KIỂM TOÁN NHÀ NƯỚC ---	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc ---
Số: 1173/QĐ-KTNN	*Hà Nội, ngày 27 tháng 7 năm 2015*

QUYẾT ĐỊNH

BAN HÀNH QUY CHẾ QUẢN LÝ VÀ SỬ DỤNG HỆ THỐNG MẠNG KIỂM TOÁN NHÀ NƯỚC

TỔNG KIỂM TOÁN NHÀ NƯỚC

Căn cứ Luật Kiểm toán nhà nước;

Căn cứ Luật Công nghệ thông tin;

Căn cứ Luật Giao dịch điện tử;

Căn cứ Nghị quyết số 916/2005/NQ-UBTVQH11 ngày 15 tháng 9 năm 2005 của Uỷ ban Thường vụ Quốc hội về cơ cấu tổ chức của Kiểm toán Nhà nước;

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước;

Xét đề nghị của Giám đốc Trung tâm Tin học,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế quản lý và sử dụng hệ thống mạng Kiểm toán Nhà nước.

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

Điều 3. Chánh Văn phòng Kiểm toán Nhà nước, Giám đốc Trung tâm Tin học, Thủ trưởng các đơn vị trực thuộc Kiểm toán Nhà nước và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

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

Hoàng Hồng Lạc

Nơi nhận:
- Như Điều 3;
- Tổng Kiểm toán Nhà nước;
- Các Phó Tổng Kiểm toán Nhà nước;
- Đảng ủy KTNN;
- BCH Công đoàn KTNN;
- BCH Đoàn TN CSHCM KTNN;
- Lưu: VT, TTTH (03).

VBL - TS24 CORP
www.TS24.com.vn

QUY CHẾ

QUẢN LÝ VÀ SỬ DỤNG HỆ THỐNG MẠNG KIỂM TOÁN NHÀ NƯỚC

(Ban hành kèm theo Quyết định số 1173 /QĐ-KTNN ngày 27 tháng 7 năm 2015 của Tổng Kiểm toán Nhà nước)

Chương I

QUY ĐỊNH CHUNG

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

1. Quy chế này quy định việc quản lý, vận hành, khai thác và sử dụng hệ thống mạng Kiểm toán Nhà nước.

2. Quy chế này áp dụng đối với đơn vị, tổ chức (gọi chung là đơn vị) trực thuộc Kiểm toán Nhà nước; cán bộ, công chức, viên chức, người lao động (gọi chung là công chức, viên chức và viết tắt là CCVC) của Kiểm toán Nhà nước và tổ chức, cá nhân có liên quan trong việc quản lý và sử dụng hệ thống mạng Kiểm toán Nhà nước.

Điều 2. Hệ thống mạng Kiểm toán Nhà nước

1. Hệ thống mạng Kiểm toán Nhà nước (viết tắt là SAVNET) bao gồm: Trung tâm dữ liệu, tài nguyên mạng của Kiểm toán Nhà nước, hệ thống mạng cục bộ (LAN) tại các đơn vị trực thuộc Kiểm toán Nhà nước.

2. Trung tâm dữ liệu (TTDL) là trung tâm chính của hệ thống mạng Kiểm toán Nhà nước.

3. Tài nguyên mạng của Kiểm toán Nhà nước bao gồm:

a) Hệ thống địa chỉ IP (Internet Protocol) sử dụng để giao tiếp trên mạng bao gồm: Địa chỉ công cộng (public IP) để giao tiếp với mạng Internet; địa chỉ dùng riêng (private IP) để giao tiếp giữa các máy tính trong mạng cục bộ (LAN) và các máy tính trong SAVNET.

b) Hệ thống tên miền của Kiểm toán Nhà nước đã đăng ký bảo vệ với Trung tâm Internet Việt Nam (VNNIC).

c) Các thiết bị truyền dẫn, kết nối mạng cục bộ của các đơn vị trực thuộc Kiểm toán Nhà nước; kết nối giữa các đơn vị trực thuộc với TTDL Kiểm toán Nhà nước; các kết nối tới nhà cung cấp dịch vụ viễn thông và Internet.

d) Các trang thiết bị công nghệ thông tin trên SAVNET bao gồm: Máy chủ, máy trạm, thiết bị ngoại vi, thiết bị phụ trợ và các thiết bị mạng.

đ) Hệ thống thư điện tử Kiểm toán Nhà nước; Hệ thống hội nghị truyền hình trực tuyến; các cơ sở dữ liệu, phần mềm hệ thống, phần mềm ứng dụng, phần mềm chuyên ngành hợp pháp được cài đặt, hoạt động trên SAVNET.

e) Cổng thông tin điện tử (Portal), Trang thông tin điện tử (Website) của Kiểm toán Nhà nước được lưu trữ trên máy chủ đặt tại TTDL Kiểm toán Nhà nước.

g) Các dịch vụ cung cấp trên SAVNET và tài khoản người sử dụng dùng trong các dịch vụ trên SAVNET.

