UBND TỈNH KHÁNH HÒA
TỔNG CÔNG TY KHÁNH VIỆT

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

Số: 103 /QĐ-HĐTV

Khánh Hòa, ngày 29 tháng 9 năm 2017

QUYẾT ĐỊNH
Về việc ban hành Quy chế bảo đảm an toàn thông tin Tổng công ty Khánh Việt

HỘI ĐỒNG THÀNH VIÊN TỔNG CÔNG TY KHÁNH VIỆT

Căn cứ Quyết định số 2914/QĐ-UBND ngày 13 tháng 11 năm 2009 của Ủy ban nhân dân tỉnh Khánh Hòa về việc phê duyệt Phương án chuyển đổi và chuyển Tổng công ty Khánh Việt thành Tổng công ty trách nhiệm hữu hạn một thành viên Khánh Việt;

Căn cứ Quyết định số 1922/QĐ-UBND ngày 29 tháng 7 năm 2010 của Ủy ban nhân dân tỉnh Khánh Hòa về việc điều chỉnh tên gọi của Tổng công ty trách nhiệm hữu hạn một thành viên Khánh Việt thành Tổng công ty Khánh Việt;

Căn cứ Điều lệ tổ chức và hoạt động của Tổng công ty Khánh Việt – Công ty trách nhiệm hữu hạn một thành viên được Uỷ ban nhân dân tỉnh Khánh Hòa ban hành theo Quyết định số 18/QĐ-UBND ngày 08 tháng 01 năm 2015;

Căn cứ Biên bản họp Hội đồng thành viên Tổng công ty Khánh Việt ngày 29 tháng 9 năm 2017,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn thông tin Tổng công ty Khánh Việt; Quy chế gồm 4 Chương, 15 Điều và có hiệu lực thi hành kể từ ngày 01 tháng 10 năm 2017.

Điều 2. Tổng Giám đốc, Trưởng các Phòng, Ban, Trung tâm thuộc Văn phòng Tổng công ty Khánh Việt, Giám đốc các đơn vị hạch toán phụ thuộc và các Công ty con của Tổng công ty Khánh Việt chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 2;
- HĐTV, KSV TCT;
- Lưu: VT,TK.

QD-23

TM. HỘI ĐỒNG THÀNH VIÊN
CHỦ TỊCH

M.S.D.N: 4200486169 - C.T.T.N.H.H
TỔNG CÔNG TY KHÁNH VIỆT
TP. NHA TRANG - T. KHÁNH HÒA

Lê Tiến Anh

UBND TỈNH KHÁNH HÒA
TỔNG CÔNG TY KHÁNH VIỆT

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

QUY CHẾ
Đảm bảo an toàn thông tin Tổng công ty Khánh Việt
(Ban hành kèm theo Quyết định số 103/QĐ-HĐTV ngày 29/9/2017 của Hội đồng thành viên Tổng công ty Khánh Việt)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Mục đích, phạm vi và đối tượng áp dụng

1. Mục đích:

Quy định này quy định về việc đảm bảo an toànthông tin dữ liệu trên môi trườngmáy tính, mạng máy tính của Tổng công ty Khánh Việt. Thông tin dữ liệu bao gồm tất cả các loại thông tin dạng số hóa (cơ sở dữ liệu, phần mềm quản lý) được gửi đi và đến Tổng công ty Khánh Việt (sau đây gọi tắt là Tổng công ty).

2. Phạm vi và đối tượng áp dụng:

Quy chế này áp dụng đối với tất cả Viên chức quản lý và toàn thể người lao động thuộc Tổng công ty (sau đây gọi tắt là CBCNV).

Điều 2. Giải thích từ ngữ

Trong quy định này, các từ ngữ dưới đây được hiểu như sau:

1. "Thông tin": là dữ liệu liên quan đến hoạt động sản xuất, kinh doanh của Tổng công ty, ví dụ: cơ sở dữ liệu của phần mềm, các file tài liệu, nội dung mail, cuộc hội thoại...

1. "An toàn thông tin": là thông tin và hệ thống thông tin không bị truy cập, sử dụng, tiết lộ, gián đoạn, sửa đổi, phá hoại trái phép.

