

UBND TỈNH KHÁNH HÒA  
BAN QLDA ĐẦU TƯ XÂY DỰNG  
CÁC CÔNG TRÌNH GIAO THÔNG

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

Số: /QĐ-DAGT

Khánh Hòa, ngày tháng năm 2021

### QUYẾT ĐỊNH

**Ban hành Quy định về quản lý, vận hành, sử dụng thiết bị công nghệ thông tin và bảo đảm an toàn thông tin trên mạng nội bộ; Trao đổi, lưu trữ, xử lý văn bản điện tử, hồ sơ điện tử; Sử dụng chứng thư số của Ban Quản lý dự án đầu tư xây dựng các công trình giao thông tỉnh Khánh Hòa**

### GIÁM ĐỐC BAN QLDA ĐẦU TƯ XÂY DỰNG

### CÁC CÔNG TRÌNH GIAO THÔNG TỈNH KHÁNH HÒA

*Căn cứ Nghị định số 43/2011/NĐ-CP ngày 13/6/2011 của Chính phủ quy định về việc cung cấp thông tin và dịch vụ công trực tuyến trên trang thông tin điện tử hoặc cổng thông tin điện tử của cơ quan nhà nước;*

*Căn cứ Thông tư số 185/2019/TT-BQP ngày 04/12/2019 của Bộ Quốc phòng hướng dẫn về việc cung cấp, quản lý, sử dụng dịch vụ chứng thực chữ ký số chuyên dùng Chính phủ;*

*Căn cứ Thông tư số 19/2017/TT-BTTTT ngày 12/09/2017 của Bộ Thông tin và Truyền thông về việc Quy định công tác bảo vệ bí mật Nhà nước trong ngành thông tin và truyền thông;*

*Căn cứ Quyết định số 28/2018/QĐ-TTg ngày 12/07/2018 của Thủ tướng Chính phủ về việc gửi, nhận văn bản điện tử giữa các cơ quan trong hệ thống hành chính nhà nước;*

*Căn cứ Quyết định số 2103/QĐ-UBND ngày 21/7/2017 của UBND tỉnh Khánh Hòa ban hành Quy định quản lý, sử dụng chứng thư số chuyên dùng trong hoạt động của các cơ quan hành chính nhà nước tỉnh Khánh Hòa;*

*Căn cứ Quyết định số 1480/QĐ-UBND ngày 18/6/2012 của UBND tỉnh Khánh Hòa ban hành Quy định quản lý, sử dụng hệ thống Thư điện tử công vụ tỉnh Khánh Hòa trong hoạt động của các cơ quan hành chính nhà nước tỉnh Khánh Hòa;*

*Căn cứ Quyết định số 04/2021/QĐ-UBND ngày 15/03/2021 của UBND tỉnh Khánh Hòa về việc ban hành quy định trao đổi, lưu trữ, xử lý văn bản điện tử trong hoạt động của cơ quan nhà nước tỉnh Khánh Hòa;*

*Căn cứ Quyết định số 4053/QĐ-UBND ngày 27/12/2016 của UBND tỉnh Khánh Hòa về việc đổi tên Ban Quản lý dự án các công trình Trọng điểm tỉnh Khánh Hòa thành*

*Ban Quản lý dự án đầu tư xây dựng các công trình Giao thông tỉnh Khánh Hòa và kiện toàn chức năng, nhiệm vụ, quyền hạn, cơ cấu tổ chức;*

*Xét đề nghị của Phụ trách, quản lý phòng Kế hoạch – Tổng hợp,*

## **QUYẾT ĐỊNH:**

**Điều 1.** Ban hành kèm theo Quyết định này là Quy định về quản lý, vận hành, sử dụng thiết bị công nghệ thông tin và bảo đảm an toàn thông tin trên mạng nội bộ; Trao đổi, lưu trữ, xử lý văn bản điện tử, hồ sơ điện tử; Sử dụng chứng thư số của Ban Quản lý dự án đầu tư xây dựng các công trình giao thông tỉnh Khánh Hòa

**Điều 2.** Quyết định này thay thế quyết định số 399/QĐ-DAGT ngày 22/5/2019 và có hiệu lực kể từ ngày ký.

**Điều 3.** Trưởng phòng; Phụ trách quản lý các phòng thuộc Ban và các cá nhân liên quan có trách nhiệm thi hành quyết định này kể từ ngày ký./.

### ***Nơi nhận:***

- Như Điều 3;
- Trang TTĐT của Ban;
- Lưu: VT, MT.

**GIÁM ĐỐC**

**Đặng Hữu Tài**

## QUY ĐỊNH

**Quy định về quản lý, vận hành, sử dụng thiết bị công nghệ thông tin và bảo đảm an toàn thông tin trên mạng nội bộ; Trao đổi, lưu trữ, xử lý văn bản điện tử, hồ sơ điện tử; Sử dụng chứng thư số của Ban Quản lý dự án đầu tư xây dựng các công trình giao thông tỉnh Khánh Hòa**

*(Ban hành kèm theo Quyết định số /QĐ-DAGT ngày / /2021  
của Ban QLDA đầu tư xây dựng các công trình Giao thông tỉnh Khánh Hòa)*

## Chương I QUY ĐỊNH CHUNG

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

1. Quy định này quy định về nguyên tắc, nội dung, trách nhiệm của công chức, viên chức và người lao động thuộc Ban QLDA đầu tư xây dựng các công trình giao thông tỉnh Khánh Hòa (sau đây gọi tắt là Người sử dụng) trong việc quản lý, vận hành, sử dụng thiết bị công nghệ thông tin (CNTT) và hệ thống mạng nội bộ của Ban.