4. Hệ thống mạng Kiểm toán Nhà nước được sử dụng để phục vụ công tác chỉ đạo điều hành, quản lý nội bộ và hoạt động kiểm toán của Kiểm toán Nhà nước; cung cấp các tài nguyên mạng phục vụ hoạt động của các đơn vị, CCVC thuộc Kiểm toán Nhà nước.

Điều 3. Giải thích thuật ngữ

1. Người sử dụng: Là CCVC thuộc Kiểm toán Nhà nước được cấp quyền khai thác, sử dụng tài nguyên mạng trên SAVNET.

2. Bộ phận quản trị: Là bộ phận được Trung tâm Tin học giao nhiệm vụ quản trị, vận hành, đảm bảo hoạt động an toàn, bảo mật, ổn định của SAVNET.

3. Cán bộ chuyên trách công nghệ thông tin: Là người được giao nhiệm vụ quản trị, vận hành, đảm bảo hoạt động an toàn, bảo mật, ổn định của hệ thống mạng tại đơn vị trực thuộc Kiểm toán Nhà nước.

4. Tài khoản người sử dụng: Bao gồm tên tài khoản (user name) và mật khẩu (password) dùng để định danh và xác định quyền hạn của người sử dụng trên các dịch vụ mạng.

5. Mạng cục bộ (LAN - Local Area Network): Là một hệ thống mạng bao gồm các máy tính, máy chủ và các thiết bị ngoại vi được kết nối với nhau thông qua các thiết bị mạng để chia sẻ tài nguyên như thông tin, dữ liệu, phần mềm và các thiết bị.

6. Mạng diện rộng (WAN - Wide Area Network): Là một hệ thống mạng được thiết lập để kết nối hai hay nhiều mạng LAN có khoảng cách xa về mặt địa lý thành mạng riêng của tổ chức hoặc kết nối qua nhiều hạ tầng mạng công cộng của các công ty viễn thông khác nhau.

7. Môi trường mạng: Là môi trường trong đó thông tin được cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông qua cơ sở hạ tầng thông tin.

8. Cơ sở hạ tầng thông tin: Là hệ thống trang thiết bị phục vụ cho việc sản xuất, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin số, bao gồm mạng viễn thông, mạng internet, mạng máy tính và cơ sở dữ liệu.

9. Thông số thiết lập mạng Kiểm toán Nhà nước: Là các thông số do Trung tâm Tin học quy định nhằm đảm bảo sự thống nhất trong việc quản lý, khai thác sử dụng tài nguyên mạng của Kiểm toán Nhà nước.

10. Cơ sở dữ liệu (Database): Là tập hợp các dữ liệu được sắp xếp, tổ chức để truy cập, khai thác sử dụng, quản lý và cập nhật thông qua phương tiện điện tử.

11. Dịch vụ mạng: Là các dịch vụ được thực hiện trên môi trường mạng nhằm giúp người sử dụng truy nhập và sử dụng chung các tài nguyên trên mạng.

12. An toàn thông tin: Bao gồm các hoạt động quản lý, nghiệp vụ và kỹ thuật đối với hệ thống thông tin nhằm bảo vệ, khôi phục các hệ thống, các dịch vụ và nội dung thông tin đối với nguy cơ tự nhiên hoặc do con người gây ra. Bảo đảm cho các hệ thống thực hiện đúng chức năng, phục vụ đúng đối tượng một cách sẵn sàng, chính xác và tin cậy.

13. Hệ thống an ninh bảo mật: Là tập hợp các thiết bị tin học hoạt động đồng bộ theo một chính sách an ninh nhất quán nhằm quản lý, giám sát, kiểm soát chặt chẽ mọi thông tin trên mạng, phát hiện và xử lý các truy cập bất hợp pháp.

14. Đảm bảo an toàn thông tin: Là đảm bảo tính bí mật, tính toàn vẹn, tính chống chối bỏ và tính sẵn sàng của thông tin, trong đó:

- Tính bí mật: Bảo đảm thông tin chỉ có thể được truy cập bởi những người có thẩm quyền đối với thông tin.

- Tính toàn vẹn: Thông tin không bị sửa đổi làm sai lệch nội dung.

- Tính chống chối bỏ: Các cá nhân tham gia vào SAVNET, sử dụng các tài nguyên mạng của Kiểm toán Nhà nước không thể chối bỏ các hoạt động đã thực hiện. Tính chống chối bỏ cung cấp các bằng chứng chống lại việc chối bỏ một hành động đã thực hiện hay đã diễn ra.

