THANH TRA CHÍNH PHỦ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 1038/QĐ-TTCP	*Hà Nội, ngày 02 tháng 5 năm 2012*

QUYẾT ĐỊNH

Về việc ban hành Quy chế an toàn, bảo mật thông tin, truyền thông trong cơ quan Thanh tra Chính phủ

TỔNG THANH TRA CHÍNH PHỦ

– Căn cứ Pháp lệnh Bảo vệ bí mật nhà nước số 30/2000/PL-UBTVQH10 ngày 28/12/2000;

– Căn cứ Nghị định số 33/2002/NĐ-CP ngày 28/12/2000 của Chính phủ quy chi tiết thi hành Pháp lệnh bảo vệ bí mật nhà nước;

– Căn cứ Quyết định số 588/2004/QĐ-BCA (A11) ngày 25/6/2005 của Bộ trưởng Bộ Công an về danh mục thông tin mật trong ngành Thanh tra;

– Căn cứ Nghị định 178/2007/NĐ-CP ngày 03/12/2007 của Chính phủ về việc quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ, cơ quan ngang bộ;

– Xét đề nghị của Giám đốc Trung tâm Thông tin Thanh tra Chính phủ,

QUYẾT ĐỊNH:

Điều 1: Ban hành kèm theo quyết định này "Quy chế an toàn, bảo mật thông tin, truyền thông trong cơ quan Thanh tra Chính phủ".

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

Điều 3: Chánh Văn phòng, Cục trưởng, Vụ trưởng, Thủ trưởng các đơn vị thuộc Thanh tra Chính phủ chịu trách nhiệm thi hành Quyết định này.

Nơi nhận:
- Như Điều 3;
- Lãnh đạo TTCP;
- Lưu: VT, TTTT.

TỔNG THANH TRA

Huỳnh Phong Tranh

THANH TRA CHÍNH PHỦ

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

QUY CHẾ
An toàn, bảo mật thông tin, truyền thông trong cơ quan Thanh tra Chính phủ

(Ban hành kèm theo Quyết định số 1038/QĐ-TTCP ngày 02 tháng 05 năm 2012 của Tổng Thanh tra Chính phủ)

Chương 1
QUY ĐỊNH CHUNG

Điều 1. Phạm vi và đối tượng áp dụng

1. Quy chế này quy định các yêu cầu đảm bảo an toàn, bảo mật thông tin và truyền thông các thông tin mật thuộc Thanh tra Chính phủ.

2. Quy chế này áp dụng đối với các cục, vụ, đơn vị (sau đây gọi chung là đơn vị) và cán bộ, công chức, viên chức, người lao động (sau đây gọi chung là người sử dụng) thuộc cơ quan Thanh tra Chính phủ.

Điều 2. Giải thích từ ngữ

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

1. *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 phục vụ cho một hoặc nhiều hoạt động kỹ thuật, nghiệp vụ của Thanh tra Chính phủ.

2. *Mạng Internet:* Là hệ thống thông tin toàn cầu có thể được truy nhập công cộng gồm các mạng máy tính được liên kết với nhau; Hệ thống này bao gồm hàng ngàn mạng máy tính nhỏ hơn của xã hội liên kết vào.

3. *Mạng LAN (mạng cục bộ):* Là một nhóm các máy tính và thiết bị truyền thông mạng được kết nối với nhau trong từng khu vực như tòa nhà, cao ốc, khu giải trí...

4. *Bản vá lỗi an ninh:* Là cập nhật phần mềm mới của Microsoft tung ra miễn phí với mục đích sửa lại các lỗi của Hệ điều hành Windows để chống lại sự tấn công của Tin tặc.

5. *Lỗ hổng phần mềm:* Là lỗi bảo mật thuộc về lỗi một phần mềm hoặc một phần cứng đã bị mã độc nhiễm vào thông qua lỗ hổng đó; lỗ hổng phần mềm là lỗi về bảo mật trong hệ điều hành hoặc phần mềm; nhà cung cấp hệ điều hành hoặc phần mềm thường sẽ cung cấp phần mềm miễn phí chương trình sữa lỗi, đặc biệt là các trình duyệt Web phiên bản cũ có thể vẫn còn các lỗ hổng bảo

mật chưa được khắc phục và Tin tặc có thể dựa vào đó để xâm nhập vào máy tính đánh cắp thông tin người dùng.

6. *Tin tặc (Hacker):* Là những chuyên gia lập trình chuyên tìm các lỗi của phần mềm để xâm nhập vào hệ thống thông qua những lỗ hổng bảo mật với mục đích tấn công trái phép vào các hệ thống phần mềm để phá hoại, lấy cắp, sửa chữa, thay thế thông tin gây hậu quả nghiêm trọng.

