



**EVN**

TẬP ĐOÀN ĐIỆN LỰC VIỆT NAM

CÔNG TY VIỄN THÔNG ĐIỆN LỰC VÀ CÔNG NGHỆ THÔNG TIN

## TRUYỀN THÔNG

# HỆ THỐNG QUẢN LÝ AN TOÀN THÔNG TIN TRONG EVNICT

HÀ NỘI, 8/14/2024



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# NỘI DUNG

1

**VĂN BẢN QUY PHẠM PHÁP LUẬT  
QUY CHẾ QUẢN LÝ NỘI BỘ EVN/EVNICT  
VỀ AN TOÀN THÔNG TIN**

2

**NGUYÊN TẮC QUẢN LÝ ATTT  
RỦI RO VÀ BIỆN PHÁP KIỂM SOÁT**

3

**TRÁCH NHIỆM QUẢN LÝ ATTT TẠI ĐƠN VỊ**

4

**QUY TẮC ĐẢM BẢO ATTT  
ĐỐI VỚI NGƯỜI SỬ DỤNG**





EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# PHẦN 1

## VĂN BẢN QUY PHẠM PHÁP LUẬT QUY CHẾ QUẢN LÝ NỘI BỘ EVN/EVNICT VỀ AN TOÀN THÔNG TIN



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# VĂN BẢN QUY PHẠM PHÁP LUẬT LIÊN QUAN VỀ AN TOÀN THÔNG TIN

1

Luật An ninh mạng

24/2018/QH14 ngày 01/06/2018

Luật An toàn thông tin mạng

86/2015/QH13 ngày 19/11/2015

Luật tiếp cận thông tin

104/2016/QH13 ngày 06/04/2016

Nghị định về Đảm bảo an toàn hệ thống thông tin theo cấp độ 85/2016/NĐ-CP ngày 01/07/2016

Nghị định về bảo vệ dữ liệu cá nhân

13/2023/NĐ-CP ngày 17/4/2023

Nghị định về Quản lý, kết nối và chia sẻ dữ liệu  
số của cơ quan nhà nước

47/2020/NĐ-CP ngày 09/04/2020

Chống tin nhắn rác, thư điện tử rác, cuộc gọi rác

91/2020/NĐ-CP ngày 01/08/2020

Quy định xử phạt vi phạm hành chính trong lĩnh vực  
bưu chính, viễn thông, tần số vô tuyến điện, công nghệ  
thông tin và giao dịch điện tử

15/2020/NĐ-CP ngày 03/02/2020



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# QUY CHẾ QUẢN LÝ NỘI BỘ EVN LIÊN QUAN VỀ AN TOÀN THÔNG TIN

1

Quy định Đảm bảo an toàn thông tin  
99/QĐ-EVN ngày 18/01/2021

Quy định quản lý, khai thác Hệ thống thông tin  
1268/QĐ-EVN ngày 18/09/2021

Quy trình ứng cứu sự cố an toàn thông tin mạng  
trong EVN  
1828/QĐ - EVN ngày 30/12/2022

Bộ quy tắc cấu hình an toàn thông tin  
QĐ 1290/EVN ngày 05/09/2022

Quy chế Quản trị trong Tập đoàn Điện lực Quốc  
gia Việt Nam  
123/QĐ-HĐTV ngày 01/10/2021

Đề án "Đảm bảo an toàn thông tin cho hệ thống thông  
tincủa Tập đoàn Điện lực quốc gia Việt Nam giai đoạn  
2023 – 2028" 168/QĐ- EVN ngày 23/02/2023

Quy định công tác văn phòng  
1080/QĐ-EVN ngày 01/08/2021

Hướng dẫn thực hiện bảo vệ dữ liệu cá nhân trong Tập  
đoàn Điện lực Quốc gia Việt Nam 654/QĐ-EVN ngày  
28/06/2024



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# QUY ĐỊNH QUẢN LÝ NỘI BỘ EVNICT VỀ AN TOÀN THÔNG TIN

1

Quy định quản lý an toàn thông tin trong EVNICT  
16/QĐ-EVNICT ngày 16/01/2024

Quy định công tác điều hành, vận hành hệ thống  
thông tin trong EVNICT 47/QĐ-EVNICT ngày  
06/02/2023

Quyết định Chính sách và biện pháp kiểm soát  
ATTT trong EVNICT 167/QĐ-EVNICT ngày  
10/5/2024

Quy định hoạt động ứng cứu sự cố an toàn  
thông tin mạng tại EVNICT 101/QĐ-EVNICT ngày  
21/03/2024

Quy trình Bảo vệ bí mật nhà nước tại Công ty  
561/QĐ-EVNICT ngày 14/09/2023

Hướng dẫn nội bộ công tác lập, thẩm định, phê  
duyệt hồ sơ đề xuất cấp độ tại EVNICT 260/QĐ-  
EVNICT ngày 9/5/2023

Hướng dẫn công tác đảm bảo an toàn thông tin  
cho các hoạt động phát triển, triển khai phần  
mềm 23/QĐ-TTPM ngày 6/9/2023

Quy định vận hành giám sát, xử lý ATTT  
theo mô hình SOC 06/QĐ - EVNICT ngày 06/01/2023



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# Quy định Đảm bảo An toàn thông tin trong EVN (QĐ số 99/QĐ-EVN)

1

- Là đơn vị chuyên trách về ATTT của EVN tại Công ty mẹ - Tập đoàn Điện lực Việt Nam.
- Xây dựng giải pháp đảm bảo an toàn, an ninh thông tin cho các hoạt động ứng dụng công nghệ thông tin của Tập đoàn trình Tập đoàn phê duyệt.
- Thực hiện các biện pháp kiểm soát, phòng ngừa, ngăn chặn các loại tội phạm lợi dụng HTTT gây hại đến an toàn, an ninh thông tin trong hoạt động của Công ty mẹ - Tập đoàn Điện lực Việt Nam.
- Phối hợp với các cơ quan chức năng trong việc trao đổi các biện pháp kỹ thuật, kiểm tra, đánh giá nhằm đảm bảo an toàn, an ninh thông tin.

## Trách nhiệm của EVNICT (Điều 9)

- Chịu trách nhiệm điều tra và xác định các trường hợp vi phạm an toàn, an ninh thông tin đối với các HTTT bao gồm cả hệ thống IT và hệ thống OT tại cơ quan Tập đoàn và các HTTT của các đơn vị trực thuộc EVN.
- Bảo đảm an toàn, an ninh thông tin cho hạ tầng kỹ thuật công nghệ thông tin và các HTTT, cơ sở dữ liệu dùng chung của Tập đoàn.
- Cập nhật các nguy cơ gây mất an toàn, an ninh thông tin đối với các HTTT nói chung và thông báo cho các đơn vị trong Tập đoàn biết để có biện pháp phòng ngừa, ngăn chặn, xử lý kịp thời.
- Là đầu mối để tiếp nhận, phối hợp, hỗ trợ các đơn vị trong Tập đoàn giải quyết các sự cố mất an toàn, an ninh thông tin vượt quá khả năng của đơn vị.
- Tùy theo mức độ sự cố, phối hợp với các đơn vị chức năng có liên quan hướng dẫn xử lý, ứng cứu các sự cố mất an toàn, an ninh thông tin.
- Tổ chức, xây dựng và duy trì lực lượng phản ứng khẩn cấp và ứng cứu nhanh để ứng phó với mọi tình huống sự cố mất an toàn, an ninh thông tin có thể xảy ra tại cơ quan Tập đoàn.
- Rà soát việc tuân thủ quy trình quy định; Rà soát kỹ thuật; hỗ trợ các đơn vị trong công tác đảm bảo ATTT (phê duyệt cấp độ, rà soát thiết kế hệ thống, rà soát kỹ thuật các hệ thống hạ tầng, phần mềm, công thông tin...). Rà soát và đánh giá các quy trình quy định về ATTT để cập nhật, hiệu chỉnh phù hợp với các yêu cầu quản lý, điều hành, sản xuất và phù hợp với các quy định của pháp luật hiện hành.



