UBND TỈNH BÌNH ĐỊNH **SỞ TƯ PHÁP**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 161/QĐ-STP	*Bình Định, ngày 30 tháng 11 năm 2020*

QUYẾT ĐỊNH
Ban hành Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của Sở Tư pháp

GIÁM ĐỐC SỞ TƯ PHÁP

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 Quyết định số 22/QĐ-UBND ngày 12 tháng 7 năm 2012 của UBND tỉnh Bình Định về việc ban hành Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan quản lý hành chính nhà nước tỉnh Bình Định;

Căn cứ Quyết định số 2581/QĐ-UBND ngày 24 tháng 7 năm 2015 của UBND tỉnh Bình Định về việc ban hành Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Sở Tư pháp tỉnh Bình Định; Quyết định số 170/QĐ-UBND ngày 19 tháng 01 năm 2018 của UBND tỉnh Bình Định sửa đổi Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Sở Tư pháp tỉnh Bình Định ban hành kèm theo Quyết định số 2581/QĐ-UBND ngày 24 tháng 7 năm 2015 của UBND tỉnh Bình Định;

Theo đề nghị của Chánh Văn phòng Sở Tư pháp.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của Sở Tư pháp.

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

Điều 3. Chánh Văn phòng Sở, Chánh Thanh tra Sở, Trưởng các phòng chuyên môn, Thủ trưởng các đơn vị trực thuộc Sở và cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Sở Thông tin & TT;
- Lãnh đạo Sở;
- Website Sở;
- Lưu: VT, VP.

GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ TƯ PHÁP
TỈNH BÌNH ĐỊNH

Sở Tư pháp
Tỉnh Bình Định
30-11-2020 09:25:26 +07:00

Lê Văn Toàn

QUY CHẾ
Đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của Sở Tư pháp

(Ban hành kèm theo Quyết định số /QĐ-STP ngày /11/2020 của Giám đốc Sở Tư pháp Bình Định)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi, đối tượng áp dụng và mục đích

1. Quy chế này quy định về bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của Sở Tư pháp tỉnh Bình Định.

2. Quy chế này áp dụng đối với tất cả các phòng chuyên môn, đơn vị trực thuộc; công chức, viên chức và người lao động và các đối tượng tham gia vận hành, khai thác các hệ thống thông tin của Sở Tư pháp.

3. Mục đích đảm bảo an toàn, an ninh thông tin: Giảm thiểu được các nguy cơ gây sự cố mất an toàn, an ninh thông tin và đảm bảo an toàn về dữ liệu, các thiết bị công nghệ thông tin trong hoạt động ứng dụng công nghệ thông tin của Sở.

Điều 2. Giải thích từ ngữ

1. An toàn, an ninh thông tin: Là sự bảo vệ thông tin và hệ thống thông tin tránh bị truy cập, 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 thông tin: Là tập hợp thiết bị 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 như: Hệ thống mạng nội bộ, hệ thống văn phòng điện tử, thư điện tử, trang thông tin điện tử...

3. Xâm phạm an toàn, an ninh thông tin: Là hành vi truy cập, sử dụng, tiết lộ, làm gián đoạn, sửa đổi, làm sai lệch chức năng, phá hoại trái phép thông tin và hệ thống thông tin.

4. Nguy cơ mất an toàn, an ninh thông tin: Là những nhân tố bên trong hoặc bên ngoài có khả năng ảnh hưởng đến trạng thái an toàn thông tin.

5. Đánh giá rủi ro an toàn, an ninh thông tin: Là việc xác định, phân tích nguy cơ mất an toàn thông tin có thể có và dự báo mức độ, phạm vi ảnh hưởng và khả năng gây thiệt hại khi xảy ra sự cố mất an toàn thông tin.

6. Quản lý rủi ro an toàn, an ninh thông tin: Là việc thực hiện đánh giá rủi ro an toàn thông tin, xác định yêu cầu bảo vệ thông tin và hệ thống thông tin và áp dụng giải pháp phòng, chống, giảm thiểu thiệt hại khi có sự cố mất an toàn thông tin.

7. Hệ thống mạng LAN: Là hệ thống mạng nội bộ dùng để kết nối các máy tính trong một phạm vi cơ quan, đơn vị. Các máy tính trong mạng LAN có thể chia sẻ tài nguyên với nhau như: tập tin, hình ảnh, máy in, máy quét và một số thiết bị khác.