7. *Hệ thống an ninh mạng:* Là tập hợp các thiết bị tường lửa; thiết bị kiểm soát, phát hiện truy cập bất hợp pháp; phần mềm quản trị, theo dõi, ghi nhật ký trạng thái an ninh mạng và các trang thiết bị khác có chức năng đảm bảo an toàn hoạt động của mạng, tất cả cùng hoạt động đồng bộ theo một chính sách an ninh mạng nhất quán nhằm kiểm soát chặt chẽ tất cả các hoạt động trên mạng.

8. *Tường lửa:* Là tập hợp các thành phần hoặc một hệ thống các trang thiết bị, phần mềm được đặt giữa hai mạng, nhằm kiểm soát tất cả các kết nối từ bên trong ra bên ngoài mạng hoặc ngược lại.

9. *Vi rút:* Là chương trình máy tính có khả năng lây lan, gây ra hoạt động không bình thường cho thiết bị số hoặc sao chép, sửa đổi, xóa bỏ thông tin lưu trữ trong thiết bị số.

10. *Phần mềm độc hại (mã độc):* Là các phần mềm có tính năng gây hại như vi rút, phần mềm do thám (spyware), phần mềm quảng cáo (adware) hoặc các dạng tương tự khác.

11. *Điểm yếu kỹ thuật:* Là vị trí trong hệ thống Công nghệ thông tin dễ bị tổn thương khi bị tấn công hoặc xâm nhập bất hợp pháp.

12. *Mã hóa:* Là quá trình biến đổi thông tin từ dạng ban đầu thành dạng khác không thể đọc và hiểu được (như file nén hoặc các định dạng khác), với mục đích giữ bí mật thông tin đó.

13. *Giải mã:* Là quá trình ngược lại với mã hóa, khôi phục lại thông tin ban đầu từ thông tin đã được mã hóa.

Điều 3. Nguyên tắc chung

Mỗi đơn vị phải:

1. Đảm bảo an toàn, bảo mật thông tin, truyền thông của đơn vị mình theo các quy định tại Quy chế này.

2. Phân loại, đánh giá và xử lý kịp thời khi có sự cố về an toàn, bảo mật thông tin xảy ra.

3. Xây dựng, triển khai quy chế an toàn, bảo mật thông tin, truyền thông trên cơ sở giảm thiểu thiệt hại tối đa khi xảy ra sự cố.

4. Bố trí đủ nguồn nhân lực có chất lượng phù hợp nhằm đảm bảo an toàn, bảo mật thông tin, truyền thông tốt nhất.

5. Xác định rõ quyền hạn, trách nhiệm của thủ trưởng đơn vị, trách nhiệm của từng cá nhân trong đơn vị đối với công tác đảm bảo an toàn, bảo mật thông tin, truyền thông.

Điều 4. Trách nhiệm của các đơn vị và người sử dụng

1. Người sử dụng làm công tác có liên quan trực tiếp đến an toàn, bảo mật thông tin, truyền thông phải có ý thức cảnh giác bảo mật, có tinh thần trách nhiệm cao, có chuyên môn, nghiệp vụ và năng lực để hoàn thành tốt nhiệm vụ được giao và thực hiện đầy đủ các quy định tại quy chế này.

2. Thủ trưởng các đơn vị thường xuyên hướng dẫn, kiểm tra, sơ kết, tổng kết công tác an toàn, bảo mật thông tin, truyền thông; rà soát, củng cố, kiện toàn tổ chức, xây dựng đội ngũ đủ mạnh để thực hiện tốt nhiệm vụ trong tình hình mới; chấp hành nghiêm túc quy định về chế độ thông tin, báo cáo về công tác an toàn, bảo mật thông tin, truyền thông; có biện pháp chủ động phòng ngừa, không để xảy ra các vụ lộ, lọt thông tin mật; phối hợp chặt chẽ với các cơ quan chức năng trong việc phát hiện, xử lý và khắc phục hậu quả kịp thời các vụ lộ, lọt các thông tin mật.

3. Các đơn vị tổ chức tốt công tác an toàn, bảo mật thông tin, truyền thông; xây dựng đội ngũ người sử dụng đáp ứng các tiêu chuẩn về chính trị, trình độ, năng lực, nhất là số người sử dụng làm việc tại các bộ phận trọng yếu, cơ mật hoặc có điều kiện tiếp xúc thông tin mật.

Điều 5. Những hành vi bị nghiêm cấm

1. Nghiêm cấm mọi hành vi thu thập, cung cấp, làm lộ, làm mất, chiếm đoạt, mua bán, tiêu hủy trái phép các thông tin mật của Thanh tra Chính phủ.

2. Nghiêm cấm mọi hành vi tiếp tay cho Tin tặc xâm nhập trái phép vào hệ thống thông tin, lấy cắp và phá hoại hệ thống an toàn, bảo mật thông tin, truyền thông.

3. Nghiêm cấm cung cấp thông tin, tài liệu mật để đăng tải trên Cổng thông tin điện tử Thanh tra Chính phủ.

4. Nghiêm cấm trao đổi thông tin mật qua điện thoại và các thiết bị liên lạc khác chưa được bảo mật thiết bị, đường truyền.

