UBND TỈNH KHÁNH HÒA
BAN QUẢN LÝ DỰ ÁN
PHÁT TRIỂN TỈNH KHÁNH HÒA

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

QUY ĐỊNH
Đảm bảo an toàn thông tin số, an ninh mạng thông tin của Ban Quản lý dự án Phát triển tỉnh Khánh Hòa

(Ban hành kèm theo Quyết định số: 118 /QĐ-BQL ngày 24 tháng 10 năm 2018 của Ban Quản lý dự án Phát triển tỉnh Khánh Hòa)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Nguyên tắc chung

Nhằm đảm bảo an toàn thông tin số, an ninh mạng thông tin của Ban Quản lý dự án Phát triển tỉnh Khánh Hòa, cụ thể như sau:

1. Nguyên tắc bảo đảm an toàn thông tin phải tuân thủ các nguyên tắc tại Điều 4 của Luật An toàn thông tin và Điều 4 của Nghị định số 85/2016/NĐ-CP;

2. Cán bộ, công chức, viên chức có trách nhiệm bảo đảm an toàn thông tin của cơ quan, đơn vị mình theo đúng quy định của pháp luật;

3. Được thực hiện thường xuyên, liên tục từ khâu thiết kế, xây dựng, vận hành đến khi hủy bỏ; tuân thủ theo các tiêu chuẩn, quy chuẩn kỹ thuật được các cơ quan chức năng ban hành;

4. Nhận biết, phân loại, đánh giá kịp thời và xử lý có hiệu quả các rủi ro an toàn thông tin mạng có thể xảy ra trong cơ quan, đơn vị.

Điều 2. Đối tượng áp dụng

Tất cả cán bộ, công chức, viên chức đang làm việc tại Ban Quản lý dự án Phát triển tỉnh Khánh Hòa.

Chương II
CÁC QUY ĐỊNH VỀ ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG

Điều 3. Quản lý tài sản công nghệ thông tin

1.Tài sản vật lý: các thiết bị công nghệ thông tin, phương tiện truyền thông và các thiết bị phục vụ cho hoạt động của hệ thống thông tin như hệ thống mạng, Switch, modem ADSL , … phải có các biện pháp bảo vệ, ngăn chặn xâm nhập trái phép;

2. Tài sản thông tin: các thông tin, dữ liệu ở dạng số;

3. Tài sản phần mềm: các phần mềm hệ thống, phần mềm tiện ích, cơ sở

dữ liệu, chương trình ứng dụng và công cụ phát triển.

Điều 4. Yêu cầu cơ bản về quản lý tài sản công nghệ thông tin

1. Lập danh mục tài sản công nghệ thông tin. Thường xuyên cập nhật và quản lý danh mục.

2. Giao, gán trách nhiệm cho cá nhân hoặc tập thể quản lý, sử dụng tài sản.

3. Quy định các quy tắc sử dụng, gìn giữ, bảo vệ tài sản trong các trường hợp như: mang tài sản ra khỏi cơ quan, tài sản liên quan tới dữ liệu nhạy cảm, cài đặt và cấu hình,...

4. Tài sản vật lý 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.

Điều 5. Yêu cầu chung đối với nơi lắp đặt

1. Có biện pháp bảo vệ, kiểm soát, hạn chế rủi ro xâm nhập trái phép, phòng chống nguy cơ do cháy nổ, thiên tai, thảm họa.

2. Các khu vực có yêu cầu cao về an toàn như khu vực lắp đặt thiết bị lưu trữ, thiết bị an ninh bảo mật, thiết bị truyền thông phải được ban hành nội quy, hướng dẫn thực hiện.

Chương III
QUẢN LÝ VẬN HÀNH VÀ THÔNG TIN LIÊN LẠC

Điều 6. Vai trò, trách nhiệm đảm bảo an toàn, an ninh thông tin mạng

1. Lãnh đạo cơ quan có vai trò lãnh đạo cao nhất về an toàn thông tin số, an ninh mạng thông tin tại đơn vị. Chỉ đạo, tổ chức, triển khai, đôn đốc việc thực hiện các chính sách, quy trình, quy định, hướng dẫn và các giải pháp kỹ thuật nhằm đảm bảo an toàn, an ninh thông tin mạng của cơ quan. Phân công CBCCVC thực hiện nhiệm vụ an toàn, an ninh thông tin mạng.

2. Thường xuyên kiểm tra, đánh giá điểm yếu về an toàn, an ninh thông tin mạng tại cơ quan; tiến hành áp dụng các biện pháp, giải pháp kỹ thuật nhằm đảm bảo an toàn thông tin của cơ quan.

