Cục An toàn thông tin, Bộ Thông tin và Truyền thông. Nội dung thông tin giám sát cần kết nối, chia sẻ theo hướng dẫn của Bộ Thông tin và Truyền thông.

**Điều 8. Ứng cứu sự cố an toàn hệ thống thông tin**

1. Cục Công nghệ thông tin là đơn vị chuyên trách về ứng cứu sự cố an toàn thông tin mạng của Kiểm toán nhà nước, theo kế hoạch hằng năm, Cục Công nghệ thông tin có trách nhiệm trình Tổng Kiểm toán nhà nước kiện toàn Đội ứng cứu sự cố an toàn thông tin mạng và tổ chức ứng cứu sự cố trong phạm vi của Kiểm toán nhà nước.

2. Quy trình ứng cứu sự cố An toàn thông tin mạng được thực hiện theo quy định tại Quyết định số 05/2017/QĐ-TTg ngày 16/03/2017 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 và Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc.

3. Diễn tập ứng cứu sự cố an toàn thông tin mạng

a) Cục Công nghệ thông tin là thành viên mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia tham gia đầy đủ các cuộc diễn tập quốc gia, quốc tế do Cơ quan điều phối quốc gia và các cơ quan chức năng thuộc Bộ Thông tin và Truyền thông, Bộ Công an, Bộ Quốc phòng tổ chức.

b) Hàng năm, Cục Công nghệ thông tin chủ trì tổ chức diễn tập ứng cứu sự cố an toàn thông tin mạng trong phạm vi các hệ thống thông tin của Kiểm toán nhà nước làm chủ quản, thực hiện theo kế hoạch ứng phó sự cố đảm bảo an toàn thông tin mạng và phương án ứng phó, khắc phục sự cố an ninh mạng được Tổng Kiểm toán nhà nước phê duyệt.

**Điều 9. Phổ biến, tuyên truyền, đào tạo, bồi dưỡng về an toàn thông tin mạng**

1. Cục Công nghệ thông tin lập kế hoạch và triển khai công tác tuyên truyền, phổ biến chủ chương, chính sách, pháp luật, biện pháp an toàn thông tin mạng, thông qua các hình thức: văn bản hướng dẫn, đào tạo, hội nghị, hội thảo, đăng bài trên Cổng thông tin điện tử Kiểm toán nhà nước, trang thông tin điện tử của Cục Công nghệ

thông tin, gửi thư điện tử và các hình thức khác phù hợp với quy định của pháp luật.

2. Các đơn vị trực thuộc Kiểm toán nhà nước quán triệt, tuyên truyền, phổ biến, nâng cao nhận thức, trách nhiệm về an toàn thông tin mạng cho công chức thuộc đơn vị.

**Điều 10. Báo cáo an toàn thông tin mạng**

1. Cục Công nghệ thông tin lập báo cáo năm về an toàn thông tin mạng theo quy định tại khoản 3 Điều 13 và Điều 14 Thông tư số 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 số 85/2016/NĐ-CP của Chính phủ gửi Tổng Kiểm toán nhà nước và Bộ Thông tin và Truyền thông trước 25 tháng 12 hàng năm.

2. Cục Công nghệ thông tin lập báo cáo hoạt động giám sát an toàn thông tin mạng của Kiểm toán nhà nước định kỳ 6 tháng theo quy định tại điểm k khoản 3 Điều 5 Thông tư 31 gửi Tổng Kiểm toán nhà nước và Bộ Thông tin và Truyền thông theo hướng dẫn của Bộ Thông tin và Truyền thông.

**Điều 11. Xác định cấp độ và phương án đảm bảo an toàn hệ thống thông tin**

1. Các hệ thống thông tin phải thực hiện đảm bảo an toàn thông tin cấp độ theo quy định tại Nghị định số 85.

2. Cục Công nghệ thông tin và các đơn vị được giao quản lý hệ thống thông tin có trách nhiệm lập hồ sơ đề xuất cấp độ an toàn thông tin, trình Tổng Kiểm toán nhà nước phê duyệt hồ sơ đề xuất cấp độ theo quy định tại Nghị định 85.