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# Quy định Đảm bảo An toàn thông tin trong EVN (QĐ số 99/QĐ-EVN)

1

## Đào tạo, tuyên truyền, phổ biến nâng cao nhận thức về ATTT (Điều 14)

1. Trình Tập đoàn phê duyệt chương trình kế hoạch đào tạo hàng năm, trung hạn và dài hạn về ATTT của đơn vị.

2. Kế hoạch đào tạo nguồn nhân lực ATTT bao gồm: định hướng, mục tiêu và các tiêu chuẩn đầu vào cho nhân lực, phương án rà soát đánh giá sau đào tạo.

Kết thúc đào tạo phải có công tác rà soát đánh giá hiệu quả của việc sử dụng nguồn nhân lực ATTT đã được đào tạo, quản lý được trình độ, chứng chỉ và lộ trình phát triển của từng cán bộ làm công tác ATTT.

3. Các đối tượng cần thực hiện đào tạo về ATTT:

a) CBCNV/Người dùng tại đơn vị thực hiện đào tạo cơ bản về ATTT.

b) Cán bộ quản lý: đào tạo nhận thức, định hướng, chiến lược và quản lý về ATTT.

c) Cán bộ công nghệ thông tin: thực hiện đào tạo nâng cao kiến thức và kỹ năng gồm các kiến thức cơ bản đảm bảo xây dựng, phát triển và vận hành an toàn cho các HTTT, các chương trình chuyên đề.

d) Cán bộ chuyên trách công tác ATTT: thực hiện đào tạo nâng cao gồm các kiến thức chuyên đề, các chứng chỉ chuyên môn, các chương trình tập huấn.

4. Thường xuyên công tác tuyên truyền, phổ biến nâng cao nhận thức cho người dùng tại đơn vị về bảo đảm ATTT: phát hành sổ tay ATTT, bảng tin, hội thảo...

5. Bộ phận chuyên trách về ATTT của chủ quản HTTT có trách nhiệm xây dựng kế hoạch tuyên truyền, phổ biến nâng cao nhận thức về ATTT, trình chủ quản HTTT phê duyệt và thực hiện các nội dung theo kế hoạch đã được phê duyệt



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# Quy định Đảm bảo An toàn thông tin trong EVN (QĐ số 99/QĐ-EVN)

1

## Công tác tổ chức và nhân sự

- Người đứng đầu đơn vị chịu trách nhiệm trực tiếp về ATTT; Người đứng đầu hoặc cấp phó được ủy quyền có trách nhiệm phụ trách công tác ATTT, trực tiếp chỉ đạo công tác: xây dựng chiến lược, kế hoạch, ứng cứu sự cố ATTT tại đơn vị
- Tổ chức nguồn lực đảm bảo tách biệt nhân sự thực hiện nhiệm vụ đảm bảo ATTT với nhiệm vụ quản trị và vận hành các HTTT. Cán bộ chuyên trách/phụ trách ATTT không thực hiện nhiệm vụ quản trị vận hành HTTT và ngược lại

- Xây dựng yêu cầu, trách nhiệm bảo đảm an toàn, an ninh thông tin đối với từng vị trí chức danh công việc và phổ biến đến toàn thể CBCNV;
- Trong Quyết định giao nhiệm vụ hoặc Hợp đồng lao động phải có các điều khoản về trách nhiệm đảm bảo an toàn, bảo mật thông tin của người được giao nhiệm vụ trong và sau khi làm việc tại đơn vị
- Ký cam kết đảm bảo an toàn thông tin với các đối tác, nhà cung cấp sản phẩm dịch vụ bên ngoài EVN khi thực hiện: xây dựng, phát triển, nâng cấp, bảo trì, lắp mới, kết nối, trao đổi dữ liệu với các HTTT của đơn vị

Khi chấm dứt hợp đồng, bộ phận Tổ chức và nhân sự thực hiện:

- Xác định trách nhiệm của cá nhân khi chấm dứt hoặc thay đổi công việc.
- Yêu cầu cá nhân bàn giao và lập biên bản bàn giao tài sản CNTT.
- Thu hồi ngay quyền truy cập HTTT của cá nhân nghỉ việc.
- Thay đổi kịp thời quyền truy cập HTTT của cá nhân thay đổi công việc bảo đảm nguyên tắc quyền vừa đủ để thực hiện nhiệm vụ được giao.
- Rà soát, kiểm tra đối chiếu định kỳ tối thiểu ba (03) tháng một lần giữa bộ phận quản lý nhân sự và bộ phận quản lý cấp phát, thu hồi quyền truy cập HTTT nhằm bảo đảm tuân thủ Khoản 3, Khoản 4 Điều này.
- Thông báo đến tất cả các đơn vị trong toàn EVN các trường hợp cá nhân tại đơn vị bị kỷ luật hoặc bị truy cứu trách nhiệm hình sự do vi phạm các quy định về ATTT.



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

1

# Quy định Đảm bảo An toàn thông tin trong EVN (QĐ số 99/QĐ-EVN)

## Bảo đảm ATTT trong hoạt động kết nối, trao đổi thông tin với các hệ thống của tổ chức, cá nhân bên ngoài Tập đoàn (Điều 22)

- Đối với cơ quan, tổ chức, cá nhân ngoài EVN có **kết nối vào hệ thống mạng** của EVN:
  - Vùng mạng của tổ chức, cá nhân bên ngoài được sử dụng để kết nối vào hệ thống mạng của EVN phải được kiểm soát bằng tường lửa;
  - Các máy tính trong vùng mạng này phải được cập nhật bản vá hệ điều hành, phần mềm phòng chống mã độc;
  - Các tài khoản truy cập hệ thống phải áp dụng quy tắc đặt mật khẩu phức tạp (từ 10 ký tự trở lên, bao gồm chữ thường, chữ hoa, số và ký tự đặc biệt trong mật khẩu) và phải thay đổi sau mỗi 3 tháng;
  - Chỉ được kết nối Internet trong trường hợp kết nối này phục vụ trực tiếp công việc của các đơn vị thuộc EVN và đáp ứng quy định về bảo đảm an toàn kết nối Internet tại đơn vị

