UBND TỈNH BẮC NINH **SỞ XÂY DỰNG**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số:558 /QĐ-SXD	*Bắc Ninh, ngày 21 tháng 7 năm 2026*

QUYẾT ĐỊNH
Ban hành Quy chế đảm bảo an ninh mạng, an toàn thông tin tại Sở Xây dựng Bắc Ninh

GIÁM ĐỐC SỞ XÂY DỰNG TỈNH BẮC NINH

Căn cứ Luật An toàn thông tin mạng số 86/2015/QH13 ngày 19/11/2025;

Căn cứ Luật An ninh mạng số 24/2018/QH14 ngày 12/6/2018;

Căn cứ Luật Bảo vệ bí mật nhà nước số 117/2025/QH15 ngày 10/12/2025;

Căn cứ 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;

Căn cứ Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 của Chính phủ Quy định chi tiết một số điều của Luật An ninh mạng;

Căn cứ Nghị định số 13/2023/NĐ-CP ngày 01/7/2023 của Chính phủ Bảo vệ dữ liệu cá nhân;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ trưởng Bộ Thông tin và Truyền thông Quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Quyết định số 40/2025/QĐ-UBND ngày 09/10/2025 của UBND tỉnh Ban hành Quy chế bảo đảm an ninh mạng, an toàn thông tin trên địa bàn tỉnh Bắc Ninh;

Căn cứ Quyết định số 12/2025/QĐ-UBND ngày 01/7/2025 của UBND tỉnh Bắc Ninh về việc ban hành Quy định chức năng, nhiệm vụ, quyền hạn của Sở Xây dựng tỉnh Bắc Ninh; Quyết định 01/QĐ-UBND ngày 01/7/2025 của UBND tỉnh Bắc Ninh về việc ban hành cơ cấu tổ chức bộ máy của Sở Xây dựng;

Căn cứ Quyết định 86/QĐ-SXD ngày 04/7/2025 của Sở Xây dựng tỉnh Bắc Ninh về việc ban hành Quy chế làm việc của Sở Xây dựng tỉnh Bắc Ninh;

Theo đề nghị của Chánh Văn phòng Sở.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế đảm bảo an ninh mạng, an toàn thông tin tại Sở Xây dựng Bắc Ninh.

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

Điều 3. Chánh Văn phòng Sở, Trưởng các phòng chuyên, đơn vị thuộc Sở, công chức, viên chức, lao động hợp đồng thuộc Sở Xây dựng chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Lãnh đạo Sở;
- Các phòng, đơn vị thuộc Sở;
- Cổng thông tin điện tử Sở;
- Lưu: VT, VP.

GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ XÂY DỰNG
TỈNH BẮC NINH

Nguyễn Việt Hùng

UBND TỈNH BẮC NINH
SỞ XÂY DỰNG

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

QUY CHẾ
Bảo đảm an ninh mạng, an toàn thông tin tại Sở Xây dựng Bắc Ninh
(Ban hành kèm theo Quyết định số 558 /QĐ-SXD ngày 21/7/2026 của Sở Xây dựng tỉnh Bắc Ninh)

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 ninh mạng, an toàn thông tin mạng trong các hoạt động ứng dụng công nghệ thông tin (CNTT), chuyển đổi số của Sở Xây dựng tỉnh Bắc Ninh.

2. Quy chế này được áp dụng đối với Văn phòng Sở, các phòng, đơn vị thuộc Sở (sau đây gọi tắt là các phòng làm việc); công chức, viên chức và lao động hợp đồng (gọi tắt là cán bộ) thuộc Sở liên quan đến hoạt động ứng dụng công nghệ thông tin (sau đây gọi tắt là CNTT), chuyển đổi số của Sở.

Điều 2. Giải thích từ ngữ

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

1. An ninh an toàn mạng là viết tắt của an ninh mạng và an toàn thông tin mạng.

2. Hệ thống thông tin: Là tập hợp 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 trên mạng.

3. Mật khẩu mạnh là mật khẩu đáp ứng các yêu cầu: Có tối thiểu từ 8 đến 12 ký tự, gồm tối thiểu 3 trong 4 loại ký tự sau: chữ cái viết hoa (A - Z), chữ cái viết thường (a - z), chữ số (0 - 9), các ký tự khác (` ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; " ' < > , . ? /).