2. Các cơ quan, tổ chức, cá nhân không thuộc Ban khi có nhu cầu tham gia vào các hoạt động trực tiếp hoặc gián tiếp liên quan đến quản lý, vận hành, sử dụng thiết bị CNTT và hệ thống mạng nội bộ của Ban phải được sự đồng ý của Lãnh đạo Ban và tuân thủ các quy định của Quy định này và các quy định khác có liên quan.

### **Điều 2. Hệ thống thông tin của Ban Quản lý dự án đầu tư xây dựng các công trình giao thông tỉnh Khánh Hòa**

a) Hệ thống Quản lý văn bản và điều hành (sau đây gọi tắt là E-Office) được triển khai trên mạng Internet tại địa chỉ <https://qlvb.bqlctgt.khanhhoa.gov.vn>, thực hiện chức năng tin học hóa toàn bộ các nghiệp vụ hành chính văn phòng của Ban.

b) Trang thông tin điện tử của Ban được đăng tải trên mạng Internet tại địa chỉ <https://bqlctgt.khanhhoa.gov.vn>, thực hiện việc đăng tải và cung cấp đầy đủ thông tin theo quy định tại Nghị định số 43/2011/NĐ-CP ngày 13/6/2011 của Chính phủ quy định về việc cung cấp thông tin và dịch vụ công trực tuyến trên trang thông tin điện tử hoặc Cổng thông tin điện tử của cơ quan nhà nước.

c) Hệ thống Đấu thầu quốc gia được triển khai trên mạng internet tại địa chỉ: <http://muasamcong.mpi.gov.vn/> thực hiện các công việc liên quan đến lĩnh vực đấu thầu của Ban theo quy định của Luật Đấu thầu và các văn bản hướng dẫn của Bộ Kế hoạch và Đầu tư.

d) Sử dụng hệ thống Thư điện tử công vụ của tỉnh để gửi/ nhận thư, các văn bản, tài liệu điện tử qua mạng phục vụ công tác theo chức năng và nhiệm vụ được phân công tại địa chỉ mail công vụ: **bqlctgt@khanhhoa.gov.vn**.

e) Phần mềm Kế toán hành chính sự nghiệp được mua sắm từ nguồn thu của Ban và để phục vụ nghiệp vụ kế toán: quản lý dự toán ngân sách nhà nước hàng năm; sử dụng tiền mặt, tiền gửi tại Ban; tài sản cố định, công cụ, dụng cụ; lập các loại báo cáo, sổ tài chính. Thuê được quản lý bằng phần mềm của Cục Thuế Việt Nam, sử dụng dịch vụ Chứng thực chữ ký số và kê khai thuế trực tuyến của Cục Chứng thực số và Bảo mật thông tin, Ban Cơ yếu Chính phủ và VNPT.

f) Phần mềm Bảo hiểm xã hội tỉnh được triển khai trên mạng internet có chức năng kê khai bảo hiểm xã hội của các bộ Ban bằng cách sử dụng dịch vụ Chứng thực chữ ký số và kê khai bảo hiểm xã hội trực tuyến của Cục Chứng thực số và Bảo mật thông tin, Ban Cơ yếu Chính phủ và VNPT.

g) Sử dụng Chứng thư số chuyên dùng của cá nhân, tổ chức thuộc Ban để ký số gửi/ nhận văn bản điện tử, tài liệu điện tử qua mạng phục vụ công tác theo chức năng và nhiệm vụ được phân công.

h) Sử dụng Chứng thư số chuyên dùng cá nhân để ký số gửi/ nhận văn bản điện tử, tài liệu điện tử qua mạng phục vụ việc triển khai các dịch vụ công trực tuyến của kho bạc Nhà nước tỉnh theo Công văn số 10448/UBND-KT ngày 12/10/2018 của UBND tỉnh.

i) Trao đổi, xử lý văn bản điện tử, hồ sơ điện tử tuân thủ theo quy định tại Điều 6, Điều 7, Điều 8, Điều 9, Điều 10, Điều 11, Điều 12 của Quyết định số 04/2021/QĐ-UBND ngày 15/03/2021 của UBND tỉnh Khánh Hòa về việc ban hành quy định trao đổi, lưu trữ, xử lý văn bản điện tử trong hoạt động của cơ quan nhà nước tỉnh Khánh Hòa.

### **Điều 3. Quản lý, vận hành, sử dụng thiết bị CNTT trên mạng nội bộ của Ban**

1. Giám đốc Ban là người có quyền cao nhất trong mạng nội bộ của Ban, chịu trách nhiệm toàn diện về an toàn thông tin và tính pháp lý của thông tin trên mạng nội bộ của Ban.

