

## QUY CHẾ

### **Đảm bảo an toàn, an ninh thông tin trong hoạt động của Sở Nội vụ tỉnh Hưng Yên**

(Ban hành kèm theo Quyết định số /QĐ-SNV ngày / /2022 của  
Giám đốc Sở Nội vụ tỉnh Hưng Yên)

## **Chương I QUY ĐỊNH CHUNG**

### **Điều 1. Phạm vi điều chỉnh**

Quy chế này quy định về công tác bảo đảm an toàn, an ninh thông tin trong hoạt động của Sở Nội vụ tỉnh Hưng Yên.

### **Điều 2. Đối tượng áp dụng**

Quy chế này áp dụng đối với các phòng, ban, trung tâm thuộc và trực thuộc Sở; công chức, viên chức, người lao động trong cơ quan và các cơ quan, đơn vị tham gia sử dụng, truy cập các hệ thống thông tin được Sở Nội vụ tỉnh Hưng Yên triển khai.

### **Điều 3. Mục đích, nguyên tắc đảm bảo an toàn, an ninh thông tin**

1. Tăng cường khả năng phòng chống nguy cơ tấn công, xâm nhập hệ thống thông tin và ngăn chặn, khắc phục kịp thời các sự cố gây mất an toàn, an ninh thông tin trên môi trường mạng.

2. Công tác đảm bảo an toàn, bí mật thông tin là yêu cầu bắt buộc trong quá trình thiết kế, vận hành, nâng cấp và hủy bỏ hạ tầng kỹ thuật, hệ thống thông tin trong cơ quan.

3. Thông tin số được quy định trong danh mục bí mật nhà nước, văn bản điện tử có nội dung mật, tối mật không được đăng tải lên môi trường mạng. Trường hợp đặc biệt, cần truyền thông tin mật trên môi trường mạng phải được Lãnh đạo Sở cho phép, trước khi truyền thông tin phải được mã hóa theo quy định của Luật Cơ yếu.

### **Điều 4. Giải thích từ ngữ**

1. *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. Việc bảo vệ thông tin, tài sản và con người trong hệ thống thông tin nhằm 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. An toàn thông tin bao hàm các nội dung bảo vệ và bảo mật thông tin, an toàn dữ liệu, an toàn máy tính và an toàn mạng.

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, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin số.

3. *An ninh thông tin*: Là việc bảo đảm thông tin, hệ thống thông tin được phục vụ liên tục, tránh bị gián đoạn, ngăn chặn các truy cập trái phép làm sửa đổi, phá hoại hoặc rò rỉ thông tin gây nguy hại đến an ninh quốc gia, bí mật nhà nước, quyền và lợi ích của tổ chức, cá nhân.

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

5. *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 tổng hệ thống thông tin.

#### **Điều 5. Các hành vi nghiêm cấm**

1. Ngăn chặn trái pháp luật việc truyền tải thông tin trên mạng; can thiệp, truy cập gây nguy hại, xóa, thay đổi, sửa chữa, sao chép, làm sai lệch thông tin trên môi trường mạng.

2. Tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng của biện pháp bảo vệ an toàn thông tin cho hệ thống thông tin; tạo, cài đặt, phát tán phần mềm độc hại, vi rút, chiếm quyền điều khiển hệ thống thông tin.

3. Quản bá, tuyên truyền, mua bán hàng hóa, dịch vụ bị cấm; truyền bá tác phẩm báo chí, văn học, nghệ thuật, xuất bản phẩm bị cấm.

4. Tiết lộ bí mật nhà nước, bí mật quân sự, an ninh, kinh tế, đối ngoại và những bí mật khác do pháp luật quy định.

5. Các hành vi khác do quy định của pháp luật.

### **Chương II**

#### **NỘI DUNG ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN**

**Điều 6. Các biện pháp quản lý, vận hành trong công tác đảm bảo an toàn, an ninh thông tin**

1. Đối với cơ quan

a. Trang bị đầy đủ kiến thức an toàn, bảo mật thông tin cho công chức, viên chức và người lao động.

b. Bố trí công chức chuyên trách về công nghệ thông tin (phụ trách quản trị mạng, an toàn, an ninh thông tin của cơ quan); tạo điều kiện để công chức chuyên trách được học tập, bồi dưỡng nâng cao kiến thức chuyên môn, nghiệp vụ.

c. Bố trí máy tính riêng không kết nối mạng nội bộ và mạng internet để quản lý, lưu trữ, soạn thảo văn bản, tài liệu mật khi cần thiết.

d. Kiểm tra thường xuyên việc thực hiện Điều 7 Quy chế này.