4. Dữ liệu cá nhân là thông tin dưới dạng ký hiệu, chữ viết, số, hình ảnh, âm thanh hoặc dạng tương tự trong môi trường điện tử gắn với một cá nhân hoặc giúp nhận biết một cá nhân. Việc thu thập, xử lý, chia sẻ dữ liệu cá nhân phải tuân thủ quy định về bảo vệ dữ liệu cá nhân.

Điều 3. Nguyên tắc bảo đảm an toàn thông tin

1. Cán bộ có trách nhiệm bảo đảm an ninh an toàn mạng. Hoạt động bảo đảm an ninh an toàn mạng phải tuân quy định của pháp luật về an ninh mạng, an

toàn thông tin, bảo vệ bí mật nhà nước, bí mật công tác, dữ liệu cá nhân và các quy định khác có liên quan.

2. Bảo đảm an ninh an toàn mạng 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.

Điều 4. Những hành vi nghiêm cấm

1. Các hành vi bị nghiêm cấm về an ninh mạng quy định tại Điều 8 Luật An ninh mạng và Điều 7 Luật An toàn thông tin mạng

2. Các hành vi nghiêm cấm khác về an ninh an toàn mạng, bí mật nhà nước, bảo vệ dữ liệu cá nhân theo quy định của pháp luật

Chương II
QUY ĐỊNH ĐẢM BẢO AN NINH AN TOÀN MẠNG

Điều 5. Trách nhiệm bảo đảm an ninh an toàn mạng

1. Sở Xây dựng là chủ quản các hệ thống thông tin thuộc phạm vi quản lý của Sở theo quy định của pháp luật. Chủ quản hệ thống thông tin thực hiện trách nhiệm theo quy định tại Điều 20 Nghị định số 85/2016/NĐ-CP và các quy định pháp luật có liên quan.

2. Văn phòng Sở là đầu mối tham mưu Giám đốc Sở tổ chức thực hiện công tác bảo đảm an ninh, an toàn mạng; phối hợp với các cơ quan, đơn vị có liên quan trong việc phòng ngừa, phát hiện, xử lý và ứng cứu sự cố an toàn thông tin theo quy định.

3. Đơn vị vận hành hệ thống thông tin là các phòng làm việc thuộc Sở được giao quản lý, vận hành hệ thống thông tin. Đơn vị vận hành thực hiện trách nhiệm theo Điều 22 Nghị định số 85/2016/NĐ-CP và các quy định pháp luật có liên quan; bảo đảm hệ thống hoạt động an toàn, liên tục; phối hợp xử lý, ứng cứu sự cố và thực hiện các yêu cầu về bảo đảm an ninh, an toàn mạng theo quy định.

Điều 6. Bảo đảm, quản lý nguồn nhân lực

1. Công chức, viên chức được giao phụ trách về an ninh, an toàn mạng có trình độ, chuyên ngành phù hợp lĩnh vực công nghệ thông tin, an toàn thông tin.

2. Trong quá trình làm việc

a) Với người sử dụng

- Có trách nhiệm tuân thủ các quy định, hướng dẫn bảo đảm an ninh an toàn mạng, bảo vệ dữ liệu cá nhân và các quy định khác của pháp luật đối với từng vị trí công việc.

- Thông báo ngay cho đơn vị chủ quản hệ thống khi nghi ngờ hoặc phát hiện sự cố, hiện tượng bất thường của hệ thống thông tin.

- Tham gia đầy đủ các lớp tập huấn, đào tạo khi có yêu cầu và tự động cập nhật kiến thức về an toàn an ninh mạng.

- Đổi mật khẩu ngay sau khi được cấp tài khoản đăng nhập các dịch vụ, ứng dụng dùng chung tại Sở Xây dựng. Giữ bí mật tài khoản cá nhân khi tham gia khai thác, sử dụng, không ghi mật khẩu ra những nơi người khác có thể biết; không lưu trữ, truyền, gửi mật khẩu khi chưa được mã hóa an toàn và chia sẻ mật khẩu của cá nhân cho người khác; định kỳ 03 tháng phải thay đổi mật khẩu hoặc ngay sau khi nghi ngờ tài khoản có dấu hiệu bị lộ, lọt.