- Đối tác phát triển ứng dụng cho EVN và các Tổng công ty, đơn vị có trách nhiệm: đảm bảo an toàn cho công tác phát triển ứng dụng, bao gồm cả giai đoạn bảo trì, bảo hành ứng dụng; sử dụng máy tính được cập nhật bản vá hệ điều hành, phần mềm phòng diệt mã độc; thực hiện các biện pháp tránh lộ lọt mã nguồn, phần mềm ứng dụng của EVN và các tài liệu liên quan; không sử dụng các công cụ phát triển ứng dụng không có bản quyền hoặc có nguồn gốc không an toàn; ký cam kết ràng buộc trách nhiệm đảm bảo bí mật và ATTT với đội ngũ nhân sự tham gia phát triển ứng dụng
- Các đối tác cung cấp dịch vụ công nghệ thông tin (bao gồm thử nghiệm sản phẩm công nghệ thông tin tại hệ thống mạng của đơn vị thuộc EVN) và nhân viên của đối tác trong trường hợp tiếp xúc với bí mật nhà nước của EVN phải ký cam kết bảo vệ bí mật nhà nước trước khi triển khai hợp đồng, thỏa thuận về dịch vụ công nghệ thông tin
- Hợp đồng với đối tác có kết nối, trao đổi thông tin với các HTTT, cung cấp triển khai các ứng dụng cho Tập đoàn phải bao gồm các điều khoản và nghĩa vụ về ATTT, cam kết không tiết lộ thông tin, trách nhiệm xử lý, vá lỗi hỏng phần mềm, điều khoản xử phạt trong trường hợp đối tác vi phạm quy định an toàn, bảo mật thông tin và trách nhiệm phải bồi thường thiệt hại do đối tác gây ra, áp dụng cho cả cá nhân, tổ chức liên quan của đối tác bao gồm nhân viên của đối tác và các nhà thầu phụ của đối tác trong trường hợp đối tác ký kết hợp đồng với nhà thầu phụ.
- Đơn vị đầu mối làm việc với đối tác phải lập hồ sơ nhật ký giám sát dịch vụ, kết nối của đối tác cung cấp



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# Quy định Đảm bảo An toàn thông tin trong EVN (QĐ số 99/QĐ-EVN)

1

## Quản lý thông tin, dữ liệu và thiết bị lưu trữ, xử lý (Điều 15, 16)

1. Giao, gắn trách nhiệm cụ thể cho cá nhân hoặc tập thể tiếp cận, quản lý, sử dụng tài sản, trang thiết bị công nghệ thông tin.
2. Trang thiết bị công nghệ thông tin được cấp phát nếu có lưu trữ dữ liệu bí mật, 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. Trường hợp không thể tiêu hủy được dữ liệu, đơn vị phải thực hiện tiêu hủy cấu phần lưu trữ dữ liệu trên trang thiết bị công nghệ thông tin đó.
3. Các thông tin thuộc loại thông tin bí mật phải được mã hóa hoặc có biện pháp bảo vệ để bảo mật thông tin trong quá trình tạo lập, trao đổi, lưu trữ.
4. Thiết bị công nghệ thông tin có bộ phận lưu trữ dữ liệu hoặc thiết bị lưu trữ dữ liệu khi mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài hoặc ngừng sử dụng phải tháo bộ phận lưu trữ khỏi thiết bị hoặc xóa thông tin, dữ liệu lưu trữ trên thiết bị (trừ trường hợp để khôi phục dữ liệu).
5. Đảm bảo các trang thiết bị điện tử có kết nối Internet trên hệ thống phải được thiết lập cấu hình phù hợp, không sử dụng cấu hình mặc định của nhà sản xuất.
6. Phải có biện pháp kiểm tra đảm bảo an toàn, an ninh thông tin đối với thiết bị di động và thiết bị lưu trữ di động trước khi sử dụng với các HTTT.
7. Thiết bị di động và thiết bị lưu trữ di động khi mang vào/ra từ đơn vị sử dụng phải được phép của đơn vị vận hành HTTT. Thiết bị di động phải có đăng ký địa chỉ MAC trước khi được sử dụng trong HTTT Cấp độ 3 trở lên.
8. Thiết bị CNTT có chứa dữ liệu (máy tính, thiết bị lưu trữ, ...) khi bị hỏng phải được cán bộ chuyên trách về công nghệ thông tin 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.
9. 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.
10. Đối với các trang thiết bị công nghệ thông tin được cấp phát, khi thực hiện chuyển đổi sang sử dụng các trang thiết bị công nghệ thông tin mới, phải tự thực hiện hoặc nhờ sự trợ giúp từ đơn vị hỗ trợ người dùng để hủy dữ liệu ở trang thiết bị cũ, đảm bảo không thể khôi phục lại. Sau khi thực hiện xong phải có xác nhận của cán bộ phụ trách ATTT của đơn vị.



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# Quy định Đảm bảo An toàn thông tin trong EVN (QĐ số 99/QĐ-EVN)

1

## Bảo đảm ATTT đối với hệ thống mạng máy tính và Internet

1. Hệ thống mạng nội bộ (LAN) phải được thiết kế phân vùng theo chức năng cơ bản (theo các chính sách ATTT riêng), bao gồm nhưng không giới hạn: vùng mạng người dùng; vùng mạng kết nối hệ thống ra bên ngoài Internet và các mạng khác; vùng mạng máy chủ công cộng; vùng mạng máy chủ nội bộ; vùng mạng máy chủ quản trị. Dữ liệu trao đổi giữa các vùng mạng phải được quản lý, giám sát bởi hệ thống các thiết bị mạng, thiết bị bảo mật.
2. Áp dụng các biện pháp kỹ thuật cần thiết bảo đảm ATTT trong hoạt động kết nối Internet, tối thiểu đáp ứng các yêu cầu sau: có hệ thống tường lửa và hệ thống bảo vệ truy nhập Internet, đáp ứng nhu cầu kết nối đồng thời, hỗ trợ các công nghệ mạng riêng ảo thông dụng(VPN) và có phần cứng mã hóa tích hợp để tăng tốc độ mã hóa dữ liệu và có khả năng bảo vệ hệ thống trước các loại tấn công từ chối dịch vụ (DDoS); Lọc bỏ, không cho phép truy nhập các trang tin có nghi ngờ chứa mã độc hoặc các nội dung không phù hợp
3. Cách ly kết nối mạng (LAN/WAN/Internet) cho các trường hợp sau:
  - Đảm bảo không kết nối mạng đối với máy tính sử dụng để đọc, soạn thảo, lưu trữ, in ấn văn bản thuộc bí mật Nhà nước;
  - Đảm bảo cách ly Internet đối với toàn bộ các máy chủ, máy tính quản trị của các HTTT (trừ các máy chủ web, máy chủ của các dịch vụ phải công khai trên Internet, các máy phục vụ cập nhật bản vá hệ điều hành, máy phục vụ cập nhật dữ liệu nhận dạng mã độc, điểm yếu, virus, mẫu tấn công);
  - Đảm bảo cách ly Internet đối với các máy tính người sử dụng của các hệ thống công nghệ thông tin quan trọng của Tập đoàn bao gồm: Hệ thống quản lý khách hàng dùng điện CMIS; Hệ thống quản lý nguồn lực doanh nghiệp ERP; Hệ thống thu thập và xử lý dữ liệu công tơ điện tử EVNHES, MDMS.



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# Quy định Đảm bảo An toàn thông tin trong EVN (QĐ số 99/QĐ-EVN)

1

- Cá nhân sử dụng HTTT được cấp và sử dụng tài khoản truy nhập với định danh duy nhất gắn với cá nhân đó
- Trường hợp cá nhân thay đổi vị trí công tác, chuyển công tác, thôi việc hoặc nghỉ hưu, trong vòng không quá 05 ngày làm việc sau khi có quyết định của cấp có thẩm quyền thì đơn vị quản lý cá nhân đó phải thực hiện điều chỉnh, thu hồi, hủy bỏ các quyền sử dụng đối với hệ thống hoặc thông báo cho đơn vị vận hành các hệ thống thực hiện
- Tất cả máy chủ, máy trạm và máy người dùng phải được đặt mật khẩu truy cập. Người sử dụng phải đăng xuất khỏi tài khoản đã truy cập hoặc khóa màn hình làm việc trước khi rời khỏi máy tính. Thiết lập chế độ màn hình chờ có mật khẩu bảo vệ sau 10 phút không sử dụng máy tính