2. Chuyên viên phụ trách về kỹ thuật và ứng dụng CNTT của Ban (sau đây gọi tắt là Quản trị mạng) là người được Giám đốc ủy quyền và chịu trách nhiệm trước Giám đốc về: quản trị mạng nội bộ của Ban; quản trị Người sử dụng mạng của Ban; giúp Giám đốc Ban thực hiện chức năng quản lý, vận hành mạng nội bộ của Ban đạt hiệu quả cao nhất;

3. Người sử dụng mạng nội bộ của Ban là những người nêu tại Điều 1 Quy định này, có kiến thức về sử dụng thiết bị CNTT, mạng nội bộ là các hệ thống thông tin được triển khai trên mạng nội bộ của Ban, được đăng ký tài khoản người dùng trong các hệ thống thông tin của Ban tương ứng với quyền và nghĩa vụ thực thi công vụ của mỗi cá nhân tại Ban.

### **Điều 4. Quyền và nghĩa vụ của Người sử dụng**

1. Tuyệt đối tuân thủ các nguyên tắc, kỹ thuật sử dụng, khai thác, trao đổi thông tin trên mạng theo quy định tại Điều 5 của Quy định này nhằm bảo đảm tính an toàn cho các hệ thống thông tin của Ban và các hệ thống thông tin dùng chung của tỉnh.

2. Được cung cấp máy tính cá nhân và quyền sử dụng các hệ thống thông tin trên mạng phục vụ cho nhiệm vụ chuyên môn của mình.

3. Được quyền chia sẻ tài nguyên (thiết bị ngoại vi, phần cứng, phần mềm, dữ liệu) trên máy tính cá nhân của mình cho những người sử dụng khác trên mạng và tự chịu trách nhiệm về các tài nguyên được chia sẻ này.

4. Có trách nhiệm cập nhật thông tin thường xuyên theo quy định cho các hệ thống thông tin theo chức năng, nhiệm vụ được phân công và chịu trách nhiệm hoàn toàn về tính chính xác của nguồn thông tin do mình cung cấp.

5. Phối hợp với Quản trị mạng (người phụ trách công nghệ thông tin) trong việc bảo đảm duy trì hoạt động thường xuyên và ổn định các phần mềm trên máy vi tính cá nhân của mình nhằm phục vụ công tác giám sát hoặc công tác chuyên môn.

6. Không đăng tải, trao đổi hoặc phát tán các thông tin không hợp pháp (thông tin có nội dung phản động, đồi trụy, phản khoa học,...) trên mạng, không được sử dụng mạng nội bộ của Ban vào mục đích riêng.

7. Không được cài đặt các phần mềm không có bản quyền trên máy tính cá nhân do cơ quan giao cho sử dụng và chịu hoàn toàn trách nhiệm trước pháp luật về việc sử dụng các phần mềm này.

8. Tất cả các thiết bị mạng, máy chủ, máy tính cá nhân, các phần mềm hệ thống, các phần mềm ứng dụng, các thiết bị và phần mềm khác hiện đang hoạt động trên mạng nội bộ của Ban phục vụ công việc quản lý, điều hành và tác nghiệp của Ban. Người sử dụng không được tự ý thay đổi vị trí kết nối, cấu hình của thiết bị; không sử dụng các thiết bị ngoài quyền hạn được phép.

9. Nghiêm cấm sử dụng máy tính đã kết nối mạng Internet để soạn thảo, gửi, nhận, lưu trữ văn bản có tính chất mật.

## **Chương II**

### **SỬ DỤNG MẠNG NỘI BỘ VÀ QUY ĐỊNH VỀ TRAO ĐỔI, LƯU TRỮ, XỬ LÝ VĂN BẢN ĐIỆN TỬ, HỒ SƠ ĐIỆN TỬ CỦA BAN**

**Điều 5. Nguyên tắc sử dụng mạng nội bộ và quy định về trao đổi, lưu trữ, xử lý văn bản điện tử, hồ sơ điện tử của Ban**

1. Tất cả các văn bản truyền nhận trên mạng nội bộ của Ban phải bảo đảm các điều kiện sau:

a) Thể thức và kỹ thuật trình bày văn bản thực hiện theo quy định tại Thông tư số 01/2011/TT-BNV ngày 19/01/2011 của Bộ Nội vụ về việc hướng dẫn thể thức và kỹ thuật trình bày văn bản hành chính.

b) Sử dụng bộ mã ký tự chữ tiếng Việt theo tiêu chuẩn TCVN 6909:2001.

2. Sử dụng tài khoản:

a) Người sử dụng chịu trách nhiệm bảo đảm bí mật các tài khoản truy cập mạng nội bộ của Ban theo quy định tại Điều 12 của Quy định này.

b) Máy tính cá nhân bắt buộc phải đặt mật khẩu người dùng, không cung cấp mật khẩu cho người khác. Các thư mục chia sẻ chung phải đặt mật khẩu để bảo đảm an toàn file dữ liệu.

c) Quản trị mạng (người phụ trách công nghệ thông tin) chỉ cung cấp mật khẩu cho người sử dụng khai thác điểm truy nhập mạng không dây sau khi được sự đồng ý của Lãnh đạo Ban.