- Chịu trách nhiệm quản lý, sử dụng thiết bị CNTT được giao bảo đảm an ninh an toàn mạng; không tự ý thay thế, lắp mới, thay đổi thành phần của máy tính công vụ khi chưa được sự cho phép của bộ phận quản lý; có trách nhiệm bàn giao các trang thiết bị CNTT khi chuyển công tác, thay đổi vị trí việc làm hoặc nghỉ việc.

- Thực hiện nghiêm túc việc soạn thảo văn bản chứa bí mật nhà nước, lưu trữ tài liệu mật tại máy tính được trang bị cho việc soạn thảo, lưu trữ văn bản mật theo quy định.

- Không tự ý thay đổi, gỡ bỏ biện pháp an toàn thông tin cài đặt trên máy tính phục vụ công việc.

b) Với cán bộ quản lý, vận hành hệ thống

- Tuyệt đối tuân thủ nghiêm các quy định đã được ban hành và chịu trách nhiệm khi xảy ra sự cố nghiêm trọng.

- Việc khai thác thông tin, dữ liệu phải bảo đảm nguyên tắc bảo mật, an toàn thông tin, không tự ý cung cấp thông tin, dữ liệu ra bên ngoài khi chưa được sự đồng ý của đơn vị chủ quản.

- Thường xuyên phổ biến, tuyên truyền nâng cao nhận thức về an ninh an toàn mạng cho công chức, viên chức, lao động hợp đồng tại Sở.

3. Đối với cán bộ nghỉ việc hoặc thay đổi vị trí việc làm

- Bàn giao công việc, tài sản CNTT được cấp, tài khoản truy cập các hệ thống thông tin tại Sở.

- Công chức, viên chức được giao phụ trách về an ninh, an toàn mạng thực hiện vô hiệu hóa tất cả các quyền truy cập hệ thống; kiểm tra lại các quyền ra vào, truy cập tài nguyên, quản trị hệ thống đã cấp sau khi cán bộ thôi việc, chuyển công tác, để đảm bảo đã hoàn toàn được gỡ bỏ khỏi hệ thống.

Điều 7. Thiết kế an toàn hệ thống thông tin

1. Bộ phận chuyên trách xây dựng tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin và thuyết minh trong Hồ sơ đề xuất cấp độ của hệ thống.

2. Bộ phận chuyên trách xây dựng tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin thuyết minh trong Hồ sơ đề xuất cấp độ của hệ thống.

Điều 8. Thử nghiệm và nghiệm thu hệ thống

1. Bên triển khai xây dựng kế hoạch, nội dung thử nghiệm hệ thống trước khi thực hiện thử nghiệm và nghiệm thu hệ thống.

2. Đơn vị vận hành thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác theo phương án thiết kế được phê duyệt trong Hồ sơ đề xuất cấp độ.

Điều 9. Quản lý an toàn mạng

1. Hệ thống mạng phải được thiết kế thống nhất, được quản lý xác thực đối với tất cả người sử dụng nhằm mục đích bảo đảm an toàn và bảo mật.

2. Hệ thống mạng nội bộ phải được bảo vệ bằng tường lửa và phân chia hệ thống mạng thành các vùng mạng quản lý theo chính sách an toàn thông tin riêng.

3. Mạng không dây (WIFI), cần thiết lập các thông số an toàn và định kỳ ít nhất 03 tháng thay đổi mật khẩu truy cập nhằm tăng cường công tác bảo mật. Hệ thống mạng không dây phải được bảo vệ bởi mật khẩu an toàn.

Điều 10. Quản lý an toàn dữ liệu

1. Có cơ chế sao lưu dữ liệu dự phòng, lưu trữ dữ liệu tại nơi an toàn đồng thời thường xuyên kiểm tra để đảm bảo sẵn sàng việc phục hồi nhằm ngăn ngừa và hạn chế khi sự cố an toàn thông tin mạng xảy ra. Quản lý chặt chẽ các thiết bị lưu trữ dữ liệu, nghiêm cấm việc di chuyển, thay đổi vị trí khi chưa được phép của người có thẩm quyền.

2. Quản lý và phân quyền truy cập phần mềm ứng dụng, cơ sở dữ liệu phù hợp với chức năng, nhiệm vụ của người sử dụng. Quyền truy cập phải được phân ra theo từng cấp độ tương ứng với từng nhiệm vụ của công chức, viên chức, người lao động và phải được phê duyệt từ cấp trên.