## Quản lý tài khoản truy cập hệ thống

- Tài khoản quản trị hệ thống (mạng, hệ điều hành, thiết bị kết nối mạng, phần mềm, ứng dụng, cơ sở dữ liệu...) phải tách biệt với tài khoản truy nhập của người sử dụng thông thường. Tài khoản hệ thống phải được giao dịch danh cá nhân làm công tác quản trị. Hạn chế tối đa dùng chung tài khoản quản trị
- Các đơn vị phải trang bị giải pháp quản lý tài khoản quản trị HTTT và phân công cán bộ chuyên trách công nghệ thông tin chịu trách nhiệm giữ và bảo mật tài khoản quản trị HTTT. Các đơn vị phải có biện pháp quản lý tài khoản quản trị HTTT đảm bảo an toàn, an ninh thông tin và truy cứu được trách nhiệm khi xảy ra sự cố bắt nguồn từ việc sử dụng tài khoản quản trị
- Hệ thống tài khoản phải được rà soát hàng năm, đảm bảo các tài khoản và quyền truy cập hệ thống được cấp phát đúng. Các tài khoản không sử dụng/truy cập trong thời gian 06 tháng phải bị khóa hoặc xóa bỏ (sau khi có thông báo với đơn vị/người sử dụng).
- Vô hiệu hóa các chức năng truy cập từ xa không an toàn đối với HTTT từ Cấp độ 3 trở lên. Khi có nhu cầu truy cập từ xa các hệ thống này phải có biện pháp kết nối an toàn (SSH, TLS/SSL) được phê duyệt bởi chủ quản HTTT, đồng thời kiểm soát chặt chẽ trong suốt quá trình thực hiện và vô hiệu hóa trở lại chức năng truy cập từ xa hệ thống sau khi kết thúc công việc



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# Quy định Đảm bảo An toàn thông tin trong EVN (QĐ số 99/QĐ-EVN)

1

## Bảo đảm ATTT mức ứng dụng

1. Yêu cầu về bảo đảm ATTT phải được đưa vào tất cả các công đoạn thiết kế, xây dựng, kiểm thử, triển khai và vận hành sử dụng phần mềm. Đồng thời phải có biên bản đánh giá ATTT sau khi kết thúc mỗi công đoạn này.
2. Phần mềm/ứng dụng phải đáp ứng các yêu cầu sau: cấu hình xác thực người sử dụng; giới hạn số lần đăng nhập sai liên tiếp; giới hạn thời gian để chờ đóng phiên kết nối; sử dụng các phương pháp mã hóa thông dụng để mã hóa thông tin xác thực khi sử dụng trên hệ thống hoặc truyền qua mạng; không khuyến khích việc đăng nhập tự động.
3. Thiết lập, phân quyền truy nhập, quản trị, sử dụng tài nguyên khác nhau của phần mềm, ứng dụng với người sử dụng/nhóm người sử dụng có chức năng, yêu cầu nghiệp vụ khác nhau; tách biệt cổng giao tiếp quản trị phần mềm ứng dụng với cổng giao tiếp cung cấp dịch vụ; đóng các cổng giao tiếp không sử dụng.
4. Chỉ cho phép sử dụng các giao thức mạng có hỗ trợ chức năng mã hóa thông tin như SSH, SSL, VPN hoặc tương đương khi truy nhập, quản trị phần mềm, ứng dụng từ xa trên môi trường mạng; hạn chế truy cập đến mã nguồn của phần mềm, ứng dụng và phải đặt mã nguồn trong môi trường an toàn do bộ phận chuyên trách công nghệ thông tin quản lý.
5. Ghi và lưu giữ bản ghi nhật ký hệ thống của phần mềm, ứng dụng trong khoảng thời gian tối thiểu 03 tháng với những thông tin cơ bản: thời gian, địa chỉ, tài khoản (nếu có), nội dung truy nhập và sử dụng phần mềm, ứng dụng; các lỗi phát sinh trong quá trình hoạt động; thông tin đăng nhập khi quản trị.
6. Phần mềm, ứng dụng cần được kiểm tra phát hiện và khắc phục các điểm yếu về an toàn, an ninh thông tin trước khi đưa vào sử dụng và trong quá trình sử dụng.
7. Thực hiện quy trình kiểm soát cài đặt, cập nhật, vá lỗi bảo mật phần mềm, ứng dụng trên các máy chủ, máy tính cá nhân, thiết bị kết nối mạng đang hoạt động thuộc hệ thống mạng nội bộ.



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# Quy định Đảm bảo An toàn thông tin trong EVN (QĐ số 99/QĐ-EVN)

1

- Phải thực hiện bảo vệ thông tin, dữ liệu, thông tin có nội dung quan trọng, nhạy cảm hoặc không phải là thông tin công khai bằng các biện pháp như: thiết lập phương án bảo đảm tính bí mật, nguyên vẹn và khả dụng của thông tin, dữ liệu; mã hóa thông tin, dữ liệu khi lưu trữ trên hệ thống/thiết bị lưu trữ dữ liệu di động; sử dụng chữ ký số để xác thực và bảo mật thông tin, dữ liệu.
- Phải triển khai hệ thống/phương tiện lưu trữ độc lập với hệ thống lưu trữ trên các máy chủ dịch vụ để sao lưu dự phòng; phân loại và quản lý thông tin, dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau; thực hiện sao lưu dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

## Bảo đảm ATTT mức dữ liệu

- Phải bố trí máy tính riêng không kết nối mạng, đặt mật khẩu, mã hóa dữ liệu và các biện pháp bảo mật khác bảo đảm ATTT để soạn thảo, lưu trữ dữ liệu, thông tin và tài liệu quan trọng ở các mức độ mật, tuyệt mật, tối mật.
- Các HTTT của đơn vị phải có cơ chế sao lưu dữ liệu dự phòng. Các dữ liệu quan trọng phải được sao lưu, bao gồm: hệ điều hành, thông tin cấu hình hệ thống (mạng, máy chủ), phần mềm ứng dụng, cơ sở dữ liệu, dữ liệu và tập tin ghi nhật ký.
- Giải pháp sao lưu của các đơn vị phải đảm bảo khả năng phục hồi dữ liệu và khôi phục hoạt động của hệ thống khi có sự cố xảy ra. Thời gian khôi phục hệ thống phải trong giới hạn cho phép của đơn vị nhằm hạn chế tối đa ảnh hưởng của sự cố đến hoạt động của đơn vị.
- Dữ liệu sao lưu phải được lưu trữ an toàn và được kiểm tra thường xuyên đảm bảo khả năng sẵn sàng cho việc sử dụng khi cần. Kiểm tra khả năng phục hồi hệ thống thành công từ dữ liệu sao lưu tối thiểu 3 tháng một lần



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# Quy định Đảm bảo An toàn thông tin trong EVN (QĐ số 99/QĐ-EVN)

2

## Bảo đảm ATTT khi tiếp nhận, phát triển, vận hành, bảo trì HTTT

1. Khi thực hiện nâng cấp, mở rộng, thay thế một phần HTTT, phải rà soát cấp độ, phương án bảo đảm an toàn của HTTT và thực hiện điều chỉnh, bổ sung hoặc thay mới hồ sơ đề xuất cấp độ trong trường hợp cần thiết.
2. Khi tiếp nhận, phát triển, nâng cấp, bảo trì HTTT, đơn vị phải tiến hành phân tích, xác định rủi ro có thể xảy ra, đánh giá phạm vi tác động và phải chuẩn bị các biện pháp hạn chế, loại trừ các rủi ro này và yêu cầu các bên cung cấp, thi công, các cá nhân liên quan thực hiện.
3. Trong quá trình vận hành HTTT, đơn vị chủ quản HTTT cần thực hiện đánh giá, phân loại HTTT theo cấp độ; triển khai phương án bảo đảm an toàn HTTT đáp ứng yêu cầu cơ bản trong tiêu chuẩn, quy chuẩn kỹ thuật về bảo đảm an toàn HTTT theo cấp độ; thường xuyên kiểm tra, giám sát an toàn HTTT; tuân thủ quy trình vận hành, quy trình xử lý sự cố đã xây dựng; ghi lại và lưu trữ đầy đủ thông tin nhật ký hệ thống để phục vụ quản lý, kiểm soát thông tin.