### 3. Truy cập mạng nội bộ của Ban:

a) Việc truy cập, sử dụng các ứng dụng trên mạng nội bộ của Ban phải tuân theo quy định tại Khoản 2, Điều 5 của Quy định này.

b) Việc đặt tên, đặt địa chỉ IP, có sự thay đổi vị trí làm việc của phòng, cá nhân, việc giữ nguyên hay thay đổi các tham số đã cài trên máy phải thông báo đến Quản trị mạng để phối hợp và báo cáo cho Lãnh đạo Ban sau khi thực hiện.

c) Việc truy cập vào mạng nội bộ của Ban thông qua thiết bị không dây (Access Point) từ các thiết bị di động (laptop, smartphone, máy tính bảng, ...) chỉ phục vụ cho các đối tượng trong nội bộ phòng. Trường hợp cần phục vụ hội nghị, hội thảo, tập huấn ... người chủ trì việc tổ chức cần báo cho Quản trị mạng (người phụ trách công nghệ thông tin) biết để phối hợp và đề xuất biện pháp giải quyết.

d) Các hành vi nghiêm cấm trong quá trình truy cập mạng nội bộ của Ban:

- Truy cập và phát tán các nội dung trái quy định của pháp luật;
- Chia sẻ hoặc tự ý cho người ngoài Ban sử dụng kết nối mạng Internet của Ban;
- Không sử dụng mạng nội bộ của Ban để sử dụng vào các mục đích khác ngoài công việc. Không được gắn thẻ nhớ usb vào máy tính khi chưa được kiểm tra và quét virus độc hại.

### 4. Truy xuất ra bên ngoài mạng nội bộ của Ban:

a) Xuất phát từ nhu cầu quản lý, điều hành tác nghiệp của người sử dụng, Quản trị mạng (người phụ trách công nghệ thông tin) có trách nhiệm phối hợp với phòng Kế hoạch – Tổng hợp tổng hợp trình Lãnh đạo Ban về mục đích, lý do, phạm vi, người chịu trách nhiệm, vị trí thực hiện và vị trí mạng bên ngoài cần truy xuất đến.

b) Việc truy xuất ra bên ngoài bảo đảm các điều kiện sau:

- Không trao đổi, truyền dẫn thông tin nghiệp vụ thuộc Ban quản lý dưới bất kỳ hình thức nào ra bên ngoài khi chưa được Lãnh đạo Ban đồng ý.

- Không trao đổi thông tin, dữ liệu lạ từ bên ngoài vào mạng nội bộ của Ban nếu chưa được Quản trị mạng (người phụ trách công nghệ thông tin) kiểm tra độ an toàn thông tin đối với mạng nội bộ Ban và chưa được sự đồng ý của Lãnh đạo Ban.

- Đối với dịch vụ Internet: Người sử dụng đều phải tuân theo các quy định sử dụng dịch vụ Internet do các cơ quan nhà nước có thẩm quyền ban hành.

### 5. Quy định về trao đổi, lưu trữ, xử lý văn bản điện tử, hồ sơ điện tử:

a) Tính hợp pháp và các loại văn bản điện tử được quy định như sau:

- Tính hợp pháp của văn bản điện tử được quy định tại Điều 3 Quyết định số 04/2021/QĐ-UBND ngày 15/03/2021 của UBND tỉnh Khánh Hòa về việc ban hành quy định trao đổi, lưu trữ, xử lý văn bản điện tử trong hoạt động của cơ quan nhà nước tỉnh Khánh Hòa;

- Danh mục văn bản trao đổi hoàn toàn dưới dạng điện tử được quy định tại Điều 4 Quyết định số 04/2021/QĐ-UBND ngày 15/03/2021 của UBND tỉnh Khánh Hòa về việc ban hành quy định trao đổi, lưu trữ, xử lý văn bản điện tử trong hoạt động của cơ quan nhà nước tỉnh Khánh Hòa.

- Danh mục văn bản trao đổi dưới dạng điện tử gửi kèm văn bản giấy được quy định tại Điều 5 của Quyết định số 04/2021/QĐ-UBND ngày 15/03/2021 của UBND tỉnh Khánh Hòa về việc ban hành quy định trao đổi, lưu trữ, xử lý văn bản điện tử trong hoạt động của cơ quan nhà nước tỉnh Khánh Hòa.