Chương 2
CÁC QUY ĐỊNH VỀ ĐẢM BẢO AN TOÀN, BẢO MẬT THÔNG TIN, TRUYỀN THÔNG

MỤC 1. ĐẢM BẢO AN TOÀN, BẢO MẬT THÔNG TIN, TRUYỀN THÔNG

Điều 6. An toàn, bảo mật thông tin, truyền thông trong nội bộ đơn vị

1. Thủ trưởng đơn vị phải trực tiếp chỉ đạo công tác an toàn, bảo mật thông tin, truyền thông và quy định rõ trách nhiệm cho từng cá nhân, bộ phận.

2. Các cá nhân trong đơn vị liên quan đến bảo mật thông tin phải ký cam kết an toàn, bảo mật thông tin, truyền thông. Tuyệt đối không được cung cấp, sao chép trái phép các thông tin vào mục đích chính trị, kinh tế, tôn giáo hoặc vi phạm các quy định của pháp luật hiện hành. Không tiến hành các hành động

gian lận hoặc can thiệp trái phép vào hệ thống nhằm truy xuất thông tin không thuộc thẩm quyền của mình hoặc tạo dữ liệu giả, thay đổi dữ liệu trong hệ thống.

Điều 7. An toàn và bảo mật thông tin trong Cổng thông tin điện tử Thanh tra Chính phủ

1. Người sử dụng khi không dùng máy tính phải tắt máy; các máy đang thực hiện tác nghiệp không có nhu cầu khai thác thông tin trên Internet phải ngắt ngay kết nối ra khỏi mạng để giảm thiểu nguy cơ Tin tặc truy cập trái phép, đánh cắp dữ liệu thông tin mật.

2. Người sử dụng tuyệt đối không được soạn thảo các văn bản mật trên máy tính của người khác bởi trên máy đó không biết chắc họ đã cài phần mềm bảo mật chưa.

3. Người sử dụng máy tính cá nhân phải cài đặt các phần mềm bảo mật và tường lửa để ngăn chặn các phần mềm gián điệp và Tin tặc xâm nhập trái phép, đánh cắp các thông tin mật.

4. Người sử dụng tuyệt đối không được tự ý sửa, gỡ bỏ hoặc thay đổi hệ thống phần mềm bảo mật và tường lửa đang cài trong máy tính bởi khi gỡ bỏ thì máy tính sẽ mất tính năng bảo vệ, tạo điều kiện cho Tin tặc tấn công.

5. Người sử dụng thường xuyên cập nhật các bản vá lỗi an ninh để máy tự động cài đặt vá lỗi các lỗ hổng đảm bảo Virus không tấn công xâm nhập trái phép qua lỗ hổng.

6. Việc lưu trữ thông tin mật tại các máy tính cá nhân và tại Trung tâm lưu trữ dữ liệu của Thanh tra Chính phủ phải được thực hiện theo phương pháp lưu trữ song hành (lưu vào nhiều chỗ); các thiết bị lưu trữ phải có tính năng an toàn, bền vững và được trang bị các phần mềm bảo mật, tường lửa.

7. Trong quá trình sao lưu, phục hồi dữ liệu để xảy ra sự cố có thể do người sử dụng không sao lưu được, hoặc vô tình bị xóa dữ liệu thì phải liên hệ ngay với Trung tâm Thông tin để được trợ giúp.

Điều 8. An toàn và bảo mật thông tin Hộp thư điện tử.

1. Người sử dụng khi gửi các văn bản mật qua hệ thống thư điện tử hoặc qua đường Internet cần được mã hóa văn bản (có thể nén file hoặc chuyển sang định dạng khác) trước khi gửi. Trong trường hợp không thể mã hóa được phải báo ngay cho Trung tâm Thông tin để được trợ giúp.

2. Người sử dụng khi truy cập vào Hộp thư điện tử, tuyệt đối không được mở các thư lạ, không rõ nguồn gốc, các tệp tin đính kèm hoặc các liên kết trong các thư lạ để tránh vi rút, mã độc tấn công.

3. Người sử dụng phải tuyệt đối giữ bí mật về tài khoản và mật khẩu cá nhân trong Hộp thư điện tử.

4. Khi tổ chức lấy ý kiến để xây dựng dự thảo văn bản có nội dung mật của Thanh tra Chính phủ và các văn bản liên quan với các cơ quan, tổ chức, cá nhân khác, thì đơn vị chủ trì soạn thảo tuyệt đối không được gửi xin ý kiến qua

đường mạng (Internet và LAN), thư điện tử và qua các phương tiện truyền thông khác.

5. Ngoài ra, người sử dụng không những phải tuân thủ các quy định an toàn, bảo mật thông tin, truyền thông trong việc khai thác, sử dụng hộp thư điện tử tại quy chế này, mà còn phải tuân thủ theo các quy định của quy chế quản lý và sử dụng Công nghệ Thông tin tại cơ quan Thanh tra Chính phủ đã được ban hành.