8. Phần mềm độc hại: Là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hoặc 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.

Điều 3. Các hành vi bị nghiêm cấm

1. Ngăn chặn việc truyền tải thông tin trên mạng, can thiệp, truy nhập, gây nguy hại, xóa, thay đổi, sao chép và làm sai lệch thông tin trên mạng trái pháp luật.

2. Gây ảnh hưởng, cản trở trái pháp luật tới hoạt động bình thường của hệ thống thông tin hoặc tới khả năng truy nhập hệ thống thông tin của người sử dụng.

3. Tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng của biện pháp bảo vệ an toàn thông tin mạng của hệ thống thông tin; tấn công, chiếm quyền điều khiển, phá hoại hệ thống thông tin.

4. Phát tán thư rác, phần mềm độc hại, thiết lập hệ thống thông tin giả mạo, lừa đảo.

5. Thu thập, sử dụng, phát tán, kinh doanh trái pháp luật thông tin cá nhân của người khác; lợi dụng sơ hở, điểm yếu của hệ thống thông tin để thu thập, khai thác thông tin cá nhân.

6. Lợi dụng mạng để truyền bá thông tin, quan điểm, thực hiện các hình vi gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, lợi ích quốc gia trên mạng, phá hại khối đại đoàn kết toàn dân; tuyên truyền chiến tranh xâm lược, khủng bố, gây hận thù, mâu thuẫn giữa các dân tộc, sắc tộc, tôn giáo và bài ngoại;

7. Lợi dụng mạng để truyền bá trái phép tài liệu, hình ảnh, âm thanh hoặc dạng thông tin khác nhằm kích động bạo lực, dâm ô, đồi trụy, tội ác, tệ nạn xã hội, mê tín dị đoan, phá hoại thuần phong mỹ tục của dân tộc; bôi nhọ, gây thù hận, xâm hại tới quyền và lợi ích hợp pháp của tổ chức, cá nhân;

8. Các hành vi nghiêm cấm khác theo quy định của pháp luật.

Chương II
NỘI DUNG BẢO ĐẢM AN TOÀN, AN NINH THÔNG TIN

Điều 4. Các biện pháp quản lý kỹ thuật cơ bản trong công tác bảo đảm an toàn thông tin

1. Tổ chức mô hình mạng: Cài đặt, cấu hình, tổ chức hệ thống mạng theo mô hình Máy khách/Máy chủ (Client/Server), hạn chế sử dụng mô hình mạng ngang hàng. Khi thiết lập các dịch vụ trên môi trường mạng Internet, chỉ cung cấp những chức năng thiết yếu nhất bảo đảm duy trì hoạt động của hệ thống thông tin; hạn chế sử dụng chức năng, cổng giao tiếp mạng, giao thức và các dịch vụ không cần thiết.

2. Quản lý hệ thống mạng không dây (Wireless LAN): Khi thiết lập mạng không dây, cần thiết lập các thông số an toàn và định kỳ ít nhất 3 tháng thay đổi mật khẩu truy cập nhằm tăng cường công tác bảo mật.

3. Tổ chức quản lý tài khoản: Tiến hành rà soát ít nhất 6 tháng một lần các tài khoản và định danh người dùng trong hệ thống thông tin. Hủy tài khoản, quyền truy nhập hệ thống thông tin, thu hồi lại tất cả các tài sản liên quan tới hệ thống thông tin (khóa, thẻ nhận dạng, thư mục lưu trữ, …) đối với người sử dụng không còn công tác hoặc không còn sử dụng do được cấp tài khoản mới.

4. Quản lý đăng nhập hệ thống: Các hệ thống thông tin cần giới hạn số lần đăng nhập vào hệ thống, tự động khóa tài khoản khi liên tục đăng nhập sai vượt quá số lần quy định. Tổ chức theo dõi, giám sát tất cả các phương pháp đăng nhập từ xa, nhất là các trường hợp đăng nhập vào hệ thống với mục đích quản trị. Tăng cường việc sử dụng mạng riêng ảo (VPN - Virtual Private Network) khi có nhu cầu làm việc từ xa; yêu cầu người sử dụng đặt mật khẩu với độ an toàn cao.