2. Đối với công chức chuyên trách về công nghệ thông tin

a. Triển khai, thực hiện các nội dung tại Điều 7 Quy chế này.

b. Tham mưu về chuyên môn và vận hành an toàn hệ thống thông tin của cơ quan, triển khai các biện pháp đảm bảo an toàn, an ninh thông tin cho công chức, viên chức trong cơ quan.

c. Nắm vững và thực hiện nghiêm túc các quy định của pháp luật về bảo vệ bí mật nhà nước, an toàn, an ninh thông tin; thường xuyên nghiên cứu, học tập trau dồi kiến thức, khắc phục mọi sự cố gây mất an toàn, an ninh thông tin;

d. Kiểm tra chặt chẽ cài đặt phần mềm trên máy chủ, máy trạm; theo dõi hoạt động của trang Thông tin điện tử đảm bảo thông tin chính xác, đúng quy định của pháp luật; phối hợp với các cá nhân, tổ chức, đơn vị liên quan trong việc kiểm soát và khắc phục sự cố an toàn, an ninh thông tin.

3. Đối với công chức, viên chức, người lao động trong cơ quan
  - a. Thường xuyên cập nhật chính sách, quy trình đảm bảo an toàn, an ninh thông tin của cơ quan, hướng dẫn của công chức chuyên trách.
  - b. Việc sử dụng, chia sẻ và lưu trữ dữ liệu, thông tin số trên mạng nội bộ, mạng internet phải tuân thủ các quy định của cơ quan và quy định của pháp luật về viễn thông, công nghệ thông tin.
  - c. Không cài đặt phần mềm không rõ nguồn gốc hoặc can thiệp tới các phần mềm ứng dụng khác trên hệ thống thông tin của cơ quan khi chưa được cấp có thẩm quyền cho phép.
  - d. Sử dụng các biện pháp mã hóa dữ liệu khi cần thiết đảm bảo không bị thay đổi nội dung khi truyền tải trên môi trường mạng; các tệp tin đính kèm thư điện tử, hoặc được tải xuống từ môi trường mạng internet hay các thiết bị lưu trữ ngoài (USB, ổ cứng...) khi thực hiện sao chép, kết nối với máy tính cần được kiểm tra, đề phòng vi rút, phần mềm độc hại.
  - e. Không sử dụng tên tài khoản hộp thư công vụ trên các trang mạng xã hội, diễn đàn và các trang thông tin tổng hợp khác trên mạng internet, thư điện tử công vụ được phép sử dụng trong các hoạt động công vụ, tuân thủ đúng quy định, quy chế của tỉnh và của cơ quan.
  - g. Sử dụng thiết bị lưu trữ ngoài và thiết bị điện tử khác an toàn, đúng quy định. Thực hiện tắt máy tính khi không sử dụng trong thời gian dài hoặc hết thời gian làm việc để tránh nguy cơ tấn công, xâm nhập trái phép.

### **Điều 7. Các biện pháp quản lý kỹ thuật trong công tác đảm bảo an toàn, an ninh thông tin**

1. Máy chủ, máy tính cá nhân, hệ thống lưu trữ, thiết bị mạng, thiết bị bảo mật, các ứng dụng của cơ quan phải đc bảo vệ bằng mật khẩu an toàn, có độ phức tạp cao, không sử dụng mật khẩu đơn giản, ngắn, mặc định.
2. Tất cả máy tính trong cơ quan phải được cài đặt và bảo vệ bởi phần mềm diệt vi rút, phần mềm độc hại.
3. Thiết lập cơ chế sao lưu và phục hồi máy chủ, máy trạm: Tiến hành sao lưu định kỳ dữ liệu hệ điều hành, phần mềm chuyên ngành, cơ sở dữ liệu quan trọng bằng các thiết bị sao lưu và phần mềm chuyên dụng nhằm phục vụ công tác phục hồi dữ liệu một cách nhanh nhất.
4. Tổ chức quản lý tài khoản, định danh người dùng trong các hệ thống thông tin bao gồm: Tạo mới, kích hoạt, sửa đổi và loại bỏ tài khoản. Đối với công chức, viên chức đã nghỉ việc, chuyển công tác phải có biện pháp khóa tài khoản, hủy quyền truy cập, thu hồi các thiết bị liên quan tới hệ thống thông tin (khóa, thẻ nhận dạng, công cụ ký số và thiết bị có liên quan) nhưng vẫn đảm bảo khả năng truy cập và hồ sơ được tạo ra bởi tài khoản đó.
5. Đối với tài khoản người dùng sử dụng để đăng nhập hệ thống thông tin, phần mềm ứng dụng, cơ sở dữ liệu và các ứng dụng chuyên ngành khác phải thiết lập mật khẩu có mức bảo mật cao nhằm đảm bảo an toàn thông tin của người dùng.
6. Các hệ thống thông tin cần giới hạn số lần đăng nhập sai liên tiếp vào hệ thống. Hệ thống tự động khóa tài khoản trong một thời gian nhất định trước khi tiếp tục cho đăng nhập nếu nhập sai mật khẩu quá số lần quy định.