b) Quy trình trao đổi, xử lý văn bản điện tử, hồ sơ điện tử được quy định tại Điều 6, Điều 7, Điều 8, Điều 9 Quyết định số 04/2021/QĐ-UBND ngày 15/03/2021 của UBND tỉnh Khánh Hòa về việc ban hành quy định trao đổi, lưu trữ, xử lý văn bản điện tử trong hoạt động của cơ quan nhà nước tỉnh Khánh Hòa;

c) Thời điểm gửi/nhận văn bản điện tử, thông báo nhận, trả lại văn bản điện tử, xử lý văn bản điện tử, hồ sơ điện tử quy định tại Điều 10, Điều 11, Điều 12 của Quyết định số 04/2021/QĐ-UBND ngày 15/03/2021 của UBND tỉnh Khánh Hòa về việc ban hành quy định trao đổi, lưu trữ, xử lý văn bản điện tử trong hoạt động của cơ quan nhà nước tỉnh Khánh Hòa;

d) Lập và nộp lưu hồ sơ điện tử vào lưu trữ cơ quan quy định tại Điều 13, Điều 14 Quyết định số 04/2021/QĐ-UBND ngày 15/03/2021 của UBND tỉnh Khánh Hòa về việc ban hành quy định trao đổi, lưu trữ, xử lý văn bản điện tử trong hoạt động của cơ quan nhà nước tỉnh Khánh Hòa.

## **Điều 6. Tác nghiệp trên hệ thống Quản lý văn bản và điều hành**

1. Người sử dụng được cấp một tài khoản (*tên đăng nhập và mật khẩu*) để đăng nhập vào Hệ thống và có trách nhiệm bảo mật thông tin về tài khoản của mình theo quy định tại Điều 12 của Quy định này.

2. Các luồng thông tin điều hành, tác nghiệp, xử lý văn bản, báo cáo nội bộ, họp nội bộ, trung cầu ý kiến và các luồng thông tin trao đổi khác trong phạm vi của Sở và các đơn vị sự nghiệp trực thuộc đều được thống nhất thực hiện trên hệ thống E-Office.

3. Người sử dụng có trách nhiệm tuân thủ các quy trình xử lý thông tin trên E-Office một cách nghiêm túc, chặt chẽ nhằm phát huy cao nhất hiệu quả của hệ thống. Các thông tin chỉ đạo, xử lý, phản hồi và trao đổi trên E-Office phải rõ ràng, minh bạch và được chuyển đúng đối tượng, đúng quy trình.

4. Việc cung cấp thông tin không đầy đủ hoặc chuyển luồng xử lý thông tin sai đối tượng, sai quy trình dẫn đến sự ách tắc, cản trở hoạt động tác nghiệp thông tin

tiếp theo của những Người sử dụng khác (mà không phải do lỗi của hệ thống E-Office) sẽ được xem như hành vi thiếu trách nhiệm trong khi thi hành công vụ.

5. Quản trị mạng có trách nhiệm thiết lập giải pháp an toàn thông tin để người sử dụng có thể truy nhập vào hệ thống E-Office từ môi trường Internet.

### **Điều 7. Sử dụng hệ thống Thư điện tử công vụ**

1. Các cán bộ Ban có trách nhiệm liên quan sử dụng thư điện tử công vụ đúng theo quy định tại Điều 10, Điều 11 và Điều 12 Quyết định số 38/2015/QĐ-UBND ngày 24/12/2015 của UBND tỉnh ban hành Quy định đảm bảo an toàn thông tin số trong hoạt động ứng dụng công nghệ thông tin trên địa bàn tỉnh Khánh Hòa và Quyết định số 1480/QĐ-UBND ngày 18/06/2012 của UBND tỉnh ban hành Quy định quản lý, sử dụng hệ thống Thư điện tử công vụ tỉnh Khánh Hòa trong hoạt động của các cơ quan hành chính nhà nước tỉnh Khánh Hòa.

2. Khi tài khoản thư điện tử công vụ khi đã đầy sẽ dẫn đến tình trạng gửi/nhận thư điện tử bị chậm, có thể xảy ra lỗi. Người sử dụng thực hiện khắc phục bằng cách: xóa toàn bộ thư rác và các thư có nội dung không quan trọng; lưu trữ nội dung thư điện tử công vụ quan trọng trên mạng dùng chung của Ban ở hoặc ổ cứng máy tính để bàn.

3. Trường hợp lỗi gắn tệp đính kèm khi gửi thư điện tử công vụ, Người sử dụng liên hệ với bộ phận Quản trị mạng (người phụ trách công nghệ thông tin) để được tư vấn và hỗ trợ.

4. Trường hợp Người sử dụng đã được cấp thư điện tử công vụ thì có nghĩa vụ thay đổi mật khẩu đối với các tài khoản đang còn sử dụng mật khẩu mặc định. Bảo vệ mật khẩu thư công vụ của mình; không cung cấp hoặc để lộ mật khẩu của mình cho người khác; không để người khác sử dụng thư công vụ của mình. Thường xuyên thay đổi mật khẩu trong quá trình sử dụng, trường hợp quên mật khẩu phải báo cho Quản trị mạng kịp thời.

5. Các cán bộ Ban được cấp thư điện tử công vụ nghiêm túc trong việc sử dụng hộp thư điện tử với tên miền “@**khanhhoa.gov.vn**” đã được cấp phát.

6. Không được sử dụng hộp thư cá nhân (như yahoo, gmail hoặc các dịch vụ cung cấp Email khác trên thị trường) để trao đổi công việc với Văn phòng chính phủ, UBND tỉnh, các Sở, ban, ngành, địa phương trên địa bàn tỉnh Khánh Hòa và các cơ quan Nhà nước hoặc các tổ chức và cá nhân khác liên quan.