Điều 9. An toàn, bảo mật thông tin trong lĩnh vực truyền thông

1. Việc trao đổi thông tin có nội dung mật của Thanh tra Chính phủ trên mạng viễn thông, Internet phải được bảo mật theo quy định của pháp luật về cơ yếu.

2. Các đơn vị phải xây dựng phương án đảm bảo tuyệt đối an toàn, bảo mật thông tin trong hệ thống cơ sở dữ liệu máy tính. Quản lý chặt chẽ các thiết bị, phương tiện kỹ thuật có chức năng lưu trữ thông tin (như USB, thẻ nhớ…), các phương tiện có nguồn gốc nước ngoài, không rõ xuất xứ (biếu, tặng, nhập khẩu…) được trang bị cho các tổ chức, cá nhân có điều kiện tiếp xúc với thông tin mật để phòng ngừa hoạt động thu thập, lấy cắp chiếm đoạt thông tin mật.

Điều 10. An toàn, bảo mật thông tin trong lĩnh vực xuất bản báo chí điện tử trên Cổng thông tin điện tử Thanh tra Chính phủ

1. Quản lý chặt chẽ việc trao đổi, cung cấp thông tin cho báo chí, báo chí điện tử và các phương tiện thông tin, truyền thông đại chúng. Việc viết tin, bài đưa lên Cổng thông tin điện tử Thanh tra Chính phủ phải chấp hành các quy định của pháp luật hiện hành về an toàn, bảo mật thông tin, truyền thông.

2. Quy trình đăng tải tin, bài, hình ảnh, Video Clip, tệp đính kèm v.v phải tuân thủ đúng quy định về bảo vệ bí mật nhà nước và các quy định về an toàn, bảo mật thông tin, truyền thông. Thực hiện nghiêm túc Quyết định số 77/QĐ-Ttg ngày 18 tháng 5 năm 2007 của Thủ tướng Chính phủ về Quy chế phát ngôn và cung cấp thông tin cho báo chí.

Điều 11. An toàn, bảo mật thông tin, truyền thông trong việc soạn thảo, in ấn, sao chép, lưu trữ văn bản mật

1. Khi soạn thảo, in ấn, sao chép, lưu trữ các văn bản mật của Thanh tra Chính phủ phải tuân theo các quy định về bảo mật thông tin. Không được sử dụng máy vi tính đã và đang kết nối mạng Internet, kết nối mạng nội bộ (mạng LAN) và các phương thức kết nối khác để soạn thảo, in ấn, sao chép, lưu trữ văn bản mật.

2. Thủ trưởng các đơn vị giao cho người có đủ tiêu chuẩn quy định tại Quy chế này thực hiện nhiệm vụ soạn thảo, in ấn, sao chép, lưu trữ tài liệu mật. Không thuê người ngoài cơ quan soạn thảo, in ấn, sao chép, lưu trữ tài liệu mật.

3. Người có trách nhiệm soạn thảo, in ấn, sao chép, lưu trữ tài liệu mật của Thanh tra Chính phủ chỉ được in đủ số lượng văn bản yêu cầu; các văn bản in hỏng phải đưa vào máy hủy tài liệu và hủy ngay. Sau khi hoàn thành việc in

tài liệu xong phải xóa ngay dữ liệu, trường hợp đặc biệt chỉ được lưu đến khi văn bản phát hành.

4. Trong quá trình đang soạn thảo dự thảo các kết luận thanh tra, kết luận giải quyết khiếu nại, tố cáo và các dự thảo văn bản khác liên quan đến công tác thanh tra, giải quyết khiếu nại, tố cáo và phòng, chống tham nhũng phải tuân thủ theo đúng quy định như các văn bản cần bảo mật.

Điều 12. An toàn, bảo mật thông tin, truyền thông trong các hoạt động tác nghiệp

1. Trong quá trình tác nghiệp, trưởng đoàn thanh tra, các thành viên trong đoàn thanh tra và những người có liên quan phải tuyệt đối bảo mật thông tin liên quan đến các hoạt động đang thanh tra; không viết bài, không đưa tin bình luận về nội dung các vụ việc đang thanh tra; nghiêm cấm không được gửi các tài liệu cũng như điện thoại tiết lộ các thông tin đang quá trình thanh tra, giải quyết khiếu nại, tố cáo, phòng chống tham nhũng.

2. Trưởng đoàn và các thành viên đoàn thanh tra phải quản lý an toàn các tài liệu, hồ sơ trong suốt quá trình thanh tra. Mọi trường hợp trao đổi, cung cấp tình hình, số liệu thông tin đang thanh tra cho các cơ quan, tổ chức, cá nhân phải được sự đồng ý của người ra quyết định thanh tra, giải quyết khiếu nại, tố cáo, phòng chống tham nhũng và phải chịu trách nhiệm về việc cung cấp thông tin này.