7. 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). Sử dụng thiết bị tường lửa, xây dựng giải pháp phù hợp để có thể ngăn chặn, phòng tránh bị ảnh hưởng trực tiếp và bảo vệ thiết bị, máy chủ.

8. Quản lý nhật ký hệ thống (Logfile): Hệ thống thông tin cần ghi nhận các bản ghi nhật ký (quá trình đăng nhập hệ thống, các thao tác cấu hình hệ thống, truy xuất hệ thống). Thường xuyên kiểm tra, lưu giữ nội dung nhật ký trong khoảng thời gian nhất định để phục vụ quản lý, kiểm soát trên hệ thống.

9. Trường hợp có sự cố máy tính nghiêm trọng vượt khả năng khắc phục của đơn vị, phải báo cáo ngay cơ quan cấp trên quản lý trực tiếp, phối hợp với Sở Thông tin và Truyền thông để được hướng dẫn, hỗ trợ khắc phục.

#### **Điều 8. Đảm bảo an toàn, an ninh thông tin cho các hệ thống thông tin**

1. Văn phòng sở có trách nhiệm đảm bảo an toàn thông tin cho các hệ thống thông tin bao gồm:

a. Nghiên cứu, đề xuất xây dựng các hệ thống thông tin dùng chung của cơ quan để tăng hiệu quả sử dụng, tiết kiệm đầu tư, đảm bảo tính liên thông và thuận tiện trong việc đảm bảo an toàn thông tin;

b. Tổ chức thực hiện giám sát, đánh giá và đảm bảo an toàn thông tin cho các hệ thống thông tin dùng chung, cơ sở dữ liệu của ngành, hệ thống thư điện tử, quản lý văn bản và điều hành, một cửa điện tử, quản lý nhân sự và các hệ thống thông tin khác;

c. Chủ trì phối hợp với các phòng, ban, chi cục xây dựng phương án, tổ chức sao lưu và phục hồi dữ liệu khi xảy ra sự cố đối với các hệ thống thông tin của ngành; hướng dẫn sao lưu dự phòng các dữ liệu quan trọng khác;

d. Tham mưu Lãnh đạo Sở, hướng dẫn việc sử dụng các thiết bị viễn thông, điện tử, máy tính dùng để lưu giữ và truyền thông tin bí mật nhà nước.

2. Các phòng, ban, trung tâm trực thuộc Sở:

a. Nghiên cứu, đề xuất xây dựng phương án an toàn, an ninh thông tin các hệ thống thông tin do cơ quan, đơn vị triển khai thực hiện.

b. Cử công chức, viên chức thực hiện giám sát, đánh giá và triển khai thực hiện hiệu quả các hệ thống thông tin chuyên chuyên ngành.

### **Chương III**

## **TRÁCH NHIỆM ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN**

#### **Điều 9. Trách nhiệm của cơ quan**

1. Thủ trưởng cơ quan có trách nhiệm tổ chức triển khai thực hiện các quy định tại Quy chế này và chịu trách nhiệm trước UBND tỉnh trong công tác đảm bảo an toàn, an ninh thông tin của cơ quan.

2. Ưu tiên nguồn kinh phí thường xuyên cho việc triển khai các biện pháp đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của cơ quan.

3. Khi xảy ra sự cố hoặc nguy cơ mất an toàn thông tin phải kịp thời áp dụng mọi biện pháp để khắc phục và hạn chế mức thấp nhất thiệt hại có thể xảy

ra, ưu tiên sử dụng cán bộ chuyên trách của cơ quan; thông báo bằng văn bản cho cơ quan cấp trên quản lý trực tiếp và Sở Thông tin và Truyền thông.