2. "Hệ thống thông tin": là tập hợp thiết bị phần cứng, phần mềm và cơ sở dữ liệu của Tổng công ty phục vụ tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin.

3. "Hệ thống quan trọng": là hệ thống thông tin có ảnh hưởng lớn tới hoạt động của Tổng công ty.

4. "Mạng nội bộ": là mạng máy tính trong phạm vi trụ sở của một đơn vị thuộc Tổng công ty.

5. "Mã độc": 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.

6. "Điểm yếu": điểm có thể bị khai thác gây mất an toàn thông tin; còn được gọi là "lỗ hổng bảo mật".

7. "Rủi ro an toàn thông tin": khả năng mất an toàn thông tin.

8. "Sự cố an toàn thông tin": là sự kiện mất an toàn thông tin.

9. "Mật khẩu phức tạp": là mật khẩu đáp ứng các yêu cầu sau:

a) Có tối thiểu 8 ký tự.

b) 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 trên bàn phím máy tính (` ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; " ' <> , . ? /) và dấu cách.

10. "Người dùng": là tất cả CBCNV thuộc Tổng công ty sử dụng máy tính để xử lý công việc.

11. Tài khoản: là tên người dùng và mật mã truy cập vào máy tính, email, các phần mềm, ...

12. Khóa máy tính: là hành động ngăn không cho người khác sử dụng máy tính trong khi máy tính vẫn hoạt động. Muốn sử dụng máy tính trở lại (mở khóa máy tính) phải có mật khẩu.

13. Tính năng Autoplay: là tính năng tự động chạy các file thực thi trên các thiết bị lưu trữ ngoài như ổ đĩa flash, ổ cứng gắn ngoài, CD, DVD... khi được gắn vào máy tính.

14. Bộ phận công nghệ thông tin (CNTT): là nhân viên hoặc nhóm nhân viên được chỉ định phụ trách các công việc liên quan đến CNTT trong tổ chức như sửa chữa máy tính, thiết bị CNTT, quản trị mạng, mail, máy chủ, đảm bảo an toàn thông tin,...

15. VNCERT: Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam, là tổ chức trực thuộc Bộ Thông tin và Truyền thông, thực hiện chức năng điều phối hoạt động ứng cứu sự cố máy tính trên toàn quốc; cảnh báo kịp thời các vấn đề về an toàn mạng máy tính; phối hợp xây dựng các tiêu chuẩn, quy chuẩn kỹ thuật về an toàn mạng máy tính.

16. Đơn vị: Văn phòng Tổng công ty, các đơn vị hạch toán phụ thuộc và các công ty con của Tổng công ty Khánh Việt.

Điều 3. Yêu cầu chung

1. Đảm bảo an toàn thông tin là yêu cầu bắt buộc trong quá trình tạo lập, xử lý, sử dụng thông tin và thiết kế, xây dựng, vận hành, nâng cấp, hủy bỏ hệ thống thông tin.

2. Đơn vị, người dùng thực hiện các công đoạn liên quan đến thông tin nêu tại khoản 1 điều này có trách nhiệm đảm bảo an toàn thông tin theo quy định và hướng dẫn của quy chế này.

Điều 4. Những hành vi bị nghiêm cấm

1. Vi phạm các quy định về quản lý, vận hành và sử dụng mạng của Tổng công ty gây rối loạn hoạt động của hệ thống, trong đó bao gồm các hành vi: tự ý đấu nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập không dây của cá nhân vào mạng nội bộ;

2. Can thiệp trái phép, gây nguy hại, xóa, thay đổi, sửa chữa, làm sai lệch thông tin trên mạng.

3. Phát tán thư rác, mã độc, thiết lập hệ thống thông tin giả mạo, lừa đảo trong mạng của Tổng công ty; lợi dụng điểm yếu của hệ thống thông tin để tấn công, chiếm quyền điều khiển trái phép đối với hệ thống.

4. Làm mất tác dụng của biện pháp an toàn thông tin do bộ phận CNTT thiết lập, trong đó bao gồm các hành vi: tự ý thay đổi, gỡ bỏ biện pháp an toàn thông tin cài đặt trên thiết bị CNTT; tự ý thay thế, lắp mới, tráo đổi thành phần của máy tính.