3. Các đơn vị lưu giữ tài liệu, thông tin trong suốt quá trình thanh tra hoặc kết thúc thanh tra, khi có yêu cầu cung cấp tài liệu, thông tin phải được cấp có thẩm quyền xét duyệt, tuyệt đối không được tự ý cung cấp. Người thực hiện chỉ được cung cấp tài liệu mật theo đúng nội dung được duyệt. Bên nhận thông tin không được làm lộ, lọt và không được cung cấp thông tin đã nhận cho người khác.

MỤC 2. NGUỒN NHÂN LỰC TRONG AN TOÀN, BẢO MẬT THÔNG TIN, TRUYỀN THÔNG

Điều 13. Phân công nhiệm vụ thực hiện an toàn, bảo mật thông tin, truyền thông

1. Xác định trách nhiệm về an toàn, bảo mật thông tin, truyền thông của vị trí được phân công.

2. Kiểm tra lý lịch, xem xét đánh giá nghiêm ngặt tư cách đạo đức, trình độ chuyên môn, phân công người sử dụng làm việc tại các vị trí trọng yếu trong công việc an toàn, bảo mật thông tin, truyền thông như quản trị hệ thống, quản trị hệ thống an ninh bảo mật, vận hành hệ thống, quản trị cơ sở dữ liệu.

3. Quyết định hoặc hợp đồng tuyển dụng (nếu có) phải bao gồm các điều khoản về trách nhiệm đảm bảo an toàn, bảo mật thông tin, truyền thông của người được tuyển dụng trong và sau khi làm việc tại đơn vị.

Điều 14. Quản lý nguồn nhân lực trong thời gian làm việc

1. Các đơn vị có trách nhiệm phổ biến và cập nhật các quy định về an toàn, bảo mật thông tin, truyền thông cho người sử dụng.

2. Tổ chức kiểm tra việc thực hiện quy định về an toàn, bảo mật thông tin, truyền thông của người sử dụng tối thiểu mỗi năm một lần theo hướng dẫn của Trung tâm Thông tin.

3. Các công việc quan trọng như cấu hình hệ thống an ninh mạng, thay đổi tham số hệ điều hành, cài đặt thiết bị tường lửa, thiết bị phát hiện và ngăn chặn xâm nhập phải được thực hiện bởi ít nhất hai người hoặc phải có người giám sát.

4. Không được cấp quyền quản trị trên hệ thống bảo mật chính và hệ thống dự phòng cho cùng một cá nhân.

Điều 15. Nhân lực khi thôi không làm công việc an toàn, bảo mật thông tin, truyền thông

1. Lập biên bản bàn giao toàn bộ những công việc người sử dụng đã làm sang cho người sử dụng mới hoặc thủ trưởng đơn vị đó tiếp nhận.

2. Thu hồi hoặc thay đổi quyền truy cập đã cấp phát vào hệ thống bảo mật cho người sử dụng đã chấm dứt công việc.

MỤC 3. AN TOÀN, BẢO MẬT THÔNG TIN, TRUYỀN THÔNG TRONG VẬN HÀNH HỆ THỐNG

Điều 16. An toàn, bảo mật trong sao lưu dự phòng

1. Thực hiện quy trình sao lưu dự phòng và phục hồi dữ liệu cho các phần mềm, các Cơ sở dữ liệu cần thiết.

2. Thống kê danh sách các dữ liệu, phần mềm cần được sao lưu, có phân loại theo thời gian lưu trữ, thời gian sao lưu, phương pháp sao lưu và thời gian kiểm tra phục hồi hệ thống từ dữ liệu sao lưu để đảm bảo dữ liệu được an toàn.

3. Các dữ liệu sao lưu phải được lưu trữ an toàn và được kiểm tra thường xuyên đảm bảo sẵn sàng cho việc sử dụng khi cần. Kiểm tra, phục hồi hệ thống từ dữ liệu sao lưu tối thiểu sáu tháng một lần.

Điều 17. An toàn, bảo mật trong hệ thống mạng

1. Thường xuyên kiểm tra, kiểm soát hệ thống mạng nhằm ngăn ngừa các nguy cơ xảy ra cho các hệ thống mạng

2. Sử dụng các thiết bị tường lửa, thiết bị phát hiện và ngăn chặn xâm nhập trái phép và các trang thiết bị khác đảm bảo an toàn bảo mật mạng.

3. Cài đặt cấu hình đầy đủ các tính năng của thiết bị an ninh mạng. Sử dụng các công cụ để dò tìm và phát hiện kịp thời các điểm yếu, lỗ hổng và các truy cập trái phép vào hệ thống mạng. Thường xuyên kiểm tra, phát hiện những kết nối, trang thiết bị, phần mềm gián điệp cài đặt bất hợp pháp vào mạng.