3. Phương án đảm bảo an toàn theo cấp độ

a) Đơn vị xây dựng hệ thống công nghệ thông tin phải xây dựng phương án đảm bảo an toàn thông tin phù hợp với cấp độ của hệ thống thông tin và đáp ứng yêu cầu quy định tại Thông tư số 12/2022/TT- BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông về Quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP của Chính phủ, phù hợp với tiêu chuẩn TCVN 11930:2017 và quy định về an toàn thông tin mạng của Kiểm toán nhà nước.

b) Đơn vị vận hành hệ thống thông tin có trách nhiệm tổ chức triển khai phương án đảm bảo an toàn hệ thống thông tin sau khi được phê duyệt.

c) Cục Công nghệ thông tin giám sát, kiểm tra, đánh giá việc triển khai các phương án đảm bảo an toàn thông tin đã được phê duyệt.

## Chương III
## TỔ CHỨC THỰC HIỆN

**Điều 12. Trách nhiệm của Cục Công nghệ thông tin**

1. Chủ trì tổ chức theo dõi, đôn đốc, kiểm tra và đánh giá việc thực hiện Quy chế này.

2. Chịu trách nhiệm trước pháp luật và Tổng Kiểm toán nhà nước về các vi phạm, thất thoát thông tin, dữ liệu thuộc phạm vi quản lý của đơn vị do không tổ chức, chỉ đạo kiểm tra công chức của đơn vị thực hiện đúng Quy chế này.

3. Đảm nhận vài trò là đơn vị vận hành hệ thống thông tin của Kiểm toán nhà nước; là đơn vị chuyên trách an toàn thông tin mạng của Kiểm toán nhà nước.

4. Lập kế hoạch hàng năm trình Tổng Kiểm toán nhà nước phê duyệt và tổ chức triển khai kế hoạch đảm bảo an toàn thông tin mạng của Kiểm toán nhà nước và kế hoạch đào tạo, bồi dưỡng nghiệp vụ cho cán bộ chuyên trách công nghệ thông tin.

5. Hàng năm, phối hợp với các đơn vị trực thuộc Kiểm toán nhà nước kiểm tra về công tác đảm bảo an toàn thông tin mạng đối với các đơn vị.

6. Nhắc nhở, tạm dừng cung cấp dịch vụ trong hệ thống mạng Kiểm toán nhà nước đối với các đơn vị, người sử dụng có liên quan đến việc kiểm tra, khắc phục sự cố. Trường hợp có sự cố nghiêm trọng vượt quá khả năng khắc phục phải báo cáo Tổng Kiểm toán nhà nước và thông báo cho các tổ chức có chuyển môn sâu hỗ trợ xử lý sự cố mất An toàn thông tin để cùng phối hợp giải quyết.

7. Trước ngày 01/03 hàng năm, thực hiện báo cáo Tổng Kiểm toán nhà nước tình hình an toàn thông tin của năm liền trước theo mẫu số 02 kèm theo Quy chế này; báo cáo cho Bộ Thông tin và Truyền thông về hoạt động giám sát của chủ quản hệ thống thông tin định kỳ 6 tháng theo mẫu tại Phụ lục 2 Thông tư số 31; báo cáo đột xuất hoặc theo yêu cầu của Tổng Kiểm toán nhà nước (nếu có).

**Điều 13. Trách nhiệm của thủ trưởng các đơn vị trực thuộc Kiểm toán nhà nước**

1. Thủ trưởng các đơn vị trực thuộc Kiểm toán nhà nước có trách nhiệm phổ biến, quán triệt đến toàn bộ công chức trong đơn vị thực hiện các quy định của Quy chế này.

2. Bố trí công chức phối hợp chặt chẽ với Cục Công nghệ thông tin trong quá trình triển khai công tác đảm bảo an toàn thông tin mạng tại đơn vị và tham gia chương trình đào tạo, tập huấn của Kiểm toán nhà nước về an toàn thông tin mạng khi có yêu cầu.

3. Thường xuyên kiểm tra, đôn đốc việc triển khai an toàn thông tin mạng trong đơn vị.

4. Trong trường hợp mua sắm trang bị thiết bị hạ tầng công nghệ thông tin, xây dựng phần mềm có liên quan hoặc ảnh hưởng tới hạ tầng công nghệ, phần mềm dùng chung của Kiểm toán nhà nước phải có tư vấn, thông qua của đơn vị chuyên trách

an toàn thông tin thẩm định để không gây ảnh hưởng tới hạ tầng công nghệ chung của Kiểm toán nhà nước.