5. Lợi dụng mạng để truyền bá thông tin, quan điểm, thực hiện các hành vi gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội; phá hoại khối đại đoàn kết toàn dân; tuyên truyền chiến tranh xâm lược, khủng bố; gây thù hận, mâu thuẫn giữa các dân tộc, sắc tộc, tôn giáo.

6. Lợi dụng mạng để truyền bá trái phép tài liệu, hình ảnh, âm thanh hoặc dạng thông tin khác làm ảnh hưởng đến uy tín công ty; kích động bạo lực, dâm ô, đồi trụy, tội ác, tệ nạn xã hội, mê tín dị đoan, phá hoại thuần phong, mỹ tục của dân tộc; bôi nhọ, gây thù hận, xâm hại tới quyền và lợi ích hợp pháp của tổ chức, cá nhân.

Chương II
TRÁCH NHIỆM CỦA NGƯỜI SỬ DỤNG

Điều 5. Đảm bảo an toàn mức vật lý

1. Các khu vực sau phải được kiểm soát truy cập vật lý để phòng tránh truy cập trái phép hoặc sai mục đích: Trung tâm dữ liệu; khu vực chứa máy chủ và thiết bị lưu trữ; tủ mạng và đấu nối; thiết bị nguồn điện và dự phòng điện khẩn cấp; phòng vận hành, kiểm soát, quản trị hệ thống.

2. Thiết bị CNTT khi mang đi bảo hành, bảo dưỡng, sửa chữa, điều chuyển nội bộ, cho, tặng phải phối hợp với Bộ phận CNTT xử lý nhằm đảm bảo an toàn dữ liệu.

3. Thiết bị lưu trữ khi thanh lý, cho, tặng hoặc không sử dụng phải được xoá nội dung hoặc hủy bằng thiết bị hủy dữ liệu chuyên dụng hay phá hủy vật lý.

Điều 6. Đảm bảo an toàn hệ thống thông tin

1. Máy tính phải được cài đặt phần mềm phòng chống mã độc, thường xuyên cập nhật mẫu mã độc cùng với bản vá lỗi an ninh hệ điều hành mới nhất.

2. Không được can thiệp vào các phần mềm đã cài đặt trên máy tính (thay đổi, gỡ bỏ,…) khi chưa được sự đồng ý của bộ phận CNTT.

3. Thực hiện thao tác khóa máy tính khi rời khỏi nơi đặt máy tính; tắt máy tính khi rời khỏi cơ quan sau giờ làm việc (Các trường hợp đặc biệt cần mở máy thì phải báo với bộ phận CNTT để ghi nhận).

4. Không mở các thư điện tử không rõ nguồn gốc.

5. Không mở các tệp tin hoặc các liên kết không rõ nguồn gốc (từ mail, chat, mạng xã hội...) để tránh virus máy tính, mã độc.

6. Không vào các trang web không có nguồn gốc xuất xứ rõ ràng, đáng ngờ.

7. Khi phát hiện những trường hợp lạ, đáng nghi hoặc trong trường hợp phần mềm phòng chống mã độc phát cảnh báo thì báo ngay cho bộ phận CNTT xử lý.

8. Không chia sẻ dữ liệu ổ cứng. Trong trường hợp cần chia sẻ thì chỉ chia sẻ thư mục cần thiết và phải sử dụng mật khẩu để bảo vệ thông tin.

9. Khi kết nối các thiết bị lưu trữ ngoài (ổ cứng di động, ổ flash, CD, DVD...), smartphone vào máy tính: Cần dùng chương trình phòng chống mã độc để quét toàn bộ nội dung các thiết bị này trước khi truy cập và sử dụng. Ngoài ra, máy tính cần được tắt tính năng Autoplay để đề phòng mã độc trong các thiết bị này tự thực thi và lây lan.

10. Không được phép truy cập từ xa vào mạng nội bộ (sử dụng một máy tính bên ngoài để điều khiển các thiết bị CNTT trong mạng nội bộ) từ những điểm truy cập Internet công cộng.

Điều 7. Đảm bảo an toàn dữ liệu

1. Các dữ liệu, thông tin mật, quan trọng hoặc nhạy cảm cần được thiết lập mật khẩu.

2. Chỉ sử dụng hệ thống thư điện tử và các công cụ trao đổi thông tin do Tổng công ty quản lý để trao đổi dữ liệu quan trọng.