- Tính sẵn sàng: Bảo đảm những người được cấp quyền có thể truy cập sử dụng thông tin ngay khi có nhu cầu.

15. Cổng thông tin điện tử (Portal): Là điểm truy cập tập trung và duy nhất, tích hợp các kênh thông tin, các dịch vụ và ứng dụng, phân phối tới người sử dụng thông qua một phương thức thống nhất trên nền tảng Web.

16. Trang thông tin điện tử: Là trang thông tin hoặc một tập hợp trang thông tin trên môi trường mạng phục vụ cho việc cung cấp, trao đổi thông tin.

17. Trung tâm dữ liệu: Là hệ thống các máy chủ, máy trạm, thiết bị lưu trữ, bảo mật và thiết bị mạng. TTDL là nơi lưu giữ các cơ sở dữ liệu, hệ thống thư điện tử, cổng thông tin điện tử, trang thông tin điện tử và các phần mềm chuyên ngành phục vụ hoạt động của Kiểm toán Nhà nước. Thông qua SAVNET, các đơn vị trực thuộc Kiểm toán Nhà nước có thể khai thác, sử dụng các dịch vụ, tài nguyên mạng tại TTDL.

Điều 4. Nguyên tắc quản lý, vận hành, khai thác và sử dụng hệ thống mạng Kiểm toán Nhà nước

1. Chỉ sử dụng SAVNET phục vụ yêu cầu công việc, nhiệm vụ được giao. Không sử dụng SAVNET vào mục đích:

- 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;

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

- Phát tán virus, gửi thư rác, làm công cụ tấn công SAVNET hoặc các mạng khác;

- Chơi các trò chơi trực tuyến (game online).

2. Thông tin thuộc danh mục bí mật nhà nước được truyền tải trên SAVNET phải tuân thủ quy định về bảo vệ bí mật nhà nước; việc sử dụng, chia sẻ và lưu trữ thông tin trên SAVNET phải tuân thủ các quy định của Nhà nước về viễn thông, công nghệ thông tin và lưu trữ.

3. Chỉ được phép sử dụng các phần mềm hợp pháp, có nguồn gốc rõ ràng do Trung tâm Tin học cài đặt hoặc Kiểm toán Nhà nước cho phép cài đặt trên các máy tính, máy chủ trong SAVNET.

4. Không tự ý gỡ bỏ kết nối mạng, thay đổi thông số của các thiết bị (tên, địa chỉ mạng,...) gây xung đột tài nguyên trên mạng; không lắp đặt, cài đặt các thiết bị phát sóng không dây (wireless) vào SAVNET khi chưa được sự đồng ý của Trung tâm Tin học.

5. Các đơn vị, CCVC thuộc Kiểm toán Nhà nước chịu trách nhiệm quản lý, sử dụng tài khoản được cấp để khai thác, sử dụng tài nguyên mạng trên SAVNET theo quy định.

6. Người sử dụng chịu trách nhiệm về các hư hỏng trực tiếp hay gián tiếp gây ra cho các tài nguyên mạng của Kiểm toán Nhà nước nếu không tuân thủ các quy định quản lý, vận hành, khai thác và sử dụng SAVNET.

7. Nghiêm cấm sử dụng SAVNET vào các mục đích trái với quy định của Kiểm toán Nhà nước và pháp luật.

Điều 5. Ngôn ngữ sử dụng trên hệ thống mạng Kiểm toán Nhà nước

Ngôn ngữ được dùng để trao đổi thông tin trên SAVNET bằng tiếng Việt và tiếng Anh. SAVNET sử dụng bảng mã chuẩn và các kiểu chữ tiếng Việt theo quy định của pháp luật hiện hành về sử dụng thống nhất bộ mã ký tự tiếng Việt trong trao đổi thông tin điện tử giữa các cơ quan Đảng và Nhà nước.

Chương II

QUẢN LÝ, VẬN HÀNH, KHAI THÁC, SỬ DỤNG HỆ THỐNG MẠNG KIỂM TOÁN NHÀ NƯỚC

Điều 6. Trách nhiệm quản lý và vận hành hệ thống mạng Kiểm toán Nhà nước

1. Trung tâm Tin học (TTTH) giúp Tổng Kiểm toán Nhà nước quản lý và vận hành SAVNET có trách nhiệm sau:

a) Quản lý, vận hành và quy hoạch các tài nguyên trên SAVNET; hỗ trợ kỹ thuật cho các đơn vị và người sử dụng khai thác tài nguyên trên SAVNET có hiệu quả và đảm bảo an toàn, an ninh thông tin.