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# Quy định quản lý, khai thác Hệ thống thông tin

## 1268/QĐ-EVN

1

### Trách nhiệm và quyền hạn của EVNICT

1. Quyền quản lý tài sản, vận hành các thiết bị thuộc HTTT do HĐTV EVN giao bao gồm:
  - a) Quản lý tài sản và vận hành thiết bị, vật tư VT
  - b) Quản lý tài sản và vận hành hệ thống CNTT dùng chung trong EVN; quản lý vận hành thiết bị CNTT trang bị đồng bộ với công trình xây dựng tòa nhà EVN, 11 Cửa Bắc, Hà Nội
2. EVNICT đại diện EVN tổ chức hệ thống giám sát thiết bị VT, CNTT, dữ liệu hệ thống cáp quang của các đơn vị thành viên trong EVN; thực hiện quyền điều khiển đối với các thiết bị VT của các TCT (theo quy định tại điểm b khoản 3 Điều 14) phù hợp với quy định của pháp luật, nhằm mục đích thu thập, đánh giá và sử dụng hiệu quả tài nguyên VT và CNTT trong EVN phục vụ việc thiết lập kênh, tối ưu hóa, xử lý sự cố hệ thống
3. EVNICT có trách nhiệm đề xuất EVN để xây dựng và ban hành các quy định/quy trình quản lý HTTT để áp dụng trong Tập đoàn Điện lực Quốc gia Việt Nam.
4. EVNICT là đơn vị chuyên trách về an toàn thông tin của EVN tại Công ty mẹ - Tập đoàn Điện lực Việt Nam
5. Công tác cập nhật tiêu chuẩn kỹ thuật/công nghệ
6. Công tác kết nối, tích hợp hệ thống: Chủ trì việc kết nối, tích hợp hệ thống phục vụ công tác điều hành hệ thống điện, sản xuất - kinh doanh điện năng
7. Công tác tối ưu hóa hệ thống:
8. Công tác xây dựng cập nhật dữ liệu hệ thống
9. Công tác điều hành HTTT
11. Xây dựng, vận hành phần mềm quản lý kỹ thuật, quản lý sự cố VT và CNTT của EVN
12. Khai thác hệ thống
13. Nghiên cứu, phát triển, ứng dụng hệ thống TĐH



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# Quy định quản lý, khai thác Hệ thống thông tin

## 1268/QĐ-EVN

1

### Điều 8. Cơ sở thiết kế hệ thống

- Được đồng bộ thời gian với đồng hồ chủ của trạm/TTĐK và/hoặc đồng hồ chủ của EVN (đồng hồ nguyên tử do EVNICT quản lý vận hành) phù hợp với tham số kỹ thuật và nguyên tắc an ninh bảo mật của từng hệ thống.
- Hệ thống DCS nhà máy được đồng bộ thời gian với đồng hồ chủ của nhà máy và/hoặc đồng hồ chủ của EVN phù hợp với tham số kỹ thuật và nguyên tắc an ninh bảo mật của từng hệ thống.

### Điều 43. Nhiệm vụ quản trị hệ thống CNTT

- Quản trị an toàn thông tin: Thiết lập/thay đổi chính sách Firewall, cấu hình IDS/IPS, quét virus, phát hiện mã độc,...

### Điều 55. Quy định về quản lý tài khoản, mật khẩu truy nhập thiết bị VT, CNTT, TĐH

2. Mật khẩu truy nhập thiết bị phải được đổi định kỳ để thực hiện bảo mật. Tần suất đổi mật khẩu do đơn vị quyết định dựa trên đặc thù của hệ thống thiết bị do đơn vị quản lý trong khoảng thời gian ít nhất 03 tháng một lần.
- b) Giữ gìn, bảo mật tài khoản; nghiêm cấm chia sẻ, cho người khác sử dụng khi chưa được phép của cấp có thẩm quyền;

### Điều 51. Kết nối hệ thống CNTT, TĐH

- b) Kết nối phục vụ công tác điều hành sản xuất kinh doanh điện năng: Để phục vụ mục đích sản xuất kinh doanh điện năng của đơn vị, TCTĐL có thể cho phép các đối tác kết nối vào hệ thống CNTT của mình trên cơ sở đảm bảo các nguyên tắc:
  - Sử dụng kết nối đúng mục đích thỏa thuận;
  - Đảm bảo an toàn thông tin.



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# Quy định quản lý, khai thác Hệ thống thông tin

## 1268/QĐ-EVN

1

### Quy định công tác xử lý sự cố hệ thống công nghệ thông tin, tự động hóa

#### Điều 45. Sự cố CNTT/TĐH nghiêm trọng

2. Yêu cầu thời gian xử lý sự cố đối với sự cố nghiêm trọng: Không quá 04 giờ tính từ thời điểm phát hiện sự cố (thời gian xử lý sự cố CNTT có thể được thay đổi theo yêu cầu của EVN dựa trên thực tế vận hành hệ thống)

#### Điều 46. Sự cố CNTT/TĐH nặng

2. Yêu cầu thời gian xử lý sự cố đối với sự cố CNTT nặng: Không quá 06 giờ tính từ thời điểm phát hiện sự cố (thời gian xử lý sự cố CNTT có thể được thay đổi theo yêu cầu của EVN dựa trên thực tế vận hành hệ thống).

#### Điều 47. Sự cố CNTT/TĐH nhẹ

2. Yêu cầu thời gian xử lý sự cố đối với sự cố CNTT nhẹ: Không quá 48 giờ tính từ thời điểm phát hiện sự cố (thời gian xử lý sự cố CNTT có thể được thay đổi theo yêu cầu của EVN dựa trên thực tế vận hành hệ thống).

### Quy định về xử lý sự cố hệ thống viễn thông

#### Điều 37. Sự cố VT nghiêm trọng

+ Chậm nhất 15 phút kể từ khi sự cố xảy ra phải báo cáo sơ bộ cho EVN về nguyên nhân và phạm vi ảnh hưởng.  
+ Thời gian xử lý sự cố VT nghiêm trọng:  
Với kênh truyền Rơ le bảo vệ: Không quá 04 giờ  
Với các kênh dịch vụ khác: Không quá 04 giờ

#### Điều 38. Sự cố VT nặng

b) Thời gian xử lý sự cố nặng:  
- Với kênh truyền Rơ le bảo vệ: Không quá 06 giờ  
- Với các kênh dịch vụ khác: Không quá 06 giờ

#### Điều 39. Sự cố VT nhẹ

b) Thời gian xử lý sự cố nhẹ: Không quá 48 giờ kể từ khi xảy ra sự cố. Thời gian đội xử lý sự cố di chuyển đến hiện trường được giảm trừ 01 giờ/40 km.