Điều 18. An toàn, bảo mật thông tin trong giám sát, ghi nhật ký

1. Thực hiện việc giám sát, ghi nhật ký thời gian lưu trữ các thông tin để phát hiện kịp thời các lỗi phát sinh, các sự cố mất an toàn thông tin nhằm khắc phục sớm sẽ tránh được hậu quả thiệt hại nghiêm trọng.

2. Lập báo cáo định kỳ theo ghi chép nhật ký để có hướng khắc phục, xử lý các lỗi, các sự cố cần thiết.

3. Bảo vệ các chức năng hệ thống tự động ghi nhật ký và thông tin nhật ký, chống giả mạo, truy cập trái phép làm sai lệch thông số nhật ký, dẫn đến quá trình xử lý lỗi sai gây thiệt hại nghiêm trọng. Người quản trị hệ thống và người sử dụng không được xóa hay sửa đổi nhật ký hệ thống ghi lại các hoạt động của hệ thống.

Điều 19. An toàn, bảo mật thông tin trong việc phòng chống vi rút và các phần mềm độc hại

1. Triển khai hệ thống phòng chống vi rút máy tính cho toàn bộ hệ thống Công nghệ thông tin của các đơn vị và của Trung tâm tích hợp dữ liệu.

2. Thường xuyên kiểm tra, diệt vi rút, mã độc cho toàn bộ hệ thống công nghệ thông tin của các đơn vị, Trung tâm tích hợp dữ liệu và các phương tiện mang tin (USB, thẻ nhớ, đĩa CD ROM, DVD…) nhận từ bên ngoài vào trước khi sử dụng.

3. Người sử dụng không vào các trang web không có nguồn gốc xuất xứ rõ ràng.

4. Người sử dụng thường xuyên cập nhật kịp thời các mẫu vi rút, mã độc mới và các phần mềm chống vi rút, mã độc mới.

5. Người sử dụng phát hiện vi rút, mã độc nhưng không diệt được phải báo ngay cho Trung tâm thông tin để xử lý kịp thời.

6. Người sử dụng không tự ý cài đặt các phần mềm khi chưa được phép của Trung tâm Thông tin.

MỤC 4. AN TOÀN, BẢO MẬT THÔNG TIN, TRUYỀN THÔNG TRONG TRUY CẬP MẠNG

Điều 20. An toàn, bảo mật thông tin trong kiểm soát truy cập

1. Người sử dụng phải thực hiện các quy định về quản lý truy cập, đảm bảo đáp ứng yêu cầu về an toàn, bảo mật thông tin. Quy định về quản lý truy cập bao gồm: Đăng ký, cấp phát, gia hạn và thu hồi quyền truy cập của người sử dụng; giới hạn và kiểm soát các truy cập đặc quyền; quản lý, cấp phát mật khẩu; rà soát, kiểm tra, xét duyệt lại quyền truy cập của người sử dụng.

2. Người sử dụng phải tuân thủ theo các quy định về quản lý mật khẩu như sau: Mật khẩu phải có độ dài sáu ký tự trở lên, cấu tạo gồm các ký tự số, chữ và các ký tự đặc biệt khác nếu hệ thống cho phép; các mật khẩu mặc định của nhà sản xuất cài đặt sẵn trên các trang thiết bị, phần mềm, cơ sở dữ liệu phải được thay đổi ngay khi đưa vào sử dụng; phần mềm quản lý mật khẩu phải có các chức năng: Thông báo người sử dụng thay đổi mật khẩu sắp hết hạn sử

dụng; hủy hiệu lực của mật khẩu hết hạn sử dụng; cho phép thay đổi ngay mật khẩu bị lộ, có nguy cơ bị lộ hoặc theo yêu cầu của người sử dụng; ngăn chặn việc sử dụng lại mật khẩu cũ trong một khoảng thời gian nhất định.

3. Trách nhiệm người sử dụng khi được cấp quyền truy cập: Sử dụng mật khẩu đúng quy định, giữ bí mật mật khẩu, thoát khỏi hệ thống khi không làm việc trên hệ thống hoặc tạm thời không làm việc trên hệ thống.

Điều 21. An toàn, bảo mật thông tin trong việc truy cập mạng

1. Người sử dụng phải tuân thủ các quy định sử dụng mạng và các dịch vụ mạng; các thủ tục cấp phép, xóa bỏ quyền kết nối đến mạng và dịch vụ mạng; những cách thức, phương tiện truy cập mạng, dịch vụ mạng.

2. Người sử dụng tuân thủ các biện pháp thích hợp để xác thực kết nối từ bên ngoài vào mạng nội bộ của cơ quan Thanh tra Chính phủ đảm bảo an toàn, bảo mật thông tin.

3. Trung tâm Thông tin phân chia mạng LAN cơ quan thành các mạng riêng ảo cho từng đơn vị để đảm bảo cho các đơn vị truy cập mạng độc lập, tránh sự truy cập trái phép.