5. Quản lý nhật ký sự kiện (Log File): Hệ thống thông tin cần ghi nhận các sự kiện: Quá trình đăng nhập hệ thống, các thao tác cấu hình hệ thống, quá trình truy xuất hệ thống... Thường xuyên kiểm tra, sao lưu (backup) các nhật ký sự kiện theo từng tháng để theo dõi, xác định những sự kiện đã xảy ra của hệ thống và hạn chế việc tràn nhật ký sự kiện gây ảnh hưởng đến hoạt động của hệ thống.

6. Chống mã độc, virus: Triển khai các phần mềm chống mã độc trên các máy tính, thiết bị di động trong mạng để phát hiện, loại trừ phần mềm độc hại. Thường xuyên cập nhật các phiên bản mới, các bản vá lỗi của các phần mềm chống virus để bảo đảm chương trình quét virus của cơ quan trên các máy chủ, máy trạm luôn được cập nhật mới nhất; thiết lập chế độ quét thường xuyên ít nhất tuần 01 lần. Thường xuyên cập nhật bản vá các lỗ hổng bảo mật của hệ điều hành và các phần mềm ứng dụng trên máy tính để hạn chế tối đa rủi ro mất an toàn thông tin.

7. Tổ chức quản lý tài nguyên: Kiểm tra giám sát chức năng chia sẻ thông tin (Network File and Folder Sharing). Tổ chức cấp phát tài nguyên trên máy chủ theo danh mục cho từng phòng, đơn vị trực thuộc; khuyến cáo người sử dụng cân nhắc việc chia sẻ tài nguyên trên máy đang sử dụng. Khi thực hiện chia sẻ tài nguyên trên máy chủ hoặc trên máy cục bộ cần sử dụng mật khẩu để bảo vệ thông tin.

8. Thiết lập cơ chế sao lưu và phục hồi cho máy chủ, máy trạm: Máy chủ và máy trạm cần được thực hiện các biện pháp sao lưu dữ liệu, thông tin quan trọng nhằm phục vụ cho công tác phục hồi dữ liệu một cách nhanh nhất.

9. Xử lý khẩn cấp: Khi phát hiện hệ thống thông tin bị tấn công cần thực hiện các bước cơ bản sau:

a) Bước 1: Ngắt kết nối máy chủ ra khỏi mạng;

b) Bước 2: Sao chép nhật ký sự kiện và toàn bộ dữ liệu của hệ thống ra thiết bị lưu trữ (phục vụ cho hoạt động phân tích, điều tra);

c) Bước 3: Khôi phục hệ thống bằng cách chuyển dữ liệu sao lưu mới nhất để hệ thống hoạt động trở lại;

d) Bước 4: Chủ trì, phối hợp với các cơ quan liên quan thành lập đoàn kiểm tra an toàn thông tin định kỳ hàng năm hoặc kiểm tra đột xuất khi phát hiện có các dấu hiệu vi phạm an toàn thông tin.

10. Hệ thống thông tin cần có cơ chế ngăn chặn hoặc hạn chế các sự cố gây ra do tấn công từ chối dịch vụ (DoS, DdoS).

Điều 5. Các biện pháp quản lý vận hành trong công tác bảo đảm an toàn, an ninh thông tin

1. Đối với các phòng và đơn vị trực thuộc:

a) Thường xuyên phổ biến, hướng dẫn, trang bị các kiến thức, kỹ năng về an toàn thông tin cho công chức, viên chức, người lao động để vận hành, khai thác, sử dụng hệ thống thông tin một cách an toàn;

b) Không sử dụng máy tính có kết nối Internet để đánh máy, in, lưu trữ tài liệu mật. Mọi thông tin thuộc bí mật nhà nước khi được lưu trữ và truyền đi trên môi trường mạng phải được mã hóa và quản lý theo quy định của pháp luật về cơ yếu, khuyến khích ứng dụng, sử dụng chữ ký số trong giao dịch điện tử;

c) Việc thanh lý, tiêu hủy thiết bị, phần mềm, vật mang thông tin của các cơ quan phải đảm bảo yêu cầu không để lộ, lọt thông tin nhà nước; phải có quy trình cụ thể và phải lưu giữ hồ sơ, biên bản thanh lý, tiêu hủy.