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# Quy định công tác văn phòng

## 1080/QĐ-EVN

1

### Quy định về quản lý văn bản trên hệ thống văn phòng số trong EVN

#### Điều 20. Các hành vi bị cấm

- Cho người khác sử dụng tài khoản và mật khẩu của mình.
- Phát tán thư rác và virus vào hệ thống văn phòng số.
- Cản trở hoặc ngăn chặn trái phép quá trình truyền, gửi và nhận văn bản trên hệ thống văn phòng số.
- Thay đổi, xóa, hủy, sao chụp, tiết lộ, di chuyển trái phép một phần hoặc toàn bộ nội dung của văn bản trên hệ thống văn phòng số.
- Các hành vi bị cấm khác theo quy định của pháp luật và quy định của EVN.

#### Điều 21. Trách nhiệm của CBCNV sử dụng Hệ thống văn phòng số

- Sử dụng Hệ thống văn phòng số theo tài khoản được cấp để thực hiện chức năng, nhiệm vụ được phân công theo quy định.
- Thực hiện trình tự xử lý công việc theo đúng quy trình nghiệp vụ.
- Lập hồ sơ công việc trên hệ thống văn phòng số đúng quy định.
- Bảo mật tài khoản được cấp, trường hợp bị mất mật mã tài khoản phải báo ngay cho lãnh đạo Ban/Văn phòng/Phòng và cán bộ chuyên trách CNTT của cơ quan để khắc phục kịp thời.
- Người được cấp chứng thư số phải đảm bảo bảo mật chứng thư số đã được cấp và bàn giao lại cho cơ quan khi chuyển công tác, nghỉ việc.

#### Điều 22. Chữ ký số của người có thẩm quyền ký ban hành văn bản

- Văn phòng EVN/Đơn vị là đầu mối quản lý chữ ký mẫu, đề xuất xóa hoặc bổ sung chữ ký mẫu vào Hệ thống văn phòng số theo đúng trình tự quy định (việc thay đổi chữ ký mẫu vào Hệ thống văn phòng số phải do người ký có yêu cầu và phải được người có chữ ký duyệt bằng văn bản). Hồ sơ đề nghị cấp chứng thư số và mẫu chữ ký bao gồm: Quyết định bổ nhiệm; giấy đề nghị; chữ ký mẫu; số căn cước công dân, số điện thoại.
- EVNICT/bộ phận Công nghệ thông tin của đơn vị chịu trách nhiệm quản trị Hệ thống văn phòng số, bảo mật an toàn tuyệt đối các chữ ký, thực hiện xóa hoặc bổ sung chữ ký mẫu theo đề nghị bằng văn bản của Văn phòng EVN/Đơn vị.



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# Quy định công tác văn phòng

## 1080/QĐ-EVN

1

### Điều 59. Các quy định có liên quan khác về công tác bảo mật, cam kết bảo vệ bí mật trong Tập đoàn Điện lực Quốc gia Việt Nam

3. CBCNV các đơn vị làm công tác liên quan trực tiếp đến bí mật trong Tập đoàn Điện lực Quốc gia Việt Nam phải cam kết bảo vệ bí mật bằng văn bản (theo mẫu tại phụ lục kèm theo) với Tổng giám đốc EVN/Tổng giám đốc/Giám đốc đơn vị. Văn bản cam kết nộp cho bộ phận bảo mật, tổ chức của đơn vị lưu giữ. Khi nhận công tác hoặc thôi làm công tác bảo mật phải có sự thoả thuận của cơ quan an ninh cùng cấp và làm cam kết bảo vệ bí mật trong Tập đoàn Điện lực Quốc gia Việt Nam. Khi ra nước ngoài phải được cơ quan có thẩm quyền cho phép. Những người được giao làm công việc liên quan đến bí mật trong Tập đoàn Điện lực Quốc gia Việt Nam phải thực hiện nghiêm túc các nội dung tại Quy định này và các quy định pháp luật có liên quan.

5. Trách nhiệm của các đơn vị/cá nhân trong việc sử dụng, quản lý điện mật:

- a) Việc sử dụng điện mật phải được thể hiện theo chế độ tài liệu mật và theo đúng quy định số 06/QĐ-VPTW ngày 01/6/2017 của Văn phòng Ban chấp hành Trung ương, các sửa đổi bổ sung sau này và các quy định hiện hành của EVN. Nội dung điện mật chỉ phổ biến đến người có trách nhiệm, không được tự ý sao chép, lưu trữ phổ biến nguyên văn hoặc chuyển cho nhiều người xem.
- b) Cơ quan/cá nhân khi giải quyết xong điện mật phải trả lại cho cơ yếu của Văn phòng Trung ương Đảng bảo quản. Điện “Tuyệt mật” phải trả lại sau một tuần; điện “Mật”, “Tối mật” phải trả lại sau một tháng. Khi cần giữ điện mật lại để nghiên cứu, phải trao đổi với cơ yếu của Văn phòng Trung ương Đảng về thời gian giữ lại.
- c) Cơ quan hoặc cán bộ làm thất lạc điện mật phải nhanh chóng lập biên bản xác nhận rõ: người làm mất, mất trong trường hợp nào, nội dung điện mật đề cập về vấn đề gì... đồng thời phải báo ngay cho Tổng giám đốc EVN/Tổng giám đốc/Giám đốc đơn vị và phụ trách cơ yếu của Văn phòng Trung ương Đảng biết để có biện pháp xử lý kịp thời.



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# Quy định công tác văn phòng

## 1080/QĐ-EVN

1

### Điều 3. Quy định chung

12. Tất cả lãnh đạo và CBCNV chịu trách nhiệm bảo mật tài khoản sử dụng văn phòng số của cá nhân được cung cấp, chịu trách nhiệm đối với các tác nghiệp bằng tài khoản văn phòng số của cá nhân. Các tác nghiệp trên Hệ thống văn phòng số phải được lưu vết chi tiết toàn bộ quá trình xử lý. CBCNV không được chuyển, gửi cho tổ chức, cá nhân trong và ngoài EVN/đơn vị văn bản, tài liệu, thông tin liên quan đến EVN/Đơn vị trong quá trình giải quyết công việc được giao hoặc không được giao giải quyết công việc nhưng biết được qua bất cứ nguồn thông tin nào mà chưa có sự chấp thuận của lãnh đạo Ban/Văn phòng.

### Điều 45. Bảo quản tài liệu lưu trữ

a) Nguyên tắc: Bảo đảm cơ sở dữ liệu tài liệu lưu trữ được bảo quản toàn vẹn, an toàn, xác thực, bảo mật trên các phương tiện lưu trữ (bao gồm các văn bản, tài liệu hồ sơ điện tử và hồ sơ lưu trữ được số hóa đưa lên Hệ thống văn phòng số). Bảo đảm khả năng truy cập, quản lý, tìm kiếm, cập nhật cơ sở dữ liệu tài liệu lưu trữ.

### Điều 57. Chế độ báo cáo, thống kê về công tác bảo mật

1. Các đơn vị lưu giữ bí mật Nhà nước, EVN phải thống kê tài liệu, vật mang bí mật Nhà nước, bí mật EVN của đơn vị mình theo trình tự thời gian và từng độ mật.
2. Báo cáo đột xuất: đơn vị phải báo cáo kịp thời về EVN/Đơn vị cấp trên những vụ việc lộ, lọt, mất bí mật Nhà nước xảy ra hoặc các hành vi vi phạm pháp luật về bảo vệ bí mật Nhà nước. Trong báo cáo cần nêu rõ lý do, nguyên nhân, các biện pháp đã tiến hành xử lý, kết quả và ý kiến đề xuất.
3. Báo cáo định kỳ: Báo cáo định kỳ là báo cáo toàn diện về công tác bảo vệ bí mật hàng năm và 5 năm của Đơn vị, báo cáo cần ngắn gọn, chính xác, phản ánh đầy đủ tình hình công tác bảo vệ bí mật trong năm và 5 năm.



