

## **QUY CHẾ**

**Bảo đảm an toàn, an ninh thông tin mạng của Sở Xây dựng**  
(Kèm theo Quyết định số      /QĐ-SXD ngày      tháng 5 năm 2021  
của Sở Xây dựng)

### **Chương I** **QUY ĐỊNH CHUNG**

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

1. Quy chế này quy định về bảo đảm an toàn, an ninh thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của Sở Xây dựng.
2. Quy chế này áp dụng đối với các Phòng, đơn vị thuộc Sở và công chức, viên chức, người lao động Sở Xây dựng.

#### **Điều 2. Giải thích từ ngữ**

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

1. *An toàn thông tin* là sự bảo vệ thông tin và hệ thống thông tin 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. *An ninh thông tin* là sự bảo đảm thông tin, hệ thống thông tin được phục vụ liên tục, tránh bị gián đoạn, ngăn chặn các truy nhập trái phép làm sửa đổi, phá hoại hoặc rò rỉ thông tin.
3. *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.
4. *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.
5. *Hạ tầng kỹ thuật* là tập hợp các thiết bị tính toán, lưu trữ, thiết bị ngoại vi, thiết bị kết nối mạng, thiết bị phụ trợ, đường truyền, mạng nội bộ, mạng diện rộng.
6. *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.
7. *Dữ liệu nhạy cảm* là dữ liệu có thông tin mật, thông tin lưu hành nội bộ của đơn vị hoặc do đơn vị quản lý, nếu lộ lọt ra ngoài sẽ gây ảnh hưởng xấu đến danh tiếng, hoạt động của đơn vị.

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

1. Bảo đảm an toàn, an ninh thông tin là yêu cầu bắt buộc, thường xuyên, liên tục, có tính xuyên suốt quá trình liên quan đến thông tin và thiết kế, xây dựng, vận hành, nâng cấp, hủy bỏ hệ thống thông tin. Bảo đảm an toàn, an ninh thông tin tuân thủ các nguyên tắc chung quy định tại Điều 4 Luật An toàn thông tin mạng và Điều 4 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.

2. Các phòng, đơn vị thuộc Sở có trách nhiệm bảo đảm an toàn, an ninh thông tin mạng của đơn vị mình; bố trí nhân sự chịu trách nhiệm bảo đảm an toàn, an ninh thông tin mạng; xác định rõ quyền hạn, trách nhiệm của Thủ trưởng đơn vị, từng bộ phận, cá nhân trong đơn vị đối với công tác bảo đảm an toàn, an ninh thông tin mạng.

3. Công chức, viên chức và người lao động trong các phòng, đơn vị thuộc Sở có trách nhiệm bảo đảm an toàn, an ninh thông tin trong phạm vi xử lý công việc của mình theo quy định của Nhà nước và của Sở Xây dựng.

4. Thông tin mật, thông tin thuộc Danh mục bí mật nhà nước ngành Xây dựng phải được bảo vệ theo quy định của Nhà nước, quy định của Sở Xây dựng về công tác bảo vệ bí mật nhà nước và các nội dung tương ứng trong Quy chế này.

5. Xử lý sự cố an toàn thông tin phải phù hợp với trách nhiệm, quyền hạn và bảo đảm lợi ích hợp pháp của cơ quan, đơn vị, cá nhân liên quan và theo quy định của pháp luật.

**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.

2. Tự ý đầu 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 mạng nội bộ; tự ý thay đổi, gỡ bỏ biện pháp an toàn thông tin cài đặt trên thiết bị công nghệ thông tin phục vụ công việc; tự ý thay thế, lắp mới, tráo đổi thành phần của máy tính phục vụ công việc.

3. Tạo ra, cài đặt, phát tán phần mềm độc hại.

4. Cản trở hoạt động cung cấp dịch vụ của hệ thống thông tin; ngăn chặn việc truy nhập đến thông tin của cơ quan, cá nhân khác trên môi trường mạng, trừ trường hợp pháp luật cho phép.

5. Bẻ khóa, trộm cắp, sử dụng 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, bí mật thông tin của cơ quan, cá nhân khác được trao đổi, truyền đưa, lưu trữ trên môi trường mạng.