Điều 22. An toàn, bảo mật thông tin trong việc truy cập hệ điều hành

1. Người sử dụng tuân thủ các quy trình kiểm soát truy cập hệ điều hành; quy định quản lý mật khẩu truy cập hệ điều hành an toàn, bảo mật.

2. Người sử dụng phải có một tài khoản duy nhất và được xác thực, nhận dạng, lưu dấu vết khi truy cập hệ điều hành.

3. Người sử dụng có thể sử dụng thêm các phương pháp xác thực khác như vân tay hoặc thẻ đối với các máy tính quan trọng ngoài việc xác thực bằng mật khẩu.

4. Người sử dụng tự động ngắt phiên làm việc sau một thời gian không sử dụng, nhằm ngăn chặn sự truy cập trái phép.

5. Người sử dụng cài đặt giới hạn thời gian kết nối với những ứng dụng cần an toàn, bảo mật cao.

Điều 23. An toàn, bảo mật thông tin trong phân quyền truy cập hệ thống và phần mềm ứng dụng

1. Trung tâm Thông tin phân quyền truy cập hệ thống và phần mềm ứng dụng theo chức năng nhiệm vụ của người sử dụng: Phân quyền truy cập đến từng thư mục, chức năng của chương trình; phân quyền đọc, ghi, xóa, thực thi đối với thông tin, dữ liệu, chương trình.

2. Các hệ thống thông tin quan trọng, cần an toàn, bảo mật cao cần phải đặt trong môi trường mạng máy tính riêng. Nếu các hệ thống thông tin cùng sử dụng nguồn tài nguyên chung thì phải được phép của cấp có thẩm quyền chấp nhận.

MỤC 5. AN TOÀN, BẢO MẬT TRONG HỆ THỐNG THÔNG TIN

Điều 24. An toàn, bảo mật thông tin trong các ứng dụng

1. Thường xuyên kiểm tra tính hợp lệ của dữ liệu nhập vào các ứng dụng, đảm bảo dữ liệu được nhập vào chính xác và hợp lệ.

2. Thường xuyên kiểm tra tính hợp lệ của dữ liệu cần được xử lý tự động trong các ứng dụng nhằm phát hiện thông tin sai lệch do các lỗi trong quá trình xử lý hoặc các hành vi sửa đổi thông tin theo mục đích riêng.

3. Thường xuyên kiểm tra tính hợp lệ của dữ liệu xuất ra từ các ứng dụng, đảm bảo quá trình xử lý thông tin của các ứng dụng là chính xác và hợp lệ.

4. Phải có các biện pháp đảm bảo tính xác thực và bảo vệ sự toàn vẹn của dữ liệu được xử lý trong các ứng dụng.

Điều 25. An toàn, bảo mật thông tin trong mã hóa dữ liệu

1. Người sử dụng khi thực hiện các tác nghiệp (gửi, truyền lên mạng và lưu trữ dữ liệu) trên các thông tin mật cần phải mã hóa dữ liệu; sử dụng các biện pháp mã hóa theo các chuẩn quốc gia hoặc quốc tế đã được công nhận để bảo vệ thông tin của đơn vị (các giải thuật mã hóa như: AES: Advanced Encryption Standard; 3DES: Triple Data Encryption Standard; RSA: Rivest-Shamir-Adleman; giải thuật khác).

2. Tất cả các dữ liệu về mật khẩu người dùng và các dữ liệu nhạy cảm khác phải được mã hóa khi gửi, truyền lên mạng và khi lưu trữ dữ liệu.

Điều 26. An toàn, bảo mật thông tin trong các tệp tin hệ thống

1. Khi cài đặt, cập nhật thêm các phần mềm ứng dụng lên hệ thống hiện tại, phải đảm bảo an toàn cho các tệp tin hệ thống sẵn có trong hệ thống.

2. Khi truy cập vào chương trình nguồn (bản quyền một chương trình của nhà sản xuất) phải được quản lý và kiểm soát chặt chẽ.

Điều 27. An toàn, bảo mật thông tin trong các điểm yếu về mặt kỹ thuật

1. Thường xuyên phải đánh giá, quản lý và kiểm soát các điểm yếu kỹ thuật của các hệ thống thông tin đang sử dụng. Định kỳ đánh giá, lập báo cáo về các điểm yếu kỹ thuật của các hệ thống thông tin đang sử dụng.

2. Phải có kế hoạch cụ thể triển khai các giải pháp khắc phục các điểm yếu kỹ thuật, hạn chế các rủi ro liên quan.

MỤC 6. AN TOÀN, BẢO MẬT THÔNG TIN KHI CÓ SỰ CỐ

Điều 28. An toàn, bảo mật thông tin trong báo cáo sự cố

1. Phải xây dựng quy trình báo cáo, các mẫu báo cáo và xác định rõ người nhận báo cáo về các sự cố an toàn, bảo mật thông tin.