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# BỘ QUY TẮC CẤU HÌNH AN TOÀN THÔNG TIN

## (QĐ 1290/EVN)

1

### Danh mục quy tắc cấu hình ATTT và phạm vi áp dụng

1. Quy tắc cấu hình ATTT cho hệ điều hành Windows của người dùng cuối
  - Áp dụng cho các máy tính người dùng sử dụng hệ điều hành Windows.
2. Quy tắc cấu hình ATTT cho hệ thống mạng nội bộ
  - Áp dụng cho bộ phận Quản trị hệ thống mạng nội bộ.
3. Quy tắc lập trình an toàn trong phát triển ứng dụng web
  - Áp dụng cho bộ phận Quản trị và phát triển ứng dụng web.
4. Quy tắc lập trình an toàn sử dụng ứng dụng C/C++
  - Áp dụng cho bộ phận Phát triển ứng dụng sử dụng C/C++.
5. Quy tắc lập trình an toàn cho ứng dụng mobile
  - Áp dụng cho bộ phận Phát triển ứng dụng Mobile.
6. Quy tắc cấu hình ATTT cho hệ điều hành máy chủ
  - Áp dụng cho bộ phận Quản trị máy chủ.
7. Quy tắc cấu hình ATTT cho web server
  - Áp dụng cho bộ phận Quản trị hệ thống web server.
8. Quy tắc cấu hình ATTT cho hệ quản trị cơ sở dữ liệu
  - Áp dụng cho bộ phận Quản trị hệ thống cơ sở dữ liệu.
9. Quy tắc cấu hình ATTT cho Email server
  - Áp dụng cho bộ phận Quản trị hệ thống Email.
10. Quy tắc cấu hình ATTT cho hệ thống Active Directory
  - Áp dụng cho bộ phận Quản trị hệ thống Active Directory.
11. Quy tắc cấu hình ATTT cho hệ thống Proxy
  - Áp dụng cho bộ phận Quản trị hệ thống Proxy.
12. Quy tắc cấu hình ATTT cho hệ thống quản lý Antivirus tập trung
  - Áp dụng cho bộ phận Quản trị hệ thống Antivirus.
13. Quy tắc cấu hình ATTT cho hệ thống VPN tập trung
  - Áp dụng cho bộ phận Quản trị hệ thống VPN.
14. Quy tắc cấu hình ATTT cho hệ thống Firewall
  - Áp dụng cho bộ phận Quản trị Firewall.
15. Quy tắc cấu hình ATTT cho thiết bị mạng
  - Áp dụng cho bộ phận Quản trị thiết bị mạng.



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# Hướng dẫn thực hiện bảo vệ dữ liệu cá nhân trong EVN (QĐ số 654/QĐ-EVN)

1

## Các đơn vị trực thuộc EVN là Bên kiểm soát và xử lý dữ liệu cá nhân đối với

- Dữ liệu cá nhân của khách hàng, đối tác phát sinh trong phát sinh trong quá trình làm việc và được đơn vị trực thuộc EVN xử lý.
- Dữ liệu vãng lai được thu thập và xử lý tại các trụ sở làm việc của đơn vị trực thuộc EVN theo từng thời kỳ (không bao gồm dữ liệu vãng lai do đơn vị quản lý tòa nhà thu thập và xử lý)

## Các đơn vị trực thuộc EVN có trách nhiệm

- Tổ chức triển khai và giám sát, kiểm tra việc thực hiện Hướng dẫn này và các quy định của pháp luật về bảo vệ dữ liệu cá nhân tại đơn vị và các đơn vị trực thuộc; tuyên truyền, nâng cao nhận thức của CBCNV thuộc đơn vị và các đối tượng thuộc lĩnh vực được giao quản lý về quy định của pháp luật về bảo vệ dữ liệu cá nhân.
- Báo cáo về bảo vệ dữ liệu cá nhân khi có yêu cầu từ các cơ quan có thẩm quyền và gửi Ban VTCNTT tổng hợp, báo cáo Lãnh đạo Tập đoàn
- Phối hợp với EVN làm việc Bộ Công an, cơ quan nhà nước có thẩm quyền trong bảo vệ dữ liệu cá nhân, cung cấp thông tin phục vụ điều tra, xử lý hành vi vi phạm quy định của pháp luật về bảo vệ dữ liệu cá nhân theo quy chế quản trị của Tập đoàn.
- Đơn vị đóng vai trò Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân thực hiện các trách nhiệm tương ứng quy định tại Nghị định số 13/2023/NĐ-CP và quy định tại Hướng dẫn này



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# Hướng dẫn thực hiện bảo vệ dữ liệu cá nhân trong EVN (QĐ số 654/QĐ-EVN)

1

## TRÁCH NHIỆM BẢO VỆ DỮ LIỆU CÁ NHÂN CỦA EVNICT

Đối với dữ liệu cá nhân được xử lý trên HTTT do EVN là Bên  
Kiểm soát và xử lý dữ liệu cá nhân

- Thay mặt cho EVN, xử lý dữ liệu theo chức năng nhiệm vụ được ghi trong các quy chế của Tập đoàn, các văn bản giao nhiệm vụ cũng như các nội dung được ghi trong hướng dẫn này.
- Phối hợp thực hiện theo yêu cầu của EVN: (i) Tiếp nhận yêu cầu cung cấp dữ liệu cá nhân, theo dõi quá trình, danh sách cung cấp dữ liệu cá nhân theo yêu cầu; (ii) Xóa dữ liệu cá nhân trên các hệ thống thông tin phù hợp với quy định; (iii) Tiến hành lập và lưu giữ Hồ sơ đánh giá tác động xử lý dữ liệu cá nhân
- Thực hiện đầy đủ các biện pháp kỹ thuật bảo vệ dữ liệu cá nhân quy định tại Nghị định 13/2023/NĐ-CP và các văn bản pháp luật khác có liên quan: (i) Thực hiện các biện pháp kỹ thuật cùng các biện pháp an toàn, bảo mật phù hợp để chứng minh các hoạt động xử lý dữ liệu đã được thực hiện theo quy định của pháp luật về bảo vệ dữ liệu cá nhân, rà soát và cập nhật các biện pháp này khi cần thiết; (ii) Ghi lại và lưu trữ nhật ký hệ thống quá trình xử lý dữ liệu cá nhân; (iii) Chịu trách nhiệm trước chủ thể dữ liệu về các thiệt hại do quá trình xử lý dữ liệu cá nhân gây ra.