b) Áp dụng các biện pháp, chính sách quản lý đối với SAVNET và người sử dụng theo yêu cầu thực tế trong từng thời kỳ, theo tiêu chuẩn kỹ thuật về dữ liệu và thiết lập thông số mạng phù hợp với các quy định của cơ quan có thẩm quyền ban hành về hệ thống mạng máy tính.

c) Nhắc nhở, tạm ngừng cung cấp dịch vụ, trường hợp nghiêm trọng có thể thu hồi tài nguyên mạng và báo cáo cấp có thẩm quyền để xử lý đối với đơn vị, CCVC vi phạm các nguyên tắc quản lý và sử dụng SAVNET.

d) Kịp thời thông báo và khắc phục sự cố khi SAVNET tạm ngừng hoạt động. Nội dung thông báo phải nêu rõ khoảng thời gian dự kiến đưa hệ thống vào hoạt động bình thường.

2. Các đơn vị trực thuộc Kiểm toán Nhà nước có trách nhiệm:

a) Quản lý, khai thác và sử dụng hệ thống mạng LAN, mạng WAN tại đơn vị mình.

b) Xây dựng cơ chế bảo mật, an toàn thông tin cho hệ thống mạng LAN của đơn vị; đảm bảo an toàn, chống truy cập trái phép từ bên ngoài cũng như từ bên trong vào hệ thống mạng LAN của đơn vị và SAVNET. Khuyến khích các đơn vị trực thuộc xây dựng Quy chế quản lý, sử dụng hệ thống mạng áp dụng cho đơn vị mình phù hợp với quy định của Quy chế này.

c) Chịu trách nhiệm về nội dung, thông tin đơn vị trao đổi trên SAVNET.

d) Phối hợp với Trung tâm Tin học trong quá trình định hướng công nghệ, quản lý, khai thác và sử dụng, đảm bảo hoạt động an toàn, ổn định cho hệ thống mạng LAN tại đơn vị và SAVNET.

đ) Khi có sự cố liên quan đến kết nối, truy cập SAVNET cần báo ngay đến bộ phận quản trị SAVNET để kịp thời khắc phục.

Điều 7. Khai thác, sử dụng hệ thống mạng Kiểm toán Nhà nước

1. Trung tâm Tin học áp dụng các biện pháp cần thiết để đảm bảo hoạt động của SAVNET được an toàn và thông suốt.

2. Các đơn vị và cá nhân tham gia vào SAVNET không được tự ý thay đổi những thông số mạng hay tự ý đưa các phần mềm và thiết bị khác tham gia vào SAVNET.

3. Các đơn vị và cá nhân sẽ được cấp tài khoản người dùng để truy cập SAVNET; khi đã đăng nhập, người dùng có quyền khai thác cơ sở dữ liệu và sử dụng các tài nguyên mạng theo quy định của Kiểm toán Nhà nước.

4. Không sử dụng SAVNET để khai thác, lưu trữ các dữ liệu, thông tin như: các trò chơi, các chương trình giải trí không lành mạnh, có nội dung xấu, các thông tin, dữ liệu trái với quy định của Kiểm toán Nhà nước và pháp luật.

Điều 8. Phần mềm và ứng dụng trong hệ thống mạng Kiểm toán Nhà nước

1. Các phần mềm, ứng dụng khi vận hành trong SAVNET tối thiểu phải đáp ứng những yêu cầu sau:

a) Phải được kiểm tra, thử nghiệm đáp ứng tiêu chuẩn an toàn thông tin hiện hành trước khi đưa vào sử dụng trong SAVNET.

b) Việc sử dụng, trang bị phần mềm hệ thống, phần mềm tiện ích và ứng dụng công nghệ thông tin phải tuân thủ theo Luật bản quyền.

c) Đảm bảo tính toàn vẹn của dữ liệu khi lưu chuyển trong SAVNET.

2. Trung tâm Tin học có trách nhiệm xây dựng quy trình hoạt động, thử nghiệm, trực tiếp cài đặt, quản lý và vận hành phần mềm hệ thống, phần mềm tiện ích và ứng dụng công nghệ thông tin trong SAVNET; nghiên cứu, đề xuất, nâng cấp phần mềm theo định hướng quản lý nhà nước của Kiểm toán Nhà nước và tuân theo quy định của pháp luật.

Thực hiện kiểm tra thường xuyên nhằm phát hiện và khắc phục lỗ hổng bảo mật của phần mềm, ứng dụng; cập nhật các bản nâng cấp mới và các bản vá lỗi cho phần mềm hệ thống.

3. Các đơn vị, người sử dụng không tự ý cài đặt các phần mềm, ứng dụng vào SAVNET; không tự ý làm thay đổi các thông số của các thiết bị trong hệ thống mạng máy tính. Trong trường hợp các đơn vị, người sử dụng có nhu cầu cài đặt mới, thay đổi, gỡ bỏ,… các phần mềm, ứng dụng để phục vụ hoạt động chuyên môn của đơn vị thì phải phối hợp với Trung tâm Tin học để thực hiện nhằm đảm bảo an toàn thông tin chung.

