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.