## **Chương II**

### **QUY ĐỊNH BẢO ĐẢM AN TOÀN, AN NINH THÔNG TIN MẠNG**

#### **Điều 5. Quản lý trang thiết bị công nghệ thông tin**

1. Giao, gán trách nhiệm cho cá nhân hoặc tập thể quản lý, sử dụng trang thiết bị công nghệ thông tin.
2. Quy định các quy tắc sử dụng, giữ gìn bảo vệ trang thiết bị công nghệ thông tin trong các trường hợp như: mang ra khỏi cơ quan, trang thiết bị công nghệ thông tin liên quan đến dữ liệu nhạy cảm, cài đặt và cấu hình.
3. Trang thiết bị công nghệ thông tin có lưu trữ dữ liệu nhạy cảm khi thay đổi mục đích sử dụng hoặc thanh lý, đơn vị phải thực hiện các biện pháp xóa, tiêu hủy dữ liệu đó đảm bảo không có khả năng phục hồi. Trường hợp không thể tiêu hủy được dữ liệu, đơn vị phải thực hiện tiêu hủy cấu phần lưu trữ dữ liệu trên trang thiết bị công nghệ thông tin đó.
4. Thiết bị tính toán có bộ phận lưu trữ hoặc thiết bị lưu trữ khi mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài hoặc ngừng sử dụng phải tháo bộ phận lưu trữ khỏi thiết bị hoặc xóa thông tin, dữ liệu lưu trữ trên thiết bị (trừ trường hợp để khôi phục dữ liệu).
5. Các đơn vị thuộc Sở có trách nhiệm xây dựng quy trình bảo dưỡng, bảo trì và hướng dẫn cách sử dụng, quản lý, vận hành hệ thống hạ tầng kỹ thuật của đơn vị; thực hiện quản lý, vận hành và định kỳ kiểm tra, sửa chữa, bảo trì thiết bị (bao gồm thiết bị đang hoạt động và thiết bị dự phòng).

#### **Điều 6. Quản lý công chức, viên chức và người lao động**

1. Các đơn vị thuộc Sở phải thường xuyên tổ chức quán triệt các quy định về an toàn, an ninh thông tin, nhằm nâng cao nhận thức về trách nhiệm bảo đảm an toàn thông tin của từng cá nhân trong đơn vị.
2. Khi công chức, viên chức và người lao động chấm dứt hoặc thay đổi công việc cơ quan, đơn vị phải:
  - a) Xác định rõ trách nhiệm của cá nhân và các bên liên quan trong quản lý, sử dụng các tài sản công nghệ thông tin được giao.
  - b) Lập biên bản bàn giao tài sản công nghệ thông tin.
  - c) Thay đổi hoặc thu hồi quyền truy cập các hệ thống thông tin.

#### **Điều 7. Bảo đảm an toàn hệ thống công nghệ thông tin**

1. Bảo đảm an toàn thông tin đối với phòng máy chủ (nếu có)
  - a) Các thiết bị kết nối mạng, thiết bị bảo mật quan trọng như tường lửa (firewall), thiết bị định tuyến (router), máy chủ, hệ thống lưu trữ... phải được đặt trong phòng máy chủ và phải được thiết lập cơ chế bảo vệ, theo dõi phát hiện xâm nhập và biện pháp kiểm soát truy nhập, kết nối vật lý phù hợp với từng khu

vực: máy chủ và hệ thống lưu trữ; tủ mạng và đầu nối; thiết bị nguồn điện và dự phòng điện khẩn cấp; vận hành, kiểm soát, quản trị hệ thống.

b) Phòng máy chủ là khu vực hạn chế tiếp cận và được lắp đặt hệ thống camera giám sát. Chỉ những cá nhân có quyền, nhiệm vụ theo quy định mới được phép vào phòng máy chủ. Quá trình vào, ra phòng máy chủ phải được ghi nhận vào nhật ký quản lý phòng máy chủ.

c) Phòng máy chủ phải được trang bị hệ thống lưu điện đủ công suất và duy trì thời gian hoạt động của các máy chủ ít nhất 15 phút khi có sự cố mất điện.

d) Phòng máy chủ phải có hệ thống giám sát, cảnh báo cháy, hệ thống chữa cháy, thiết bị phòng cháy, chữa cháy khẩn cấp; hệ thống cảnh báo hệ thống nguồn điện; hệ thống chống sét lan truyền.