5. Chịu trách nhiệm trước pháp luật và Tổng Kiểm toán nhà nước về các vi phạm, thất thoát thông tin, dữ liệu thuộc phạm vi quản lý của đơn vị do không tổ chức, chỉ đạo kiểm tra công chức của đơn vị thực hiện đúng Quy chế này.

6. Trước ngày 01/02 hàng năm, thực hiện gửi báo cáo tình hình đảm bảo an toàn thông tin tại các đơn vị về Cục Công nghệ thông tin của năm liền trước theo mẫu số 01 kèm theo Quy chế này.

**Điều 14. Trách nhiệm của công chức**

1. Thực hiện các quy định tại Quy chế này về đảm bảo an toàn thông tin mạng.

2. Tham gia đầy đủ các lớp đào tạo ngắn hạn, tuyên truyền, phổ biến nâng cao nhận thức, diễn tập an toàn thông tin và ứng cứu sự cố để bảo đảm an toàn thông tin mạng theo kế hoạch.

3. Chịu trách nhiệm trước lãnh đạo đơn vị và Tổng Kiểm toán nhà nước về các vi phạm làm mất an toàn thông tin mạng do không tuân thủ Quy chế này.

**Điều 15. Trách nhiệm thi hành**

1. Các đơn vị, công chức thuộc Kiểm toán nhà nước chịu trách nhiệm thực hiện các quy định của Quy chế này.

2. Các tổ chức, cá nhân khác có sử dụng, kết nối hoặc truy cập vào các hệ thống thông tin do Kiểm toán nhà nước triển khai hoặc liên quan đến hoạt động ứng dụng công nghệ thông tin của Kiểm toán nhà nước phải tuân thủ Quy chế này và các quy định hiện hành của pháp luật có liên quan.

3. Các đơn vị, tổ chức, cá nhân cung cấp dịch vụ công nghệ thông tin và an toàn thông tin mạng cho các đơn vị trực thuộc Kiểm toán nhà nước phải tuân thủ Quy chế này và các quy định hiện hành của pháp luật có liên quan.

4. Trong quá trình thực hiện nếu có khó khăn vướng mắc, đơn vị phản ánh về Cục Công nghệ thông tin để tổng hợp, báo cáo Tổng Kiểm toán nhà nước xem xét sửa đổi, bổ sung Quy chế cho phù hợp./.

*Mẫu số 01*

KIỂM TOÁN NHÀ NƯỚC
**<< ĐƠN VỊ BÁO CÁO >>**

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

*Hà Nội, ngày tháng năm 20...*

# BÁO CÁO TÌNH HÌNH ĐẢM BẢO AN TOÀN THÔNG TIN

**Năm: <Năm báo cáo>**

Kính gửi: Cục Công nghệ thông tin

*I. Tình hình triển khai các giải pháp an toàn thông tin tại đơn vị*

| STT | Nội dung | Kết quả | Ghi chú |
|---|---|---|---|
| *1* | *2* | *3* | *5* |
| 1 | Triển khai phần mềm diệt virus trên máy tính | Tỷ lệ triển khai | Tỷ lệ % số lượng triển khai/tổng số công chức, viên chức |
| 2 | Phổ biến cho công chức, viên chức, người lao động về các văn bản hướng dẫn về an toàn thông tin phát sinh trong năm | Tỷ lệ phổ biến | Tỷ lệ % số lượng văn bản đã phổ biến/tổng số văn bản phát sinh trong năm |

*II. Tình hình mất an toàn thông tin phát sinh tại đơn vị*

| STT | Nội dung | Kết quả | Ghi chú |
|---|---|---|---|
| *1* | *2* | *3* | *4* |
| I | Số lượng sự cố an toàn thông tin phát sinh tại đơn vị | Số lượng | Số lượng sự cố an toàn thông tin phát sinh trong năm |
| II | Chi tiết sự cố an toàn thông tin phát sinh | | |
| 1 | Sự cố 1: Mô tả sự cố:<br>- Nội dung sự cố<br>- Thời điểm xảy ra sự cố<br>- Thời gian khắc phục sự cố<br>- Ảnh hưởng sự cố an toàn thông tin | Kết quả xử lý sự cố | Ghi nhận sự phối hợp với Cục CNTT và các đơn vị xử lý sự cố an toàn thông tin phát sinh tại đơn vị |

| STT | Nội dung | Kết quả | Ghi chú |
|---|---|---|---|
| 2 | Sự cố 2: Ví dụ: Sự cố tấn công chiếm quyền email, gửi thư Spam | - Đã phối hợp với Cục CNTT xử lý sự cố. | |