Điều 9. Quản trị hệ thống mạng

Trung tâm Tin học khi thực hiện nhiệm vụ quản trị SAVNET có trách nhiệm sau:

1. Quản lý, vận hành và giám sát SAVNET; phát hiện các hành vi sử dụng mạng không hợp lệ; xử lý các lỗi kỹ thuật; ngăn ngừa các sự cố trên mạng để đảm bảo tính an toàn, tính tin cậy và đảm bảo sự vận hành thông suốt SAVNET.

2. Thực hiện việc sao lưu dữ liệu theo kế hoạch.

3. Ghi nhật ký ca trực và thực hiện báo cáo định kỳ hoặc đột xuất khi có sự cố cho Thủ trưởng đơn vị để phối hợp xử lý.

4. Cấp địa chỉ mạng (IP address) và thông số mạng cho các đơn vị và người sử dụng tham gia SAVNET.

5. Lọc bỏ, chặn truy cập hoặc hạn chế truy cập các trang tin, ứng dụng có nghi ngờ chứa mã độc hoặc các nội dung không phù hợp phục vụ công việc.

6. Thông báo, tạm ngừng cung cấp dịch vụ; trong trường hợp nghiêm trọng có thể thu hồi tài nguyên mạng và báo cáo các cấp có thẩm quyền để xử lý đối với các đơn vị, người sử dụng vi phạm các nguyên tắc quản lý, khai thác tài nguyên trên SAVNET.

7. Tổ chức đào tạo cán bộ quản lý, triển khai, vận hành hệ thống công nghệ thông tin có kiến thức chuyên môn, nghiệp vụ về công nghệ thông tin đáp ứng yêu cầu.

8. Phối hợp với các đơn vị có thẩm quyền như: Bộ Công an, Ban Cơ yếu chính phủ, Trung tâm ứng cứu khẩn cấp máy tính Việt Nam (VN-CERT) và các đơn vị khác có liên quan để thường xuyên theo dõi và phối hợp ngăn ngừa nguy cơ tấn công mạng đảm bảo an toàn thông tin.

9. Có biện pháp dự phòng về thiết bị, phần mềm đối với các hệ thống mạng và ứng dụng, để đảm bảo sự hoạt động liên tục của hệ thống.

10. Cần cập nhật bản vá hệ điều hành, mẫu phòng diệt virus, các mẫu lỗ hổng bảo mật, mẫu tấn công,… đối với máy chủ và thiết bị tin học, chỉ thiết lập kết nối Internet cho các máy chủ hoặc thiết bị cần phải có giao tiếp ra Internet (các máy chủ, thiết bị cung cấp giao diện ra Internet như Trang thông tin điện tử, Cổng thông tin điện tử, các dịch vụ công, thư điện tử,…).

Điều 10. Quản lý, sử dụng thiết bị tin học

1. Trang thiết bị tin học do Kiểm toán Nhà nước trang bị cho các đơn vị và cá nhân là tài sản Nhà nước, được quản lý, sử dụng theo quy định của Kiểm toán Nhà nước và pháp luật về quản lý tài sản Nhà nước.

2. Các đơn vị và cá nhân có trách nhiệm quản lý trang thiết bị tin học được giao, tự bảo quản dữ liệu trên máy. Trong quá trình sử dụng các trang thiết bị tin học, nếu có sự cố xảy ra, các đơn vị, cá nhân, có trách nhiệm phối hợp với Trung tâm Tin học (trong trường hợp không tự khắc phục được) để tìm biện pháp khắc phục sự cố.

3. Trong trường hợp các đơn vị tự trang bị thiết bị tin học theo phân cấp của Kiểm toán Nhà nước phải có ý kiến tư vấn của Trung tâm Tin học về kỹ thuật, công nghệ để đảm bảo an toàn, đồng bộ khi tham gia kết nối và khai thác SAVNET. Đối với các thiết bị tin học có tính chất thông dụng, các đơn vị có thể làm chủ được kỹ thuật, công nghệ của các thiết bị thì không cần qua tư vấn của Trung tâm Tin học.

4. Các đơn vị và cá nhân sử dụng thiết bị đã kết nối với hệ thống mạng máy tính của Ngành không được tự ý thay đổi các thông số đã được cài đặt trên các thiết bị.

Điều 11. Bảo trì, nâng cấp hệ thống mạng Kiểm toán Nhà nước

1. Trung tâm Tin học chủ trì đề xuất, tham mưu giúp Tổng Kiểm toán Nhà nước trong việc lựa chọn công nghệ, đầu tư, nâng cấp, thay thế thiết bị phần cứng, phần mềm, hạ tầng truyền thông, kinh phí duy trì hoạt động hàng năm, đảm bảo hiệu quả và phù hợp với yêu cầu hoạt động của Kiểm toán Nhà nước.