2. Đối với cán bộ chuyên trách Công nghệ thông tin (CNTT):

a) Tham mưu cho lãnh đạo đơn vị, cơ quan về công tác đảm bảo an toàn thông tin; vận hành an toàn các hệ thống thông tin của cơ quan, đơn vị; triển khai các biện pháp bảo đảm an toàn thông tin cho tất cả công chức, viên chức, người lao động trong cơ quan đơn vị mình;

b) Nắm vững và thực hiện nghiêm túc các quy định về bảo vệ bí mật Nhà nước. Thường xuyên tự cập nhật các kiến thức về an toàn thông tin, nguy cơ tiềm ẩn

có thể gây mất thông tin và các biện pháp phòng tránh khi tiến hành các hoạt động quản lý hay kỹ thuật nghiệp vụ;

c) Áp dụng biện pháp quản lý và kỹ thuật phù hợp với tiêu chuẩn, quy chuẩn kỹ thuật về an toàn thông tin để phòng, chống nguy cơ, khắc phục sự cố an toàn thông tin;

d) Thực hiện đánh giá, báo cáo các rủi ro gây mất an toàn thông tin và mức độ nghiêm trọng của các rủi ro đó. Các rủi ro gây mất an toàn thông tin có thể xảy ra do sự truy cập trái phép, sử dụng trái phép, mất, thay đổi, hoặc phá hủy thông tin và hệ thống thông tin;

e) Phối hợp chặt chẽ với Sở Thông Tin và Truyền thông, cơ quan Công an trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn, an ninh thông tin.

3. Đối với công chức, viên chức và người lao động:

a) Thường xuyên cập nhật những chính sách, quy trình, thủ tục an toàn thông tin của đơn vị cũng như thực hiện những hướng dẫn về an toàn thông tin của cơ quan hoặc cán bộ chuyên trách công nghệ thông tin.

b) Hạn chế việc sử dụng chức năng chia sẻ tài nguyên, khi sử dụng chức năng này cần bật thuộc tính bảo mật bằng mật khẩu và thực hiện việc thu hồi chức năng này khi đã sử dụng xong.

c) Các tài khoản đăng nhập cần phải đặt mật khẩu, thay đổi mật khẩu định kỳ. Cần đăng xuất tài khoản khỏi hệ thống khi không còn sử dụng. Hoặc ngắt kết nối mạng để tránh bị các tin tặc lợi dụng, chiếm quyền điều khiển máy tính từ xa.

d) Chỉ sử dụng Hệ thống Hộp thư điện tử (mail) công vụ, Hệ thống Văn phòng điện tử liên thông, cổng/trang thông tin điện tử, các hệ thống thông tin khác của cơ quan Nhà nước để gửi, nhận, đăng tải văn bản điện tử trong hoạt động của Sở.

e) Sử dụng chức năng mã hóa ở mức hệ điều hành để bảo đảm các dữ liệu nhạy cảm như tài khoản, mật khẩu, các tập tin quan trọng, v,v... được mã hóa. Các tập tin đính kèm thư điện tử, tải xuống từ Internet hoặc sao chép từ thiết bị lưu trữ cần được kiểm tra để tránh lây nhiễm các phần mềm độc hại.

Điều 6. Xây dựng và áp dụng quy trình đảm bảo an toàn thông tin

Các cơ quan, đơn vị phải xây dựng và áp dụng quy trình bảo đảm an toàn cho hệ thống thông tin nhằm giảm thiểu các nguy cơ gây ra sự cố, tạo điều kiện cho việc khắc phục và truy vết trong trường hợp có sự cố xảy ra.

Nội dung của quy trình bao gồm các bước cơ bản sau:

a) Lập kế hoạch bảo vệ an toàn cho hệ thống thông tin;

b) Xây dựng hệ thống bảo vệ an toàn thông tin;

c) Quản lý và vận hành hệ thống bảo vệ an toàn thông tin;

d) Kiểm tra đánh giá hoạt động của hệ thống bảo vệ an toàn thông tin;

e) Bảo trì và nâng cấp hệ thống bảo vệ an toàn thông tin.

Điều 7. Quy định quản lý và sử dụng thiết bị CNTT soạn thảo, lưu trữ văn bản mật.

1. Đảm bảo an toàn thông tin văn bản mật:

a) Máy tính soạn thảo văn bản mật: là máy tính không kết nối mạng LAN, WAN, internet và được kiểm định bảo mật an toàn thông tin (sau đây gọi tắt là máy tính mật).

b) Soạn thảo, lưu trữ văn bản mật:

- Cơ quan, đơn vị khi soạn thảo văn bản mật hoặc có tính mật phải sử dụng máy tính mật để soạn thảo.