**Đại diện Lãnh đạo đơn vị báo cáo**
*(Ký, ghi rõ họ tên, chức vụ, đóng dấu)*

*Mẫu số 02*

KIỂM TOÁN NHÀ NƯỚC
**CỤC CÔNG NGHỆ THÔNG TIN**

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

*Hà Nội, ngày tháng năm 20...*

# BÁO CÁO TỔNG HỢP
# TÌNH HÌNH ĐẢM BẢO AN TOÀN THÔNG TIN TOÀN NGÀNH
## Năm: <Năm báo cáo>

Kính gửi: Tổng Kiểm toán nhà nước

*I. Tình hình triển khai các giải pháp an toàn thông tin tại các đơn vị*

| STT | Nội dung | Kết quả | Ghi chú |
|---|---|---|---|
| *1* | *2* | *3* | *5* |
| 1 | Triển khai phần mềm diệt virus trên máy tính | Tỷ lệ triển khai | Tỷ lệ % số lượng triển khai/tổng số công chức, viên chức |
| 2 | Phổ biến cho công chức, viên chức, người lao động về các văn bản hướng dẫn về an toàn thông tin phát sinh trong năm | Tỷ lệ phổ biến | Tỷ lệ đơn vị đã phổ biến đầy đủ cho công chức, viên chức, người lao động về các văn bản hướng dẫn an toàn thông tin phát sinh trong năm/Tổng số đơn vị |

*II. Tình hình mất an toàn thông tin phát sinh tại đơn vị*

| STT | Nội dung | Kết quả | Ghi chú |
|---|---|---|---|
| *1* | *2* | *3* | *4* |
| I | Số lượng sự cố an toàn thông tin phát sinh tại các đơn vị | Số lượng | Số lượng sự cố an toàn thông tin phát sinh trong năm |
| II | Tổng hợp sự cố an toàn thông tin phát sinh | | |

| STT | Nội dung | Kết quả | Ghi chú |
|---|---|---|---|
| 1 | Sự cố mức độ đặc biệt nghiêm trọng | Số lượng sự cố đặc biệt nghiêm trọng | |
| 1 | Sự cố mức độ nghiêm trọng | Số lượng sự cố nghiêm trọng | |
| 2 | Sự cố mức độ thông thường | Số lượng sự cố thông thường | |

*III. Tổng hợp sự cố an toàn thông tin tại Trung tâm dữ liệu (báo cáo theo mẫu hướng dẫn của Bộ Thông tin và truyền thông)*

| Loại sự cố/tấn công mạng | Số lượng | Số sự cố tự xử lý | Số sự cố có sự hỗ trợ xử lý từ các tổ chức khác | Số sự cố có hỗ trợ xử lý từ tổ chức nước ngoài | Số sự cố đề nghị VNCERT hỗ trợ xử lý | Thiệt hại ước tính |
|---|---|---|---|---|---|---|
| Từ chối dịch vụ | | | | | | |
| Tấn công giả mạo | | | | | | |
| Tấn công sử dụng mã độc | | | | | | |
| Truy cập trái phép, chiếm quyền điều khiển | | | | | | |
| Thay đổi giao diện | | | | | | |
| Mã hóa phần mềm, dữ liệu, thiết bị | | | | | | |
| Phá hoại thông tin, dữ liệu, phần mềm | | | | | | |
| Nghe trộm, gián điệp, lấy | | | | | | |

| Loại sự cố/tấn công mạng | Số lượng | Số sự cố tự xử lý | Số sự cố có sự hỗ trợ xử lý từ các tổ chức khác | Số sự cố có hỗ trợ xử lý từ tổ chức nước ngoài | Số sự cố đề nghị VNCERT hỗ trợ xử lý | Thiệt hại ước tính |
|---|---|---|---|---|---|---|
| cắp thông tin, dữ liệu | | | | | | |
| Tấn công tổng hợp sử dụng kết hợp nhiều hình thức | | | | | | |
| Các hình thức tấn công khác | | | | | | |
| Các cảnh báo liên quan đến hệ thống máy chủ | | | | | | |
| **Tổng số** | | | | | | |

**CỤC TRƯỞNG**

*(Ký, ghi rõ họ tên, chức vụ, đóng dấu)*