Điều 11. Quản lý an toàn thiết bị đầu cuối

Các thiết bị đầu cuối khi kết nối vào hệ thống phải được quản lý như sau:

1. Thông tin về các thiết bị đầu cuối phải được theo dõi quản lý, cập nhật.

2. Các thiết bị đầu cuối phải được quản lý theo kết nối vào hệ thống mạng theo địa chỉ IP.

3. Kiểm tra, đánh giá, xử lý các điểm yếu an ninh an toàn mạng cho các thiết bị đầu cuối trước khi đưa vào sử dụng

4. Quy định đối với máy tính kết nối mạng truyền số liệu chuyên dùng

a) Sử dụng hệ điều hành có bản quyền được hỗ trợ bản vá lỗ hổng bảo mật; trường hợp đã hết hỗ trợ phải có kế hoạch nâng cấp, thay thế. Chỉ cài đặt tiện ích thiết yếu được cung cấp kèm theo hệ điều hành và các phần mềm phục vụ công việc, có bản quyền hoặc được các cơ quan chức năng đánh giá, xác nhận an toàn. Cài đặt phần mềm phòng chống mã độc và cập nhật phần mềm thường xuyên.

b) Không kết nối với mạng không dây (WIFI), mạng dữ liệu di động.

c) Máy tính trước khi kết nối vào truyền số liệu chuyên dùng phải đáp ứng được quy định tại điểm a của khoản này; ngắt kết nối mạng của máy tính không đáp ứng quy định.

d) Máy tính khi được chuyển sử dụng từ cá nhân này sang cá nhân khác hoặc không tiếp tục sử dụng cho công việc của cơ quan phải thực hiện xóa toàn bộ dữ liệu trên ổ cứng và có biên bản về việc xóa dữ liệu. Máy tính khi mang đi bảo hành, bảo dưỡng, sửa chữa, phải tháo ổ cứng hoặc xóa dữ liệu lưu trên ổ cứng.

5. Máy tính soạn thảo, lưu trữ bí mật nhà nước

a) Sử dụng hệ điều hành và các phần mềm soạn thảo văn bản có bản quyền. Không kết nối vào mạng Internet, mạng nội bộ, mạng không dây, mạng viễn thông, trừ trường hợp đã áp dụng các biện pháp bảo vệ theo quy định. Không sử dụng thiết bị lưu trữ ngoại vi, trừ trường hợp cần cài đặt hệ điều hành, sửa chữa, nâng cấp phần mềm cho máy tính hoặc phục vụ công tác kiểm tra, thanh tra về an ninh an toàn mạng;

b) Phân quyền truy cập máy tính theo tên người hoặc đơn vị cấp phòng được giao soạn thảo bí mật nhà nước.

c) Trường hợp ổ cứng lỗi cần mang đi bảo hành, phải thực hiện biện pháp xóa dữ liệu vĩnh viễn trước khi mang ổ cứng ra khỏi cơ quan. Việc sửa chữa, nâng cấp phần mềm cho máy tính (sau khi đã đưa vào sử dụng), nếu yêu cầu phải tiếp cận các tệp tin trên ổ cứng, phải thực hiện dưới sự giám sát của đơn vị sử dụng máy tính, đảm bảo không lộ lọt dữ liệu trên ổ cứng máy tính ra bên ngoài trong quá trình này.

d) Đơn vị được cấp sử dụng máy tính soạn thảo, lưu trữ bí mật nhà nước chịu trách nhiệm giám sát, đảm bảo việc sử dụng máy tính tuân thủ đúng quy định tại khoản này.

6. Máy tính cán bộ tự trang bị khi kết nối vào mạng truyền số liệu chuyên dùng phải đáp ứng đầy đủ các điều kiện dưới đây:

a) Cài đặt đầy đủ các bản vá lỗ hổng bảo mật của hệ điều hành; cài đặt phần mềm phòng chống mã độc và cập nhật mẫu nhận diện mã độc mới nhất.

b) Không cài đặt, sử dụng phần mềm, công cụ có tính năng hoặc tạo rủi ro mất an ninh an toàn mạng (như cấp phát địa chỉ mạng, dò quét mật khẩu, dò quét cổng mạng, giả lập tấn công).