7. Thường xuyên kiểm tra thư công vụ của đơn vị, cá nhân mình để tiếp nhận và xử lý kịp thời các thông tin, các ý kiến của Lãnh đạo, các phòng ban, cơ quan, đơn vị và cá nhân khác gửi đến.

8. Không được sử dụng thư điện tử công vụ nhằm phát tán thư rác. Người sử dụng chịu trách nhiệm về nội dung thư điện tử của mình gửi lên mạng.

9. Không được mở những thư có địa chỉ không rõ ràng hoặc những thư có dấu hiệu nghi ngờ không an toàn. Thường xuyên dọn dẹp và xóa bỏ các thư rác hoặc thư không cần thiết trong hộp thư điện tử công vụ của mình.

### **Điều 8. Sử dụng các phần mềm khác của Ban**



1. Người sử dụng tham gia vận hành, sử dụng phần mềm theo đúng chức năng, nhiệm vụ được giao; được cấp tài khoản (*tên đăng nhập và mật khẩu*) để đăng nhập vào phần mềm và có trách nhiệm bảo mật thông tin về tài khoản của mình theo quy định tại Điều 11 của Quy định này.

2. Trong trường hợp xảy ra sự cố làm phần mềm tạm ngừng hoạt động, Người sử dụng phải báo cáo với Quản trị mạng (người phụ trách công nghệ thông tin); đồng thời thực hiện giải quyết công việc bằng biện pháp thủ công và nhập đầy đủ thông tin vào hệ thống ngay sau khi phần mềm hoạt động trở lại.

3. Quản trị mạng (người phụ trách công nghệ thông tin) có trách nhiệm tạo mới và phân quyền cho người sử dụng tham gia phần mềm theo chức năng, nhiệm vụ được giao; bảo đảm hệ thống vận hành thông suốt; hướng dẫn người sử dụng sử dụng hiệu quả phần mềm.

### **Điều 10. Sử dụng chứng thư số chuyên dùng**

1. Người sử dụng khi sử dụng chứng thư số chuyên dùng thực hiện đúng theo quy định tại Thông tư số 185/2019/TT-BQP ngày 04/12/2019 của Bộ Quốc phòng hướng dẫn về việc cung cấp, quản lý, sử dụng dịch vụ chứng thực chữ ký số chuyên dùng Chính phủ.

2. Người sử dụng hoàn toàn chịu trách nhiệm về việc quản lý chứng thư số chuyên dùng của mình. Trường hợp mất, thất lạc phải thông báo ngay cho Quản trị mạng để thực hiện thủ tục hủy bỏ chứng thư số cũ và làm lại đề nghị cấp mới.

3. Người sử dụng khi được cấp sử dụng chứng thư số thì phải thực hiện thay đổi mật khẩu mặc định ngay khi đăng nhập sử dụng lần đầu tiên.

4. Người sử dụng không được phép giao chứng thư số của mình đang sử dụng cho người khác khi chưa được sự đồng ý của Giám đốc Ban.

5. Thẩm quyền thu hồi chứng thư số được thực hiện theo qui định tại Điều 10 Thông tư số 185/2019/TT-BQP ngày 04/12/2019 của Bộ Quốc phòng hướng dẫn về việc cung cấp, quản lý, sử dụng dịch vụ chứng thực chữ ký số chuyên dùng Chính phủ.

6. Việc thay đổi thông tin người quản lý chứng thư số của cơ quan (chứng thư số của thiết bị, dịch vụ, phần mềm) áp dụng theo quy định tại Điều 9 Thông tư số 185/2019/TT-BQP ngày 04/12/2019 của Bộ Quốc phòng hướng dẫn về việc cung cấp, quản lý, sử dụng dịch vụ chứng thực chữ ký số chuyên dùng Chính phủ.

7. Việc cấp chứng thư số sau khi chứng thư số cũ hết hạn hoặc chứng thư số bị thu hồi thì áp dụng theo quy định tại Điều 9, Điều 10 của Thông tư số 185/2019/TT-BQP ngày 04/12/2019 của Bộ Quốc phòng hướng dẫn về việc cung cấp, quản lý, sử dụng dịch vụ chứng thực chữ ký số chuyên dùng Chính phủ.

8. Việc khôi phục và quản lý thiết bị lưu khóa bí mật: áp dụng theo quy định tại Điều 11 Thông tư số 185/2019/TT-BQP ngày 04/12/2019 của Bộ Quốc phòng hướng dẫn về việc cung cấp, quản lý, sử dụng dịch vụ chứng thực chữ ký số chuyên dùng Chính phủ.

## **Chương III**

## **QUY ĐỊNH VỀ BẢO MẬT VÀ AN TOÀN THÔNG TIN**

### **Điều 10. Bảo đảm an toàn thông tin trong việc sử dụng máy tính cá nhân**

1. Máy tính cá nhân do cơ quan cấp cho người sử dụng để phục vụ công việc và được quản lý theo các quy định của pháp luật về quản lý tài sản nhà nước.