3. Không sử dụng mạng Internet công cộng trong việc trao đổi dữ liệu quan trọng.

Điều 8. Sao lưu, dự phòng sự cố

1. Sao lưu dữ liệu thường xuyên trên thiết bị lưu trữ ngoài hoặc dịch vụ lưu trữ trực tuyến có uy tín (khuyến nghị 1 lần/ tuần hoặc thường xuyên hơn).

2. Đối với cơ sở dữ liệu các chương trình quan trọng như kế toán, bán hàng, quản trị doanh nghiệp, ... phối hợp với Bộ phận CNTT (nếu cần) để sao lưu hàng ngày ra thiết bị lưu trữ riêng biệt.

Điều 9: Quản lý tài khoản

1. Xác thực tài khoản:

a) Mật khẩu phức tạp nên được áp dụng cho tất cả các tài khoản truy cập, sử dụng, quản trị hệ thống.

b) Đổi mật khẩu ngay sau khi nhận bàn giao từ người khác hoặc có thông báo về sự cố an toàn thông tin, điểm yếu liên quan đến khả năng lộ mật khẩu; khuyến nghị đổi mật khẩu tối thiểu 03 tháng một lần đối với tài khoản của người dùng.

c) Người dùng có trách nhiệm bảo mật thông tin tài khoản được cấp.

2. Thay đổi tài khoản:

Khi có người lao động thay đổi vị trí, luân chuyển công tác, thôi việc hoặc nghỉ hưu, bộ phận quản lý hoặc nhân viên chuyên trách nhân sự có trách nhiệm thông báo cho Bộ phận CNTT đơn vị và Bộ phận CNTT Tổng công ty (nếu cần) để xử lý các tài khoản liên quan:

- Đối với tài khoản cá nhân: điều chỉnh hay hủy bỏ các quyền sử dụng đối với hệ thống mạng, ứng dụng (trừ một số trường hợp đặc biệt phải có sự đồng ý của lãnh đạo đơn vị).

- Đối với tài khoản dùng chung: Thay đổi mật khẩu.

Điều 10. Phối hợp xử lý sự cố an toàn thông tin

1. Báo cáo kịp thời cho Bộ phận CNTT khi phát hiện các sự cố, nguy cơ gây mất an toàn thông tin Tổng công ty.

2. Phối hợp và tạo điều kiện cho Bộ phận CNTT trong suốt quá trình giải quyết sự cố.

Chương III
TRÁCH NHIỆM CỦA BỘ PHẬN CÔNG NGHỆ THÔNG TIN

Điều 11. Yêu cầu chung

1. Đơn vị phải thành lập Bộ phận CNTT hoặc cử nhân viên phụ trách CNTT.

2. Nhân viên Bộ phận CNTT phải có kiến thức về an toàn thông tin trên môi trường máy tính, mạng máy tính.

Điều 12. Quản trị hệ thống mạng và thiết bị CNTT.

1. Kiểm tra, bảo dưỡng định kỳ hệ thống mạng và các thiết bị CNTT.

2. Có kế hoạch dự phòng khi xảy ra sự cố hệ thống thông tin.

3. Quy hoạch hệ thống mạng nội bộ thành các vùng mạng theo phạm vi truy cập:

- Vùng mạng máy chủ nội bộ;

- Vùng mạng người dùng, trong đó tách riêng vùng mạng cho kết nối có dây và không dây;

- Vùng mạng riêng cho khách (Chặn truy cập vào hệ thống mạng nội bộ của công ty nhưng có thể sử dụng Internet).

4. Giám sát và phòng chống các cuộc tấn công vào hệ thống mạng nội bộ.

5. Hệ thống mạng không dây phải được áp dụng phương pháp xác thực WPA/WPA2 (Wi-Fi protected access - một giao thức an ninh trên mạng không dây) hoặc các phương pháp an toàn hơn. Tắt tính năng WPS (Wi-Fi Protected Setup - một tiêu chuẩn cho việc thiết lập dễ dàng mạng không dây) trên các thiết bị không dây có hỗ trợ WPS.