## 2. Bảo đảm an toàn thông tin khi sử dụng máy tính

a) Cá nhân chỉ cài đặt phần mềm hợp lệ và thuộc danh mục phần mềm được phép sử dụng do cơ quan có thẩm quyền ban hành trên máy tính được đơn vị cấp cho mình; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm khi chưa có sự đồng ý của lãnh đạo Sở; thường xuyên cập nhật phần mềm và hệ điều hành.

b) Cài đặt phần mềm xử lý phần mềm độc hại và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm; khi phát hiện bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại trên máy tính phải tắt máy và báo trực tiếp cho công chức chuyên trách về công nghệ thông tin để được xử lý kịp thời.

c) Chỉ truy nhập vào các trang thông tin điện tử, ứng dụng trực tuyến tin cậy và các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình; có trách nhiệm bảo mật tài khoản truy nhập thông tin, không chia sẻ mật khẩu, thông tin cá nhân với người khác.

## 3. Quản lý tài khoản truy cập

a) Cá nhân sử dụng hệ thống thông tin được cấp và sử dụng tài khoản truy nhập với định danh duy nhất gắn với cá nhân đó.

b) Trường hợp cá nhân thay đổi vị trí công tác, chuyển công tác, thôi việc hoặc nghỉ hưu, trong vòng không quá 05 ngày làm việc, đơn vị quản lý cá nhân đó phải thông báo cho đơn vị chủ quản hệ thống thông tin để điều chỉnh, thu hồi, hủy bỏ các quyền sử dụng đối với hệ thống thông tin.

c) Khi có yêu cầu khóa quyền truy cập hệ thống thông tin của tài khoản đang hoạt động, lãnh đạo phòng, đơn vị phải yêu cầu bằng văn bản gửi đơn vị chủ quản hệ thống thông tin. Đơn vị vận hành hệ thống thông tin thực hiện việc khóa quyền truy cập của tài khoản khi có chỉ đạo của Lãnh đạo Sở. Đơn vị chủ quản hệ thống thông tin có quyền khóa quyền truy cập của tài khoản trong trường hợp tài khoản đó thực hiện các hành vi tấn công hoặc để xảy ra vấn đề mất an toàn, an ninh thông tin.

d) Việc quản lý tài khoản thư điện tử của Sở Xây dựng được thực hiện theo quy định Quyết định số 08/2014/QĐ-UBND ngày 09/5/2014 của UBND tỉnh về việc ban hành Quy chế quản lý, khai thác, sử dụng và vận hành hệ thống thư điện tử tỉnh Đắk Lắk.

#### 4. Bảo đảm an toàn thông tin mức dữ liệu

a) Đơn vị phải thực hiện bảo vệ thông tin, dữ liệu liên quan đến hoạt động công vụ, thông tin có nội dung quan trọng, nhạy cảm hoặc không phải là thông tin công khai bằng các biện pháp như: thiết lập phương án bảo đảm tính bí mật, nguyên vẹn và khả dụng của thông tin, dữ liệu; mã hóa thông tin, dữ liệu khi lưu trữ trên hệ thống/thiết bị lưu trữ dữ liệu di động; sử dụng chữ ký số để xác thực và bảo mật thông tin, dữ liệu.

b) Đơn vị cần triển khai hệ thống/phương tiện lưu trữ độc lập với hệ thống lưu trữ trên các máy chủ dịch vụ để sao lưu dự phòng; phân loại và quản lý thông tin, dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau; thực hiện sao lưu dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

c) Bố trí máy tính riêng không kết nối mạng, đặt mặt khẩu, mã hóa dữ liệu và các biện pháp bảo mật khác bảo đảm an toàn thông tin để soạn thảo, lưu trữ dữ liệu, thông tin và tài liệu quan trọng ở các mức độ mật, tuyệt mật, tối mật.

d) Các đơn vị thuộc Sở phải thường xuyên kiểm tra, giám sát các hoạt động chia sẻ, gửi, nhận thông tin, dữ liệu trong hoạt động nội bộ của mình; khuyến cáo việc chia sẻ, gửi, nhận thông tin trên môi trường mạng cần phải sử dụng mặt khẩu để bảo vệ thông tin.