Điều 7. Sao lưu dữ liệu

1. Lập danh sách các dữ liệu, phần mềm cần được sao lưu, có phân loại theo mức độ quan trọng, thời gian lưu trữ, thời gian sao lưu, phương pháp sao lưu và thời gian kiểm tra phục hồi hệ thống từ dữ liệu sao lưu.

2. Dữ liệu của các hệ thống thông tin quan trọng phải được sao lưu ra phương tiện lưu trữ ngoài (như băng từ, đĩa cứng, đĩa quang hoặc phương tiện lưu trữ khác) và cất giữ, bảo quản an toàn tách rời với khu vực tiến hành sao lưu. Kiểm tra, phục hồi dữ liệu sao lưu từ phương tiện lưu trữ ngoài tối thiểu sáu tháng một lần.

3. Cần tách biệt giữa sao lưu dữ liệu và sao lưu ứng dụng. Mọi ứng dụng được cài đặt hoặc xóa bỏ khỏi hệ thống thông tin đều cần được sao lưu vào hệ

thống dự phòng, tách biệt khỏi hệ thống sao lưu dữ liệu.

4. Định kỳ sao lưu hàng tuần, tháng, quý.

Điều 8. Đảm bảo an toàn, bảo mật trong trao đổi thông tin

1. Ban hành quy định về trao đổi thông tin tối thiểu gồm: Phân loại thông tin theo mức độ nhạy cảm; quyền và trách nhiệm của cá nhân khi tiếp cận thông tin; biện pháp đảm bảo tính toàn vẹn, bảo mật khi truyền nhận, xử lý, lưu trữ thông tin; chế độ bảo quản thông tin.

2. Các thông tin, tài liệu, dữ liệu nhạy cảm phải được mã hóa trước khi trao đổi, truyền nhận qua mạng máy tính.

3. Thực hiện các biện pháp quản lý, giám sát và kiểm soát chặt chẽ Trang thông tin điện tử tổng hợp của cơ quan khi cung cấp thông tin cho các tổ chức, cá nhân bên ngoài.

4. Thực hiện biện pháp bảo vệ trang thiết bị, phần mềm phục vụ trao đổi thông tin nội bộ nhằm hạn chế việc xâm nhập, khai thác bất hợp pháp các thông tin nhạy cảm.

Điều 9. Phòng chống mã độc

1. Xác định trách nhiệm của người sử dụng và các bộ phận liên quan trong công tác phòng chống mã độc.

2. Triển khai biện pháp, giải pháp phòng chống mã độc cho toàn bộ hệ thống thông tin của cơ quan.

3. Cập nhập thông tin về các loại mã độc hại mới, triển khai các hành động phòng ngừa tại cơ quan khi có các nguy cơ về các loại mã độc này.

4. Kiểm tra, diệt mã độc đối với vật mang tin nhận từ bên ngoài trước khi sử dụng.

5. Kiểm soát việc cài đặt phần mềm đảm bảo tuân thủ theo quy chế an toàn, an ninh thông tin của cơ quan.

6. Xây dựng các kế hoạch phục hồi đối với từng hệ thống CNTT trong trường hợp xảy ra các sự cố về mã độc máy tính.

7. Phối hợp với các cơ quan, đơn vị liên quan thường xuyên cập nhật thông tin về các loại mã độc hại mới để có các phương án phòng ngừa các nguy cơ về các loại mã độc này gây ra.

Điều 10. Vai trò, trách nhiệm của cán bộ, công chức, viên chức

1. Nghiêm túc chấp hành các chính sách, quy trình, quy định, hướng dẫn, các giải pháp kỹ thuật để đảm bảo an toàn, an ninh thông tin trong hoạt động chuyên môn, nghiệp vụ của cơ quan.

2. Nắm, hiểu và tuân thủ các quy trình, quy định, chính sách, hướng dẫn về an toàn thông tin trong quá trình thực hiện nhiệm vụ được giao.

3. Quy định bảo vệ thông tin/dữ liệu: Nghiệm cấm CBCCVC không thu thập, cung cấp, trao đổi, làm lộ, làm mất, chiếm đoạt, mua bán, tiêu hủy trái phép các thông tin về chủ trương, chính sách của Đảng và nhà nước, các thông tin có liên quan đến hoạt động chuyên môn, nghiệp vụ của cơ quan.

4. Quy định sử dụng mật khẩu: Phải đặt mật khẩu truy cập máy tính, thiết bị và các phần mềm nội bộ (email, phần mềm quản lý văn bản...) theo đúng quy định mật khẩu mạnh:

- Có ít nhất 8 ký tự;

- Mật khẩu bao gồm: chữ, số, ký tự đặc biệt;

- Định kỳ đổi mật khẩu theo quy định, đối với mật khẩu máy tính người dùng là 90 ngày;

- Giữ bí mật, không chia sẻ mật khẩu cho người khác. Khi bị lộ mật khẩu, hoặc nghi ngờ mật khẩu bị lộ phải đổi ngay mật khẩu mới, trong trường hợp không thể tự đổi phải làm thủ tục reset mật khẩu theo quy trình quản lý cấp phát tài khoản tương ứng. Khi được cung cấp mật khẩu mới hoặc được reset mật khẩu cần phải đổi ngay mật khẩu mới.