6. Hệ thống camera an ninh: Thiết lập camera ở mạng độc lập so với mạng nội bộ. Các hệ thống camera an ninh được lắp đặt cần tuân thủ các điều kiện sau:

- Đổi mật khẩu quản trị camera ngay sau khi lắp đặt, không dùng mật khẩu mặc định của nhà sản xuất.

- Thường xuyên theo dõi và cập nhật bản vá lỗi an ninh phần mềm cho camera.

- Chỉ cho phép xem camera từ Bộ phận an ninh hoặc các phòng chức năng được lãnh đạo phê duyệt (không cho kết nối đến camera từ xa).

7. Trong trường hợp phát hiện sự cố xảy ra ngoài khả năng giải quyết của mình phải báo cáo ngay cho cơ quan cấp trên quản lý trực tiếp hoặc Sở Thông tin và Truyền thông địa phương hoặc VNCERT để được hỗ trợ, hướng dẫn và phối hợp khắc phục sự cố.

Điều 13. An toàn kết nối Internet

1. Áp dụng các biện pháp cần thiết để đảm bảo an toàn thông tin trong hoạt động kết nối Internet, tối thiểu đáp ứng yêu cầu sau:

a) Có tường lửa kiểm soát truy cập Internet.

b) Lọc bỏ, không cho phép truy cập các trang tin có nghi ngờ chứa mã độc hoặc các nội dung không phù hợp (phản động hoặc trái thuần phong mỹ tục).

2. Cập nhật thường xuyên danh sách các máy địa chỉ IP, tên miền được cảnh báo từ VNCERT để ngăn chặn quá trình hoạt động của mã độc trong hệ thống mạng nội bộ.

Điều 14. Quản trị phần mềm

1. Chịu trách nhiệm cài đặt phần mềm ứng dụng và phần mềm phòng chống mã độc cho các máy tính tại đơn vị mình.

2. Cập nhật bản vá an ninh cho hệ điều hành, cơ sở dữ liệu cho phần mềm phòng chống mã độc, tường lửa, hệ thống phát hiện và phòng chống tấn công,...

3. Kiểm soát việc cài đặt phần mềm trên các máy chủ, máy tính của người dùng, thiết bị mạng đang hoạt động thuộc hệ thống mạng nội bộ, đảm bảo các phần mềm khi cài đặt trong hệ thống có nguồn gốc an toàn, không bị nhiễm mã độc.

4. Đối với phần mềm mua ở dạng đóng gói:

a) Theo dõi, nắm bắt thông tin về các điểm yếu được phát hiện và cập nhật thường xuyên bản vá lỗi về an ninh cho phần mềm.

b) Trường hợp điểm yếu đã được phát hiện mà chưa có bản vá lỗi của đơn vị sản xuất phần mềm, phải thực hiện đánh giá rủi ro và có biện pháp phòng tránh phù hợp.

Chương IV
ĐIỀU KHOẢN THI HÀNH

Điều 15. Tổ chức thực hiện

1. CBCNV Tổng công ty có trách nhiệm thực hiện các nội dung có liên quan của Quy chế này.

2. Tập thể, cá nhân vi phạm quy chế đảm bảo an toàn thông tin làm ảnh hưởng đến việc sản xuất kinh doanh của Tổng công ty thì tùy theo tính chất, mức độ của hành vi vi phạm sẽ bị xử lý theo quy định của Tổng công ty.

3. Trong quá trình thực hiện Quy chế, Bộ phận CNTT Tổng công ty có thể trình lãnh đạo sửa đổi, bổ sung quy định này để phù hợp với tình hình và điều kiện thực tế.

4. Trưởng các Phòng, Ban, Trung tâm thuộc Văn phòng Tổng công ty và Giám đốc các đơn vị thuộc Tổng công ty có trách nhiệm phổ biến cho CBCNV của đơn vị mình thực hiện quy chế này.

5. Quy chế này gồm 4 Chương, 15 Điều và có hiệu lực thi hành theo Quyết định ban hành Quy chế của Hội đồng thành viên Tổng công ty Khánh Việt./.

TM. HỘI ĐỒNG THÀNH VIÊN
CHỦ TỊCH

M.S.D.N: 4200486169 - C.T.T.N.H.H - TỔNG CÔNG TY KHÁNH VIỆT - TP. NHA TRANG - T. KHÁNH HÒA

Lê Tiến Anh