đ) Đối với hoạt động trao đổi thông tin, dữ liệu với bên ngoài, đơn vị và cá nhân thực hiện trao đổi thông tin, dữ liệu ra bên ngoài cam kết và có biện pháp bảo mật thông tin, dữ liệu được trao đổi. Giao dịch trực tuyến phải được truyền đầy đủ, đúng địa chỉ, tránh bị sửa đổi, tiết lộ hoặc nhân bản một cách trái phép; sử dụng các cơ chế xác thực mạnh, chữ ký số khi tham gia giao dịch, sử dụng các giao thức truyền thông an toàn.

### **Điều 8. Xác định cấp độ và phương án bảo đảm an toàn hệ thống thông tin**

1. Việc xác định cấp độ hệ thống thông tin và xây dựng phương án bảo vệ hệ thống thông tin theo cấp độ phục vụ mục đích đánh giá an toàn thông tin và bảo đảm an toàn thông tin cho các hệ thống thông tin.

2. Nguyên tắc bảo đảm an toàn thông tin theo cấp độ và nguyên tắc xác định cấp độ căn cứ trên các nguyên tắc quy định tại Điều 4, Điều 5 Nghị định số 85/2016/NĐ-CP.

### **Điều 9. Quy trình ứng cứu sự cố an toàn thông tin mạng**

1. Đơn vị, cá nhân khi phát hiện dấu hiệu tấn công hoặc sự cố an toàn thông tin mạng cần nhanh chóng báo cho đơn vị vận hành hệ thống thông tin, Văn phòng Sở để tổng hợp, báo cáo Lãnh đạo Sở.

2. Khi xảy ra sự cố an toàn thông tin mạng thuộc loại hình tấn công mạng, đơn vị vận hành hệ thống thông tin thực hiện báo cáo theo quy định tại Điểm a Khoản 1 Điều 11 Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 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 Điều 9 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. Trách nhiệm của các đơn vị khi phát hiện, tiếp nhận xác minh, xử lý ban đầu và phân loại sự cố an toàn thông tin mạng theo quy định tại Điều 12 Quyết định số 05/2017/QĐ-TTg và Điều 10 Thông tư số 20/2017/TT-BTTTT.

3. Quy trình ứng cứu sự cố an toàn thông tin mạng theo quy định tại Điều 13, Điều 14 Quyết định số 05/2017/QĐ-TTg và Điều 11 Thông tư số 20/2017/TT-BTTTT.

## **Chương III TỔ CHỨC THỰC HIỆN**

### **Điều 10. Kinh phí thực hiện**

Kinh phí bảo đảm an toàn, an ninh thông tin mạng được lấy từ nguồn ngân sách nhà nước dự toán hàng năm của Sở Xây dựng.

### **Điều 11. Khen thưởng, kỷ luật**

Công chức, viên chức, người lao động có thành tích trong công tác bảo đảm an toàn, an ninh thông tin mạng thì được xét khen thưởng theo quy định của pháp luật; trường hợp vi phạm các quy định của pháp luật về bảo đảm an toàn, an ninh thông tin mạng và quy định tại Quy chế này thì tùy theo mức độ vi phạm sẽ bị xử lý kỷ luật, xử phạt vi phạm hành chính hoặc bị truy cứu trách nhiệm hình sự theo quy định của pháp luật.

### **Điều 12. Trách nhiệm thi hành**

1. Giao Chánh Văn phòng giúp Giám đốc Sở theo dõi việc triển khai và thực hiện Quy chế này.

2. Trưởng các Phòng, đơn vị thuộc sở có trách nhiệm tổ chức phổ biến, quán triệt nội dung Quy chế này đến toàn thể công chức, viên chức và người lao động trong đơn vị biết để thực hiện nghiêm túc.

3. Công chức, viên chức, người lao động của Sở Xây dựng có trách nhiệm: tuân thủ Quy chế; thông báo các vấn đề bất thường liên quan tới an toàn thông tin mạng của đơn vị cho Văn phòng Sở; chịu trách nhiệm trước pháp luật và

Lãnh đạo Sở về các vi phạm, thất thoát dữ liệu mật của ngành Xây dựng do không tuân thủ Quy chế.

4. Trong quá trình thực hiện nếu có khó khăn, vướng mắc phát sinh cần phản ánh về Văn phòng Sở để tổng hợp, báo cáo Lãnh đạo Sở xem xét, sửa đổi, bổ sung cho phù hợp./.