2. Các đơn vị trực thuộc Kiểm toán Nhà nước xây dựng, nâng cấp, bổ sung hệ thống mạng tại đơn vị mình phải xin ý kiến và được sự đồng ý của Tổng Kiểm toán Nhà nước thông qua Trung tâm Tin học về giải pháp công nghệ hạ tầng trước khi triển khai.

3. Văn phòng Kiểm toán Nhà nước có trách nhiệm tham mưu giúp Tổng Kiểm toán Nhà nước trong việc bố trí kinh phí và phối hợp với Trung tâm Tin học trong việc đầu tư, nâng cấp, thay thế thiết bị phần cứng, phần mềm, hạ tầng truyền thông,... đảm bảo hoạt động an toàn, ổn định của SAVNET.

Chương III

ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 12. Đảm bảo an toàn thiết bị

1. Các thiết bị tại TTDL phải được vận hành và kiểm soát để phòng tránh truy cập trái phép hoặc sai mục đích. Trung tâm Tin học có trách nhiệm xây dựng nội quy vận hành TTDL.

2. Cá nhân sử dụng các thiết bị lưu trữ dữ liệu di động (máy tính xách tay, thiết bị số cầm tay, thẻ nhớ USB, ổ cứng ngoài, băng từ,…) để lưu thông tin phải có trách nhiệm bảo vệ các thiết bị này và thông tin lưu trên thiết bị, tránh làm mất, lộ thông tin; không mang ra nước ngoài thông tin của cơ quan, Nhà nước không liên quan tới nội dung công việc thực hiện ở nước ngoài.

3. Các thiết bị lưu trữ không sử dụng tiếp cho công việc của đơn vị (thanh lý, cho, tặng) phải được xóa nội dung bằng phần mềm hoặc thiết bị hủy dữ liệu chuyên dụng hay phá hủy vật lý.

Điều 13. Đảm bảo an toàn dữ liệu

1. Phân loại thông tin: Tiến hành phân loại thông tin, dữ liệu theo mức độ quan trọng, giá trị của thông tin đối với cơ quan, đơn vị về tần suất sử dụng, thời gian lưu trữ và giá trị pháp lý của nó, bảo đảm thông tin đó và tài sản gắn liền với các phương tiện xử lý thông tin một cách thích hợp cho việc phân loại.

2. Áp dụng các thuật toán mã hóa cho các hoạt động sau: đăng nhập quản trị hệ thống; đăng nhập vào các ứng dụng; gửi nhận dữ liệu tự động giữa các máy chủ; nhập và biên tập dữ liệu; tra cứu dữ liệu mật, quan trọng.

3. Các thông tin quan trọng phải được mã hóa bằng thuật toán mã hóa an toàn hoặc sử dụng công nghệ chữ ký số để xác thực và mã hóa bảo mật dữ liệu.

4. Nghiêm cấm việc soạn thảo, trao đổi, lưu trữ thông tin, tài liệu bí mật nhà nước trên máy tính có nối mạng Internet. Các cơ quan, đơn vị phải bố trí máy vi tính riêng, không kết nối mạng nội bộ và Internet dùng để soạn thảo văn bản, lưu giữ thông tin có nội dung mật theo quy định của pháp luật và của Kiểm toán Nhà nước.

5. Trung tâm Tin học xây dựng quy trình, nhân sự phục vụ công tác bảo quản, sao lưu dữ liệu và định kỳ kiểm tra dữ liệu đã sao lưu, việc sao lưu dữ liệu được thực hiện trên hệ thống sao lưu đặt tại TTDL Kiểm toán Nhà nước.

6. Các cá nhân được phân công thực hiện soạn thảo, gửi, nhận dữ liệu có trách nhiệm xác định mức độ mật, quan trọng của dữ liệu để thực hiện phương thức bảo vệ dữ liệu phù hợp hoặc yêu cầu Trung tâm Tin học hướng dẫn, hỗ trợ phương thức bảo vệ trong trường hợp cần thiết.