- Thiết bị dùng để lưu trữ văn bản mật là ổ cứng (HDD) của máy tính mật hoặc thiết bị lưu trữ di động chỉ được kết nối với máy tính mật, không được kết nối với bất kỳ máy tính, thiết bị nào khác và được kiểm định bảo mật an toàn thông tin.

2. Quản lý thiết bị CNTT soạn thảo, lưu trữ văn bản mật:

a) Cơ quan, đơn vị có thực hiện việc soạn thảo văn bản mật theo quy định của pháp luật phải bố trí thiết bị CNTT để soạn thảo và lưu trữ văn bản mật.

b) Cơ quan, đơn vị khi mua sắm, trang thiết bị CNTT soạn thảo và lưu trữ văn bản mật (máy tính mật và thiết bị lưu trữ dữ liệu di động) phải được Sở Thông tin và Truyền thông có ý kiến đảm bảo bảo mật an toàn thông tin trước khi sử dụng.

c) Các thiết bị CNTT soạn thảo và lưu trữ văn bản mật phải được kiểm tra định kỳ hàng tháng/quý/06 tháng (bảo hành, bảo trì) an toàn bảo mật thông tin do cơ quan có chức năng thực hiện được quy định tại Quy chế này.

3. Tiêu hủy thiết bị CNTT soạn thảo, lưu trữ văn bản mật:

a) Xóa văn bản mật: thực hiện thao tác xóa (delete) văn bản mật trên máy tính kể cả trong thùng rác (Recycle Bin).

b) Tiêu hủy ổ cứng trên máy tính mật: Khi máy tính mật hết thời gian khấu hao, ổ cứng có dấu hiệu hư hỏng hoặc đã hư hỏng thì không được tận dụng hoặc sửa chữa để sử dụng vào mục đích khác mà tiến hành tiêu huỷ theo các bước thực hiện như sau:

Bước 1: Tiến hành sao chép dữ liệu ra thiết bị lưu trữ di động dữ liệu mật để bảo quản (trường hợp còn sử dụng được);

Bước 2: Tháo ổ cứng ra khỏi máy tính mật. Thực hiện niêm phong ổ cứng bằng cách dán giấy niêm phong bao quanh các cổng kết nối, lập biên bản niêm phong và giao cho lãnh đạo cơ quan bảo quản trong thời gian 06 tháng nhằm mục đích phục vụ công tác điều tra, thanh tra, khiếu nại, tố cáo (nếu có) liên quan đến dữ liệu lưu trữ trong ổ cứng;

Bước 3: Sau thời hạn 06 tháng kể từ ngày niêm phong nếu không có trường hợp điều tra, thanh tra, khiếu nại, tố cáo các vấn đề liên quan đến dữ liệu lưu trữ trong ổ cứng thì cơ quan, đơn vị quản lý tiến hành tiêu hủy ổ cứng ở mức độ vật lý có sự giám sát của lãnh đạo cơ quan và lập biên bản tiêu hủy;

c) Tiêu hủy thiết bị lưu trữ di động dữ liệu mật: Khi thiết bị lưu trữ hết thời gian khấu hao, có dấu hiệu hư hỏng hoặc đã hư hỏng thì không được tận dụng hoặc sửa chữa để sử dụng vào mục đích khác mà tiến hành tiêu hủy, các bước thực hiện như điểm b khoản 3 điều này.

Chương III
TRÁCH NHIỆM BẢO ĐẢM AN TOÀN, AN NINH THÔNG TIN

Điều 8. Trách nhiệm của lãnh đạo các Phòng, đơn vị trực thuộc

1. Quan tâm và ưu tiên bố trí kinh phí cho việc triển khai các biện pháp bảo đảm an toàn thông tin trong hoạt động ứng dụng CNTT của cơ quan, đơn vị.

2. Xây dựng quy chế, quy trình nội bộ về bảo đảm an toàn thông tin theo quy định tại Điều 6 và các quy định của pháp luật.

3. Khi có sự cố mất an toàn thông tin phải kịp thời chỉ đạo khắc phục ngay, ưu tiên sử dụng cán bộ kỹ thuật chuyên trách trong cơ quan, đơn vị và thông báo bằng văn bản cho Sở Thông tin và Truyền thông, cơ quan cấp trên quản lý trực tiếp để biết và phối hợp xử lý.

4. Phối hợp chặt chẽ với cơ quan Công an trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn thông tin. Tạo điều kiện thuận lợi cho các cơ quan chức năng tham gia khắc phục sự cố và thực hiện đúng theo hướng dẫn.