Điều 12. Phòng chống phần mềm độc hại

1. Các máy tính phải được trang bị phần mềm chống mã độc.

2. Khi gửi văn bản điện tử gửi qua hệ thống thư điện tử phải có định dạng theo Danh mục tiêu chuẩn kỹ thuật về ứng dụng CNTT trong cơ quan nhà nước như: (.txt), (.doc), (.odt), (.pdf) và các định dạng khác theo quy định, không được gửi các file thực thi (.com), (.bat), (.exe).

3. Cán bộ trong cơ quan không được tự ý cài đặt hoặc gỡ bỏ phần mềm phòng chống mã độc khi chưa có sự đồng ý của người có thẩm quyền theo quy định.

4. Khi phát hiện ra bất kỳ dấu hiện nào liên quan đến việc bị nhiễm mã độc trên máy trạm (ví dụ: máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống mã độc, mất dữ liệu…), người sử dụng phải báo trực tiếp cho bộ phận có phụ trách an ninh an toàn mạng của đơn vị để xử lý.

Điều 13. Quản lý rủi ro lỗ hổng, điểm yếu an ninh an toàn mạng

1. Phân loại mức độ nghiêm trọng của sự cố

a) Thấp: Sự cố gây ảnh hưởng cá nhân và không làm gián đoạn hay đình trệ hoạt động chính của các phòng, đơn vị thuộc Sở.

b) Trung bình: Sự cố ảnh hưởng đến một nhóm người dùng nhưng không gây gián đoạn hay đình trệ hoạt động chính của các phòng, đơn vị thuộc Sở.

c) Cao: Sự cố làm cho thiết bị, phần mềm hay hệ thống không thể sử dụng được và gây ảnh hưởng đến một trong các hoạt động chính của các phòng, đơn vị thuộc Sở.

d) Nghiêm trọng: Sự cố gây gián đoạn hoặc đình trệ hệ thống trong một khoảng thời gian ngắn, ảnh hưởng nghiêm trọng đến dữ liệu, thiết bị của hệ thống, gây thiệt hại nghiêm trọng cho cơ quan, đơn vị và người dân, doanh nghiệp.

đ) Đặc biệt nghiêm trọng: Sự cố làm tê liệt toàn bộ hoạt động của hệ thống, gây thiệt hại đặc biệt nghiêm trọng cho cơ quan, đơn vị và người dân, doanh nghiệp, đe dọa trật tự an toàn xã hội

2. Xử lý sự cố

Khi có sự cố thì cán bộ phải báo với bộ phận chuyên trách CNTT để kịp thời phối hợp xử lý. Đối với sự cố nghiêm trọng ở mức độ cao, khẩn cấp hoặc vượt quá khả năng khắc phục của bộ phận phụ trách CNTT tại Sở tỉnh thì bộ phận chuyên trách CNTT báo cáo ngay lãnh đạo Sở để phối hợp xử lý theo (thực hiện quy trình 5 bước tại khoản 5 Điều 16 Quyết định số 40/2025/QĐ-UBND tỉnh ngày 09/10/2025) quy định.

Điều 14. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ

Quy định, quy trình về Kết thúc vận hành, khai thác, thanh lý, hủy bỏ bao gồm các nội dung sau:

1. Thiết bị CNTT có chứa dữ liệu (máy tính, thiết bị lưu trữ, ...) khi bị hỏng phải được cán bộ vận hành kiểm tra, sửa chữa, khắc phục. Phải có biện pháp kiểm tra, giám sát đảm bảo không để lọt lộ thông tin hay lây nhiễm mã độc đối với máy tính mang ra bên ngoài sửa chữa, bảo hành.

2. Trước khi tiến hành thanh lý/loại bỏ thiết bị công nghệ thông tin cũ, phải áp dụng các biện pháp kỹ thuật xoá bỏ hoàn toàn dữ liệu người dùng đã tạo ra, đảm bảo không thể phục hồi.

3. Các phương tiện và thiết bị CNTT: Máy tính cá nhân (PC), máy tính xách tay, máy chủ, các thiết bị mạng, phương tiện lưu trữ như CD/DVD, thẻ nhớ, ổ cứng phải xóa sạch dữ liệu khi chuyển giao hoặc thay đổi mục đích sử dụng.