Điều 14. Quản lý các tài khoản trong hệ thống

1. Tài khoản cá nhân

a) Mỗi cá nhân khi sử dụng hệ thống mạng, các ứng dụng của Kiểm toán Nhà nước được cấp tài khoản truy cập với định danh duy nhất gắn với cá nhân đó. Trường hợp tài khoản dùng chung cho đơn vị thì thủ trưởng đơn vị có trách nhiệm quản lý hoặc ủy quyền cho một cá nhân quản lý tài khoản đó.

b) Thực hiện đổi mật khẩu định kỳ, tối thiểu 3 tháng một lần.

c) Mọi trường hợp cấp mới, cấp lại tài khoản và mật khẩu cho đơn vị, cá nhân phải có công văn đề nghị qua đường bưu điện hoặc gửi công văn qua thư điện tử có chữ ký số của lãnh đạo đơn vị. Khi đơn vị có cán bộ chuyển vị trí công tác hoặc nghỉ việc thì đơn vị phải có trách nhiệm thông báo cho Trung tâm Tin học để tiến hành điều chỉnh, thu hồi, hủy bỏ các quyền truy cập hệ thống và các ứng dụng đối với cán bộ đó hoặc chuyển đổi tài khoản cá nhân cho phù hợp với vị trí mới nhằm tránh tình trạng truy cập không đúng thẩm quyền vào hệ thống.

d) Trung tâm Tin học phối hợp với các đơn vị định kỳ rà soát lại các quyền truy nhập đã cấp phát nhằm phát hiện ra tình trạng phân quyền gây mất an toàn như: vượt quyền, không thu hồi khi người sử dụng đã hết quyền sử dụng, quá thời hạn sử dụng,…

2. Tài khoản quản trị:

a) Tài khoản quản trị (của thiết bị mạng, các ứng dụng, phần mềm hệ thống, cơ sở dữ liệu,…) phải tách biệt với tài khoản truy cập mạng, ứng dụng với tư cách cá nhân thông thường.

b) Tài khoản quản trị phải có định danh duy nhất và gắn với trách nhiệm cá nhân. Nghiêm cấm dùng chung tài khoản quản trị.

c) Mật khẩu phức tạp phải được áp dụng cho tất cả các tài khoản truy cập, sử dụng, quản trị hệ thống mạng, các ứng dụng trên SAVNET.

d) Thực hiện đổi mật khẩu định kỳ, tối thiểu 2 tháng một lần.

đ) Cá nhân, người làm công tác quản trị hệ thống có trách nhiệm bảo vệ thông tin tài khoản được cấp, không tiết lộ mật khẩu 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; cần cung cấp, bàn giao cho đơn vị các thông tin, tài liệu do cá nhân quản lý. Chủ tài khoản phải đổi mật khẩu ngay sau khi kết thúc xử lý các việc này.

Điều 15. Đảm bảo an toàn trong công tác quản trị hệ thống

1. Máy tính dùng để quản trị hệ thống chỉ được cài đặt các phần mềm cần thiết cho hoạt động quản trị hệ thống, đặt trong vùng mạng phục vụ công tác quản trị hệ thống và chỉ được cấp quyền truy cập cho các cá nhân được giao trách nhiệm quản trị hệ thống.

2. Thường xuyên được kiểm tra cài đặt các bản cập nhật mới cho các thiết bị tường lửa bên ngoài, tường lửa ứng dụng, IPS, Proxy, thiết bị chống Spam mail… để khắc phục các điểm yếu; có chế độ bảo trì, bảo hành hoặc thiết bị dự phòng để đảm bảo sự hoạt động liên tục của hệ thống.

3. Cá nhân làm công tác quản trị hệ thống phải thay đổi mật khẩu mặc định tài khoản quản trị của mình ngay khi được bàn giao.

4. Sử dụng kênh trao đổi thông tin an toàn (có mã hóa) khi truy cập quản trị hệ thống.

5. Tất cả các truy cập quản trị hệ thống đăng nhập (log-in), đăng xuất (log-out); các lần xác thực thành công hoặc thất bại; thời gian xảy ra; các hành động, thao tác thực thi các công cụ hệ thống,… khi quản trị viên thực hiện đều phải được ghi nhật ký quản trị để phục vụ cho việc theo dõi và quản lý.

Điều 16. Đảm bảo an toàn thông tin

1. Đối với các đơn vị và cá nhân

a) Các đơn vị cử CCVC tham gia các lớp tập huấn, bồi dưỡng do Trung tâm Tin học tổ chức để trang bị các kiến thức về an toàn thông tin phù hợp trước khi cho phép truy cập, vận hành, khai thác và sử dụng hệ thống thông tin.

b) Cá nhân đặt chế độ bảo vệ màn hình và mật khẩu sử dụng máy tính để đảm bảo an toàn cho dữ liệu cá nhân, khi không làm việc với máy tính trong thời gian dài phải thoát khỏi phiên làm việc và tắt máy. Mật khẩu tài khoản của cá nhân yêu cầu đặt mật khẩu phức tạp với độ an toàn cao để truy cập mạng, không được chuyển cho người khác sử dụng.

c) Hạn chế việc sử dụng chức năng chia sẻ tài nguyên (sharing), khi sử dụng chức năng này cần bật thuộc tính bảo mật bằng mật khẩu khi chia sẻ dữ liệu, tránh chia sẻ trực tiếp với chế độ truy cập đọc/ghi và thực hiện việc tắt chức năng này khi đã sử dụng xong.