5. 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 hoặc các đơn vị khác có liên quan.

6. Không dùng thư điện tử công vụ của cá nhân hoặc của cơ quan vào mục đích cá nhân như đăng ký tài khoản mạng xã hội, đăng ký mua sắm qua mạng...

7. Nghiêm cấm các hành vi sau:

- Lợi dụng mạng máy tính, Internet để hoạt động xâm phạm an ninh quốc gia, trật tự an toàn xã hội, vi phạm thuần phong mỹ tục, bản sắc văn hoá Việt Nam, xâm phạm các quyền và lợi ích hợp pháp của tổ chức, công dân cũng như tiến hành các hoạt động tội phạm dưới bất cứ hình thức, phương tiện nào;

- Lưu giữ trên máy tính kết nối Internet tin, tài liệu, số liệu thuộc bí mật nhà nước.

Chương IV
QUẢN LÝ SỰ CỐ AN TOÀN THÔNG TIN MẠNG

Điều 11. Yêu cầu về an toàn, an ninh cho hệ thống thông tin

1. Xây dựng các yêu cầu về an toàn, an ninh đồng thời với việc đưa ra các yêu cầu kỹ thuật, nghiệp vụ.

2. Đánh giá, xác định cấp độ và tuân thủ đầy đủ các quy định về bảo đảm an toàn thông tin của hệ thống theo cấp độ tương ứng.

3. Xây dựng các yêu cầu về trách nhiệm cập nhật, vá lỗi, khắc phục lỗ hổng bảo mật… của hệ thống thông tin, được phát hiện trong quá trình vận hành.

4. Xây dựng kế hoạch định kỳ, kiểm tra, rà soát về an toàn an ninh thông tin trong quá trình vận hành hệ thống.

Điều 12. Quy trình xử lý sự cố

1. Tiếp nhận thông tin sự cố.

2. Xác thực sự cố.

3. Thông tin cho lãnh đạo cơ quan về sự cố.

4. Thu thập thông tin về sự cố.

5. Phân tích thông tin về sự cố.

6. Xử lý sự cố (yêu cầu hỗ trợ nếu cần).

7. Tổng kết đánh giá kết quả.

8. Báo cáo lãnh đạo cơ quan và các đơn vị liên quan.

Điều 13. Nguyên tắc kiểm soát và khắc phục sự cố

1. Các sự cố mất an toàn thông tin mạng phải được lập tức báo cáo đến những người có thẩm quyền và những người có liên quan.

2. Xác định nguyên nhân và thực hiện các biện pháp phòng ngừa.

3. Quá trình xử lý sự cố phải được ghi chép và lưu trữ. Thực hiện biện pháp bảo vệ, chống chỉnh sửa, hủy hoại đối với tài liệu lưu trữ về sự cố.

4. Thu thập, ghi chép, bảo toàn bằng chứng, chứng cứ phục vụ cho việc kiểm tra, xử lý, khắc phục và phòng ngừa sự cố.

Chương V
KHEN THƯỞNG KỶ LUẬT

Điều 14. Khen thưởng

Định kỳ hàng năm cơ quan xem xét, đề xuất khen thưởng, hình thức khen thưởng cho các cá nhân/tập thể có thành tích trong công tác đảm bảo an toàn thông tin.

Điều 15. Kỷ luật

Đối với các CBCCVC có hành vi vi phạm Quy định này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật theo trách nhiệm. Nếu gây thiệt hại thì phải bồi thường theo quy định hiện hành của pháp luật.

Chương VI
TỔ CHỨC THỰC HIỆN

Điều 16. Trách nhiệm thi hành

1. Cán bộ, công chức, viên chức và các đơn vị liên quan có trách nhiệm thực hiện nghiêm túc Quy định này.

2. Trong quá trình thực hiện nếu có khó khăn, vướng mắc phát sinh thì phản ánh về Phòng Tổ chức hành chính để tổng hợp, báo cáo lãnh đạo Ban xem xét, sửa đổi, bổ sung cho phù hợp./.

GIÁM ĐỐC

Người ký: Châu Ngô Anh Nhân
Cơ quan: Ban Quản lý dự án phát triển, Tỉnh Khánh Hòa
Chức vụ: Giám đốc
Thời gian ký: 24.10.2018 21:59:25 +07:00