Chương III
TỔ CHỨC BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 15. Trách nhiệm của Sở Xây dựng

1. Thực hiện trách nhiệm theo quy định tại Điều 22 Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

2. Bố trí nhân lực chuyên trách để thực hiện công tác bảo đảm an ninh an toàn mạng tại Sở Xây dựng.

3. Thực hiện báo cáo định kỳ vào ngày 15/10 hàng năm hoặc đột xuất khi có yêu cầu về Công an tỉnh để tổng hợp, báo cáo Ủy ban nhân dân tỉnh, Bộ Công an.

Điều 16. Trách nhiệm của bộ phận đảm bảo an ninh an toàn mạng

1. Tham mưu lãnh đạo Sở duy trì hoạt động ổn định của hệ thống mạng của Sở Xây dựng, đảm bảo hệ thống hoạt động an toàn, thông suốt, đáp ứng nhu cầu của người dùng và các quy định theo quy chế an toàn thông tin của tỉnh và các quy định có liên quan.

2. Là đầu mối tiếp nhận, hỗ trợ xử lý các sự cố có nguy cơ làm mất an toàn thông tin trong hoạt động của cơ quan.

3. Thường xuyên giám sát, nhắc nhở, khuyến cáo cán bộ trong cơ quan tuân thủ các quy định tại Quy chế này và các quy định bảo đảm an toàn thông tin theo quy định hiện hành.

4. Thường xuyên cập nhật Quy định an toàn an ninh thông tin trong quá trình vận hành hệ thống an toàn thông tin.

5. Tham mưu lãnh đạo Sở phối hợp với các cơ quan chuyên môn liên quan về công tác bảo đảm an toàn thông tin để triển khai các nhiệm vụ về an toàn thông tin theo quy định.

6. Là đầu mối triển khai các hoạt động nghiệp vụ nhằm bảo đảm an toàn thông tin trong nội bộ cơ quan.

Điều 17. Trách nhiệm của cán bộ

1. Tuân thủ quy chế này và các quy định khác của pháp luật về bảo đảm an ninh an toàn mạng.

2. Khi phát hiện sự cố ảnh hưởng đến an ninh an toàn hệ thống thông tin, phải thông báo ngay đến cán bộ chuyên trách an ninh an toàn mạng; chịu trách nhiệm trước pháp luật và Lãnh đạo Sở về các vi phạm, thất thoát dữ liệu mật do không tuân thủ Quy chế.

3. Cán bộ chuyên trách an ninh an toàn mạng

a) Theo nhiệm vụ được phân công, chịu trách nhiệm tham mưu chuyên môn và vận hành bảo đảm an toàn hệ thống thông tin tại Sở Xây dựng;

b) Hướng dẫn, hỗ trợ người dùng giải pháp phòng, chống mã độc. Thực hiện việc đánh giá, báo cáo các rủi ro và mức độ các rủi ro ảnh hưởng đến hoạt động hệ thống thông tin của đơn vị, các giải pháp cơ bản khắc phục các rủi ro.

c) Phối hợp với các cá nhân, tổ chức có liên quan trong việc kiểm tra, phát hiện, phòng ngừa, đấu tranh, ngăn chặn xâm phạm an ninh an toàn mạng; tham gia khắc phục các sự cố mất an ninh an toàn mạng.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 18. Kinh phí thực hiện

1. Đối với Cơ quan Văn phòng Sở: Phòng Kinh tế - Kế hoạch chủ trì, phối hợp với Văn phòng Sở tham mưu Giám đốc Sở bố trí kinh phí thực hiện công tác bảo đảm an ninh, an toàn mạng theo quy định.

2. Đối với các đơn vị trực thuộc: Hằng năm, các đơn vị chủ động bố trí, sử dụng kinh phí của đơn vị để thực hiện công tác ứng dụng công nghệ thông tin và bảo đảm an ninh, an toàn mạng theo quy định hiện hành.

Điều 19. Trách nhiệm thi hành

1. Giao Văn phòng Sở là đơn vị đầu mối, chủ trì, phối hợp với các phòng, đơn vị triển khai thực hiện Quy chế này.

2. Trong quá trình thực hiện nếu có phát sinh khó khăn, vướng mắc kịp thời báo cáo Lãnh đạo Sở để xem xét, quyết định./.