4. Phối hợp với Sở Thông tin và Truyền thông và các đơn vị liên quan thực hiện công tác kiểm tra, khắc phục sự cố nhanh chóng, kịp thời, giảm mức thấp nhất thiệt hại.

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

6. Định kỳ hàng năm báo cáo kết quả thực hiện công tác đảm bảo an toàn, an ninh thông tin gửi Sở Thông tin và Truyền thông trước ngày 15/11 hàng năm để tổng hợp báo cáo UBND tỉnh.

#### **Điều 10. Trách nhiệm của Văn phòng**

1. Tham mưu Lãnh đạo Sở về công tác đảm bảo an toàn, an ninh thông tin trong hoạt động của cơ quan và chịu trách nhiệm trước Lãnh đạo Sở trong việc đảm bảo an toàn cho các hệ thống thông tin của cơ quan.

2. Hàng năm xây dựng kế hoạch, dự toán nguồn kinh phí để triển khai công tác đảm bảo an toàn, an ninh thông tin phục vụ cho hoạt động ứng dụng công nghệ thông tin tại cơ quan; vận hành, khai thác các hệ thống trong phạm vi quản lý.

3. Chủ trì, phối hợp với các đơn vị liên quan tổ chức kiểm tra theo định kỳ hoặc kiểm tra đột xuất công tác đảm bảo an, an ninh thông tin trong cơ quan.

4. Là đầu mối về ứng cứu sự cố máy tính, tham gia vào mạng lưới điều phối, ứng cứu sự cố, tiếp nhận và xử lý các thông báo sự cố về an toàn thông tin. Tùy theo mức độ sự cố, phối hợp với các cơ quan liên quan khắc phục kịp thời, hiệu quả.

5. Tổng hợp báo cáo tình hình đảm bảo an toàn, an ninh thông tin gửi Sở Thông tin và Truyền thông theo định kỳ.

#### **Điều 11. Trách nhiệm của công chức, viên chức và người lao động trong cơ quan**

1. Nghiêm chỉnh chấp hành các quy định tại Quy chế nội bộ đảm bảo an toàn, an ninh thông tin của cơ quan, các quy định tại Quy chế này và quy định khác của pháp luật về an toàn, an ninh thông tin. Chịu trách nhiệm đảm bảo an toàn, an ninh thông tin trong phạm vi trách nhiệm, quyền hạn được giao.

2. Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin phải báo cáo ngay với cấp trên và cán bộ chuyên trách của cơ quan để kịp thời ngăn chặn, xử lý.

3. Tham gia đầy đủ các chương trình, khóa đào tạo, bồi dưỡng, tập huấn, hội nghị về an toàn thông tin do Sở Thông tin và Truyền thông hoặc cơ quan chuyên môn tổ chức.

### **Chương IV TỔ CHỨC THỰC HIỆN**

#### **Điều 12. Khen thưởng và xử lý vi phạm**

1. Hàng năm, lập báo cáo gửi Sở Thông tin và Truyền thông về công tác an toàn, an ninh thông tin của cơ quan; trên cơ sở đó đề xuất UBND tỉnh xem xét, khen thưởng theo quy định hiện hành.

2. Tập thể, cá nhân có hành vi vi phạm Quy chế này tùy theo tính chất, mức độ vi phạm sẽ bị xử lý theo quy định của pháp luật.

**Điều 13. Điều khoản thi hành**

Văn phòng Sở có trách nhiệm chủ trì, phối hợp với các cơ quan, tổ chức liên quan hướng dẫn, triển khai và kiểm tra, đôn đốc việc thực hiện Quy chế này.

Trưởng các phòng, ban, chi cục thuộc và trực thuộc Sở triển khai Quy chế đến công chức, viên chức và người lao động trong đơn vị mình; phối hợp, thông tin đến Văn phòng Sở cùng khắc phục khi xảy ra sự cố mất an toàn, an ninh thông tin.

Trong quá trình thực hiện Quy chế nếu có khó khăn, vướng mắc đề nghị gửi văn bản về Văn phòng Sở tổng hợp, báo cáo Lãnh đạo Sở xem xét, hướng dẫn, sửa đổi, bổ sung cho phù hợp./.

**SỞ NỘI VỤ**