2. Quản trị mạng (người phụ trách công nghệ thông tin) có trách nhiệm cài đặt các chương trình, phần mềm trên các máy tính cá nhân của cơ quan phục vụ công việc của từng nhóm người sử dụng (văn thư, kế toán, ...).

3. Quản trị mạng (người phụ trách công nghệ thông tin) có trách nhiệm thực hiện các biện pháp cơ bản sau nhằm bảo đảm an toàn thông tin cho các máy tính cá nhân của cơ quan:

- a) Cài đặt và sử dụng các phần mềm, hệ điều hành có bản quyền;
- b) Thường xuyên cập nhật các bản vá bảo mật cho phần mềm và hệ điều hành;
- c) Cài đặt phần mềm chống phần mềm có hại, kiểm tra toàn bộ thông tin, dữ liệu, tập tin ngay khi được tải về hoặc trước khi sao chép, lưu trữ vào máy tính;
- d) Cài đặt tường lửa cá nhân để chặn các truy cập từ bên ngoài trái với quy định;
- đ) Cấu hình máy tính cá nhân để mỗi người sử dụng chỉ được phép truy cập các thư mục lưu trữ dữ liệu của mình, không truy cập các thư mục lưu trữ dữ liệu của cá nhân khác trên máy tính dùng chung;
- e) Sử dụng chức năng mã hóa dữ liệu, khóa thư mục để đề phòng trường hợp dữ liệu bị đánh cắp;
- g) Hiện thị đầy đủ phần mở rộng của tập tin để không kích hoạt nhầm tập tin thực thi mà tập tin đó có thể là phần mềm có hại hoặc chứa mã độc.

#### **4. Máy tính soạn thảo văn bản bảo mật:**

a) Máy tính dùng để soạn thảo, lưu trữ, trao đổi, sao chụp tin, tài liệu mật không có kết nối Internet hoặc không có kết nối với các thiết bị khác có kết nối Internet;

b) Việc sửa chữa, thay thế các máy tính dùng để soạn thảo, lưu trữ thông tin bí mật nhà nước chỉ được tiến hành tại Ban và phải do cá nhân có trách nhiệm đối với những thông tin bí mật này thực hiện hoặc giám sát. Khi thay thế ổ đĩa cứng của máy vi tính có thông tin về tài liệu, vật mang bí mật nhà nước phải xóa, hủy thông tin trong ổ đĩa cũ, khi bị hỏng thì được tiêu hủy theo quy định.

c) Việc soạn thảo, lưu trữ, trao đổi, sao chụp tin, tài liệu mật trên máy tính bảo mật tuân thủ theo Thông tư số 19/2017/TT-BTTTT ngày 12/09/2017 của Bộ Thông tin và Truyền thông quy định công tác bảo vệ bí mật Nhà nước trong ngành thông tin và truyền thông.

5. Các hành động sau đây phải được thông báo đến Quản trị mạng và phòng Kế hoạch – Tổng hợp để được xem xét tư vấn và phải có sự đồng ý của thủ trưởng cơ quan trước khi tiến hành:

- a) Thay đổi cấu hình máy tính cá nhân do cơ quan cấp;

- b) Kết nối máy tính cá nhân do cơ quan cấp vào các mạng nội bộ khác;
- c) Cài đặt các phần mềm khác lên máy tính cá nhân do cơ quan cấp;
- d) Kết nối máy tính thuộc sở hữu cá nhân vào mạng nội bộ của Ban;
- đ) Nhận hỗ trợ các thiết bị CNTT hoặc phần mềm ứng dụng từ các tổ chức, cá nhân khác bên ngoài Ban;
- e) Thay đổi vị trí công tác hoặc chuyển công tác sang đơn vị khác;
- f) Sử dụng máy tính của người khác.

**Điều 11. Bảo đảm an toàn thông tin trong việc quản lý và sử dụng tài khoản và mật khẩu**

1. Người sử dụng khi được cấp tài khoản và mật khẩu để truy cập vào các hệ thống thông tin trong mạng nội bộ của Ban có trách nhiệm:

a) Thay đổi mật khẩu ngay lần đầu đăng nhập. Mật khẩu thay đổi yêu cầu phải đáp ứng các nguyên tắc sau:

- Có ít nhất 08 ký tự;
- Có chứa cả các ký tự chữ in và chữ thường;
- Có chứa ký tự số, các ký tự dấu câu hoặc các ký tự đặc biệt;
- Không phải là một từ hoàn chỉnh trong các ngôn ngữ thông dụng (tiếng Việt, tiếng Anh, tiếng Pháp, ...);
- Không phải là một dãy ký tự lặp lại có quy luật;
- Không dựa vào thông tin cá nhân (ngày sinh, số điện thoại, ...), tên người, tên địa danh, tên cơ quan hoặc các tên gọi khác;

b) Mật khẩu phải được thay đổi định kỳ 06 tháng một lần.

2. Quản trị mạng (người phụ trách công nghệ thông tin) có trách nhiệm thay đổi mật khẩu quản trị hệ thống định kỳ 03 tháng một lần. Nguyên tắc thay đổi mật khẩu được áp dụng theo quy định tại Điểm a Khoản 1 Điều này.