5. Báo cáo tình hình và kết quả thực hiện công tác đảm bảo an toàn thông tin tại cơ quan, đơn vị và gửi Sở Thông tin và Truyền thông khi có yêu cầu.

Điều 9. Trách nhiệm của Văn Phòng sở

1. Tham mưu giúp Giám đốc Sở trong công tác quản lý về công tác đảm bảo an toàn thông tin trong cơ quan Sở Tư pháp.

2. Chủ trì tham mưu lãnh đạo Sở tổ chức kiểm tra định kỳ hoặc đột xuất khi phát hiện có dấu hiệu hành vi vi phạm an toàn thông tin, xử lý nghiêm các hành vi vi phạm an toàn thông tin theo quy định của pháp luật.

3. Hướng dẫn các tiêu chí và quy trình kỹ thuật nhằm đảm bảo an toàn Thông tin, kiểm tra công tác đảm bảo an toàn thông tin, cử chuyên viên tham gia các chương trình đào tạo, bồi dưỡng và tuyên truyền về an toàn thông tin.

4. Hướng dẫn các phòng, đơn vị thực hiện các báo cáo về sự cố mất an toàn thông tin và kết quả thực hiện công tác đảm bảo an toàn thông tin.

5. Tùy theo mức độ sự cố, phối hợp các đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố mất an toàn thông tin.

6. Đưa nội dung đảm bảo an toàn thông tin vào Kế hoạch ứng dụng CNTT hàng năm của Sở, dự toán kinh phí để triển khai công tác đào tạo, hướng dẫn đảm bảo an toàn, an ninh thông tin cho các hệ thống thông tin của Sở.

Điều 10. Trách nhiệm của cán bộ công chức, viên chức

1. Nghiêm chỉnh chấp hành các quy định, quy trình về an toàn, an ninh thông tin của Sở Tư pháp cũng như quy định khác của pháp luật, nâng cao ý thức cảnh giác và trách nhiệm bảo đảm an toàn, an ninh thông tin tại cơ quan, đơn vị.

2. Khi phát hiện sự cố phải báo ngay với lãnh đạo Phòng, đơn vị và công chức chuyên trách CNTT để kịp thời ngăn chặn, xử lý.

3. Hưởng ứng, tham gia các chương trình đào tạo, hội nghị về an toàn, an ninh thông tin do Sở Thông tin và Truyền thông tổ chức (nếu có).

4. Có trách nhiệm bảo vệ, quản lý tài khoản được cấp tạm thời (nếu có) để đăng nhập vào hệ thống thông tin thực hiện giao dịch với các cơ quan qua các dịch vụ công trực tuyến, hệ thống mail công vụ, hệ thống Văn phòng điện tử liên thông, không giao, cung cấp tài khoản cho người khác sử dụng.

Chương IV
KHEN THƯỞNG, KỶ LUẬT

Điều 11. Các phòng, đơn vị sự nghiệp trực thuộc Sở; công chức, viên chức và người lao động thực hiện tốt Quy chế này. Nếu vi phạm tùy theo tính chất, mức độ sẽ xử lý, kỷ luật theo quy định.

Điều 12. Các phòng, đơn vị sự nghiệp trực thuộc Sở; công chức, viên chức và người lao động thực hiện tốt quy chế này được xét thi đua khen thưởng hàng năm. Người có công phát hiện, ngăn chặn kịp thời các hành vi vi phạm sẽ được khen thưởng theo Quy định của pháp luật.

Chương V
TỔ CHỨC THỰC HIỆN

Điều 13. Quy chế này được phổ biến đến tất cả công chức, viên chức, người lao động trong cơ quan, đơn vị thuộc Sở và có hiệu lực kể từ ngày ký ban hành.

Điều 14. Trong quá trình thực hiện nếu cần bổ sung chỉnh sửa, các cá nhân, đơn vị gửi kiến nghị về Văn phòng Sở để tổng hợp, trình Giám đốc Sở xem xét, quyết định.

Điều 15. Chánh Văn phòng Sở; Chánh Thanh tra Sở; Trưởng các phòng, đơn vị sự nghiệp trực thuộc Sở, trong phạm vi chức năng, nhiệm vụ được giao có trách nhiệm chỉ đạo, hướng dẫn, kiểm tra và đôn đốc thực hiện Quy chế này./.