2. Phải quy định rõ trách nhiệm báo cáo của người sử dụng về các sự cố an toàn, bảo mật thông tin.

3. Khi có sự cố mất an toàn xảy ra, ngay lập tức phải báo cáo cho người có thẩm quyền và những người có liên quan để có biện pháp khắc phục trong thời gian sớm nhất.

Điều 29. An toàn, bảo mật thông tin trong kiểm soát và khắc phục sự cố

1. Người sử dụng phải có trách nhiệm khắc phục và phòng ngừa sự cố an toàn, bảo mật thông tin; đảm bảo sự cố được xử lý trong thời gian ngắn nhất và giảm thiểu khả năng sự cố lặp lại.

2. Trong quá trình xử lý sự cố phải được ghi chép và lưu trữ đầy đủ tại đơn vị.

3. Quá trình khắc phục, phòng ngừa các sự cố phải được ghi chép, bảo toàn bằng chứng, chứng cứ phục vụ cho việc kiểm tra, xử lý, khắc phục và phòng ngừa sự cố. Trong trường hợp sự cố về an toàn, bảo mật thông tin có liên quan đến các vi phạm pháp luật, đơn vị có trách nhiệm thu thập và cung cấp chứng cứ cho cơ quan có thẩm quyền đúng theo quy định của pháp luật.

MỤC 7. AN TOÀN, BẢO MẬT THÔNG TIN, TRUYỀN THÔNG TRONG HOẠT ĐỘNG LIÊN TỤC CỦA HỆ THỐNG CNTT

Điều 30. An toàn, bảo mật thông tin trong các hoạt động liên tục

1. Phải luôn đảm bảo an toàn, bảo mật thông tin cho hệ thống hoạt động liên tục 24h/24h, đáp ứng yêu cầu công việc của đơn vị.

2. Xây dựng và triển khai kế hoạch, quy trình đảm bảo hoạt động liên tục của các hệ thống an toàn, bảo mật thông tin trọng yếu.

3. Quá trình kiểm tra, đánh giá phải tuân thủ tối thiểu sáu tháng một lần để tiến hành đánh giá và cập nhật các quy trình đảm bảo hoạt động liên tục của các hệ thống an toàn, bảo mật thông tin trọng yếu.

Điều 31. An toàn, bảo mật thông tin trong dự phòng thảm họa

1. Phải xây dựng hệ thống dự phòng cho các hệ thống an toàn, bảo mật thông tin trọng yếu của đơn vị.

2. Hệ thống dự phòng phải thay thế được hệ thống chính trong vòng 4 giờ kể từ khi hệ thống chính có sự cố không khắc phục được.

3. Tối thiểu ba tháng một lần, phải chuyển hoạt động từ hệ thống chính sang hệ thống dự phòng để đảm bảo tính đồng nhất và sẵn sàng của hệ thống dự phòng.

4. Tối thiểu ba tháng một lần, tiến hành kiểm tra, đánh giá hoạt động của hệ thống dự phòng.

Chương 3
ĐIỀU KHOẢN THI HÀNH

Điều 32. Xử lý vi phạm

Các đơn vị, cá nhân vi phạm quy định tại Quy chế này, tùy theo mức độ vi phạm sẽ bị xử lý theo các quy định của pháp luật.

Điều 33. Hiệu lực thi hành

1. Quy chế này có hiệu lực thi hành kể từ ngày ký ban hành.

2. Trong quá trình thực hiện nếu có vấn đề phát sinh, vướng mắc, các đơn vị liên quan phản ánh kịp thời về Trung tâm Thông tin, Thanh tra Chính phủ để trình Tổng Thanh tra Chính phủ xem xét, bổ sung, sửa đổi.

Điều 34. Trách nhiệm thi hành

1. Trung tâm Thông tin có trách nhiệm theo dõi, kiểm tra việc thi hành Quy chế này tại các cục, vụ, đơn vị.

2. Việc thực hiện công tác an toàn, bảo mật thông tin, truyền thông của Thanh tra Chính phủ là trách nhiệm của các đơn vị, cá nhân thuộc Thanh tra Chính phủ. Trong phạm vi chức năng nhiệm vụ, quyền hạn được giao, thủ trưởng các đơn vị thuộc Thanh tra Chính phủ có trách nhiệm tổ chức triển khai và kiểm tra việc thi hành tại đơn vị mình theo đúng các quy định của Quy chế này.

3. Chánh Văn phòng, Giám đốc Trung tâm Thông tin có trách nhiệm theo dõi, hướng dẫn, kiểm tra, tổng hợp tình hình thực hiện công tác an toàn, bảo mật thông tin, truyền thông trong toàn cơ quan Thanh tra Chính phủ.

4. Ngoài các quy định về an toàn, bảo mật thông tin, truyền thông của Thanh tra Chính phủ tại Quy chế này, cần phải thực hiện các quy định của Pháp lệnh về bảo vệ bí mật Nhà nước đã ban hành.

TỔNG THANH TRA

Huỳnh Phong Tranh