2. Đối với Trung tâm Tin học:

a) Hàng năm có trách nhiệm tổ chức các lớp tập huấn, bồi dưỡng để trang bị các kiến thức phù hợp về an toàn thông tin trước khi cho phép truy cập, vận hành, khai thác và sử dụng hệ thống thông tin.

b) Áp dụng các biện pháp bảo đảm an toàn, bảo mật những thông tin truyền dẫn trên SAVNET.

c) Bố trí bộ phận quản trị chuyên trách về an toàn hệ thống thông tin trên môi trường mạng (bao gồm công tác giám sát, kiểm tra việc thực hiện quy định này tại Kiểm toán Nhà nước).

d) Ban hành quy trình cụ thể về việc phát hiện, báo cáo, xử lý và quản lý hoạt động khắc phục các sự cố liên quan đến an toàn thông tin tại Kiểm toán Nhà nước.

đ) Giám sát thường xuyên các hệ thống an ninh mạng để đảm bảo tác dụng của hệ thống, đồng thời phát hiện và xử lý sớm các vấn đề về an toàn thông tin. Thực hiện kết xuất định kỳ hàng tháng hoặc hàng quý các báo cáo từ hệ thống an ninh mạng để theo dõi, đánh giá các vấn đề của hệ thống.

e) Thường xuyên nghiên cứu, cập nhật các kiến thức về an toàn thông tin, có biện pháp phòng tránh các nguy cơ tiềm ẩn có thể gây mất thông tin khi tiến hành các hoạt động quản lý hay kỹ thuật nghiệp vụ.

g) Kịp thời thông báo cho các đơn vị, người sử dụng biết khi tạm dừng để nâng cấp, bảo trì định kỳ, khắc phục sự cố của từng dịch vụ mạng hoặc hệ thống mạng.

Điều 17. Phòng, chống virus tin học

1. Trung tâm Tin học có trách nhiệm:

a) Duy trì hệ thống phòng chống virus, giảm thiểu tối đa tác hại của việc lây lan, tấn công của các loại virus, các loại mã nguồn độc hại và ngăn chặn kịp thời sự bùng nổ virus trong SAVNET.

b) Thường xuyên cập nhật, cung cấp các phiên bản mới, các bản vá lỗi của phần mềm chống virus để đảm bảo chương trình quét virus của các đơn vị và cá nhân trên các máy chủ, máy trạm luôn được cập nhật mới nhất, thiết lập chế độ quét thường xuyên ít nhất là hàng tuần.

c) Lựa chọn, triển khai các phần mềm phòng chống virus, thư rác trên các máy chủ, các thiết bị di động trong mạng và những hệ thống thông tin xung yếu như: cổng thông tin điện tử,

thư điện tử, … để phát hiện, loại trừ những đoạn mã độc hại (virus, troijan, worms,…) và hỗ trợ người sử dụng cài đặt các phần mềm này trên máy trạm.

2. Các đơn vị và cá nhân sử dụng SAVNET có trách nhiệm:

a) Tuân thủ các biện pháp phòng và chống virus máy tính. Mọi dữ liệu từ các thiết bị lưu trữ bên ngoài và từ Internet đều phải được quét diệt virus trước khi sử dụng. Những máy tính phát hiện có virus phải được tách khỏi mạng về mặt vật lý để tránh tình trạng lây nhiễm sang các máy tính khác.

b) Nghiêm cấm các cá nhân sử dụng máy tính chưa cài đặt phần mềm phòng chống virus hoặc phần mềm chống virus không còn hiệu lực kết nối vào SAVNET.

Chương IV

TỔ CHỨC THỰC HIỆN

Điều 18. Trách nhiệm thi hành

1. Thủ trưởng các đơn vị trực thuộc Kiểm toán Nhà nước, CCVC, các tổ chức, cá nhân có liên quan có trách nhiệm thi hành Quy chế này.

2. Các Quy định áp dụng đối với các phần mềm ứng dụng, chính sách an ninh, bảo mật và các tài nguyên mạng khác phục vụ hoạt động của Kiểm toán Nhà nước triển khai trên SAVNET cần phải được xây dựng phù hợp với đặc thù riêng và không trái với Quy chế này.

3. Trong quá trình thực hiện nếu có khó khăn vướng mắc, cần phản ánh kịp thời về Trung tâm Tin học để tổng hợp báo cáo Tổng Kiểm toán Nhà nước sửa đổi, bổ sung cho phù hợp./.

VBPL-TS24-CORP
www.TS24.com.VN