3. Các hành vi bị nghiêm cấm trong việc sử dụng tài khoản được cấp:

- a) Lưu trữ hoặc gửi mật khẩu các tài khoản trên các phương tiện điện tử;
- b) Dùng cùng một mật khẩu cho các tài khoản khác nhau để truy cập vào hệ thống mạng nội bộ của Ban;
- c) Dùng mật khẩu trong hệ thống mạng nội bộ của Ban cho các tài khoản cá nhân;
- d) Cho người khác biết mật khẩu (trừ trường hợp Lãnh đạo Ban yêu cầu);
- đ) Dùng chức năng ghi nhớ mật khẩu của các ứng dụng trên máy tính dùng chung;
- e) Sử dụng mật khẩu đã bị đánh cắp hoặc nghi ngờ bị đánh cắp cho tài khoản cũ hoặc các tài khoản khác do Quản trị mạng (người phụ trách công nghệ thông tin) cấp;

g) Không kịp thời thông báo cho Quản trị mạng (người phụ trách công nghệ thông tin) biết khi nghi ngờ mật khẩu tài khoản của mình bị người khác biết ngoài ý muốn.

## **Điều 12. Phòng chống các phần mềm có hại (virus, worm, spyware, ...)**

1. Quản trị mạng (người phụ trách công nghệ thông tin) có trách nhiệm thực hiện các quy định tại Điều a, b, c, d Khoản 3, Điều 11 của Quy định này.

2. Người sử dụng có trách nhiệm bảo đảm các biện pháp phòng chống các phần mềm độc hại như sau:

a) Sử dụng các chương trình chống phần mềm độc hại do Quản trị mạng cài đặt. Cập nhật phiên bản và cơ sở dữ liệu mới nhất theo chính sách của Ban;

b) Không tải dữ liệu từ nguồn thông tin không rõ ràng hay nghi ngờ có hại cho máy tính cá nhân và mạng nội bộ của Ban;

c) Không mở tài liệu, tập tin gửi kèm trong các thư điện tử từ những địa chỉ không biết rõ hoặc không đáng tin cậy;

d) Không tự ý sử dụng chức năng chia quyền truy cập đĩa trực tiếp (disk sharing). Nếu do yêu cầu công việc cần sử dụng tính năng này cần phải thông báo với Quản trị mạng;

đ) Luôn luôn quét virus từ các phương tiện lưu trữ thứ cấp như USB, đĩa cứng ngoài,...trước khi sử dụng;

e) Khi phát hiện các chương trình làm ảnh hưởng đến hoạt động của chương trình chống phần mềm độc hại hoặc các phần mềm ứng dụng của Ban, Người sử dụng phải kịp thời thông báo cho Quản trị mạng (người phụ trách công nghệ thông tin) biết để có biện pháp xử lý.

## **Điều 13. Xử lý sự cố**

Khi gặp bất kỳ sự cố về điện, sét,...hoặc các hiện tượng khác ảnh hưởng tới hoạt động của thiết bị liên quan đến các bộ phận của mạng như: phần cứng, phần mềm, cơ sở dữ liệu thì Người sử dụng phải lập tức ngừng các hoạt động giao dịch thông tin và báo ngay cho Quản trị mạng (người phụ trách công nghệ thông tin) để khắc phục, sửa chữa.

## **Chương IV KHEN THƯỞNG, XỬ PHẠT**

### **Điều 14. Khen thưởng**

Mọi cá nhân phải có ý thức bảo vệ và phát triển mạng nội bộ của Ban. Cá nhân, tập thể thực hiện tốt các quy định của Quy định này và có nhiều đóng góp xây dựng, phát triển mạng nội bộ của Ban sẽ được khen thưởng theo quy định.

### **Điều 15. Xử phạt**

Mọi hành vi cố ý vi phạm các quy định của Quy định này đều bị xử lý kỷ luật hoặc xử phạt theo các quy định tại Quy chế chi tiêu nội bộ và quản lý, sử dụng tài sản

công của Ban Quản lý dự án đầu tư xây dựng các công trình giao thông tỉnh Khánh Hòa.

## **Chương V** **TỔ CHỨC THỰC HIỆN**

### **Điều 16. Tổ chức thực hiện**

1. Quản trị mạng có trách nhiệm chủ trì tổ chức triển khai và hướng dẫn thực hiện Quy định này; phối hợp với Lãnh đạo các phòng thuộc Ban thường xuyên kiểm tra, đôn đốc, nhắc nhở các cá nhân có liên quan thực hiện nghiêm Quy định này.

2. Các tổ chức, cá nhân khác được Giám đốc Ban cho phép sử dụng mạng nội bộ của Ban có trách nhiệm thực hiện nghiêm Quy định này.

3. Trong quá trình thực hiện, nếu có khó khăn vướng mắc, đề nghị kịp thời phản ánh về Quản trị mạng (người phụ trách công nghệ thông tin) và phòng Kế hoạch – Tổng hợp để tổng hợp báo cáo Giám đốc Ban xem xét, giải quyết./.

**GIÁM ĐỐC**

**Đặng Hữu Tài**