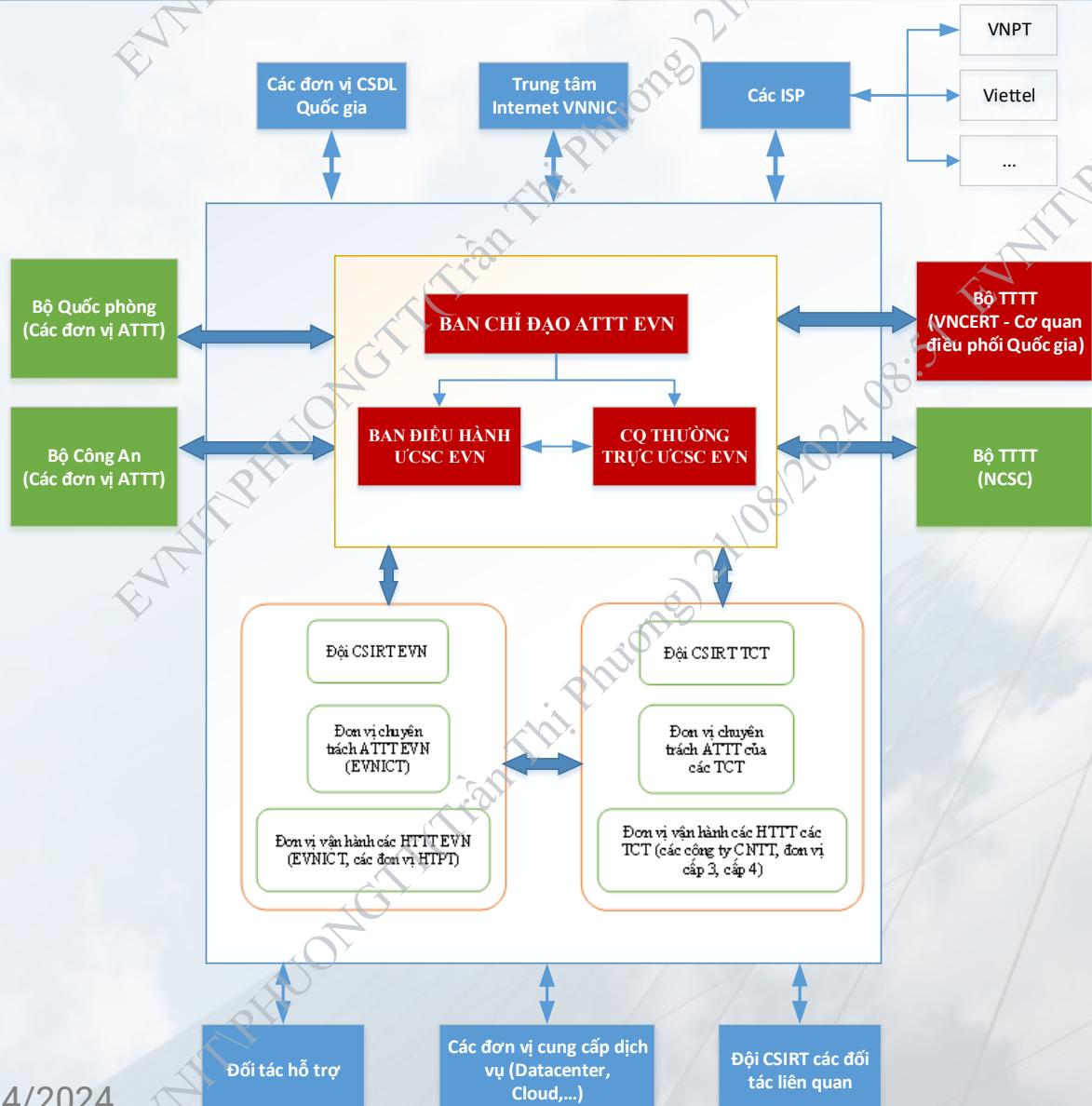
EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# Quy trình UCSC ATTT mạng trong EVN

## (QĐ số 1828/QĐ – EVN)

1



### Điều 8. Mạng lưới ứng cứu sự cố an toàn thông tin mạng của EVN

ĐVCT ATTT của Tập đoàn (EVNICT) và các Tổng công ty, các đơn vị trực thuộc Tập đoàn vận hành HTTT từ cấp độ 3 trở lên có nghĩa vụ, trách nhiệm tham gia vào MLUCSC EVN, chịu sự điều phối và huy động của BĐH UCSC EVN

Danh sách các thành viên MLUCSC EVN được lập theo Mẫu 01 và Mẫu 02 của Phụ lục 03, công bố cho tất cả các thành viên trong MLUCSC EVN biết và được ĐVCT UCSC cập nhật định kỳ mỗi 6 tháng cho các thành viên trong MLUCSC EVN



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# Quy trình UCSC ATTT mạng trong EVN

## (QĐ số 1828/QĐ – EVN)

1

EVNICT phải thành lập Đội CSIRT gồm:

Mẫu 03: Danh sách Đội ứng cứu sự cố (CSIRT)

### 1 Các thành viên chuyên trách ATTT thuộc Đội CSIRT

Bao gồm tối thiểu các vị trí như sau:

- Đội trưởng/Đội phó/Đội phó thường trực.
- Tiếp nhận, phân loại sự cố ATTT.
- Phân tích/giám sát ATTT.
- Ứng cứu sự cố ATTT.
- Đảm bảo ATTT hệ thống cơ sở hạ tầng.
- Điều tra sự cố.

### 2 Các thành viên hỗ trợ:

Bao gồm cán bộ thuộc các phòng/trung tâm/bộ phận làm công tác liên quan đến các HTTT, tùy theo đặc thù của từng đơn vị và cấu trúc của HTTT, bao gồm các vị trí như sau:

- Quản trị cơ sở dữ liệu.
- Quản trị hệ thống cơ sở hạ tầng mạng, máy chủ.
- Quản trị ứng dụng.
- Cung cấp dịch vụ và sửa chữa HTTT.

EVNICT phải lập Danh sách các thành viên MLUCSC EVN:

**ĐVCT UCSC cập nhật định kỳ mỗi 6 tháng** Danh sách các thành viên MLUCSC EVN, được lập theo Mẫu 01 và Mẫu 02 của Phụ lục 03, công bố cho tất cả các thành viên trong MLUCSC EVN biết



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# Quy trình UCSC ATTT mạng trong EVN

## (QĐ số 1828/QĐ – EVN)

1

### EVNICT/ Trung tâm phải xây dựng phương án phòng ngừa, xử lý và ứng cứu sự cố

1. Các **Đơn vị QLVH** hệ thống thông tin, **ĐVCT ATTT** tổ chức xây dựng, phê duyệt kế hoạch ứng cứu xử lý sự cố cho các HTTT do đơn vị trực tiếp quản lý (hoặc được giao quản lý vận hành) theo quy định tại Điều 21, QĐ99. **Mẫu đề cương kế hoạch ứng cứu xử lý sự cố theo Phụ lục II, QĐ05** (bao gồm các điều chỉnh do Bộ TT&TT ban hành nếu có).
2. **ĐVQLVH** chủ trì, **ĐVCT ATTT** và **Đội CSIRT** đơn vị phối hợp: lập mới/cập nhật/hiệu chỉnh phương án phòng ngừa, xử lý và ứng cứu sự cố các HTTT do mình quản lý, trình Chủ quản HTTT xem xét phê duyệt; lập mới/cập nhật/hiệu chỉnh các mô hình/kiến trúc hệ thống mức logic/vật lý, xây dựng, phân loại mức độ quan trọng của dữ liệu để áp dụng các phương án ứng cứu sự cố phù hợp.
3. Phương án phòng ngừa, xử lý và ứng cứu sự cố cần xem xét cập nhật, **hiệu chỉnh tối thiểu mỗi năm một lần** hoặc khi có thay đổi về kiến trúc hệ thống, thực hiện nâng cấp mở rộng, thay đổi hoặc cập nhật cấp độ HTTT, khi phát hiện các nguy cơ mới hoặc khi có yêu cầu của Chủ quản HTTT hoặc theo yêu cầu của BCĐ ATTT EVN.

### EVNICT/ Trung tâm phải lập báo cáo sự cố

Mẫu 01: Báo cáo ban đầu sự cố

Mẫu 02: Báo cáo kết thúc ứng cứu sự cố

Mẫu 03. Báo cáo tổng hợp về hoạt động tiếp nhận và xử lý sự cố



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# PHẦN 2

## HỆ THỐNG QUẢN LÝ AN TOÀN THÔNG TIN: QUẢN LÝ RỦI RO VÀ BIỆN PHÁP KIỂM SOÁT



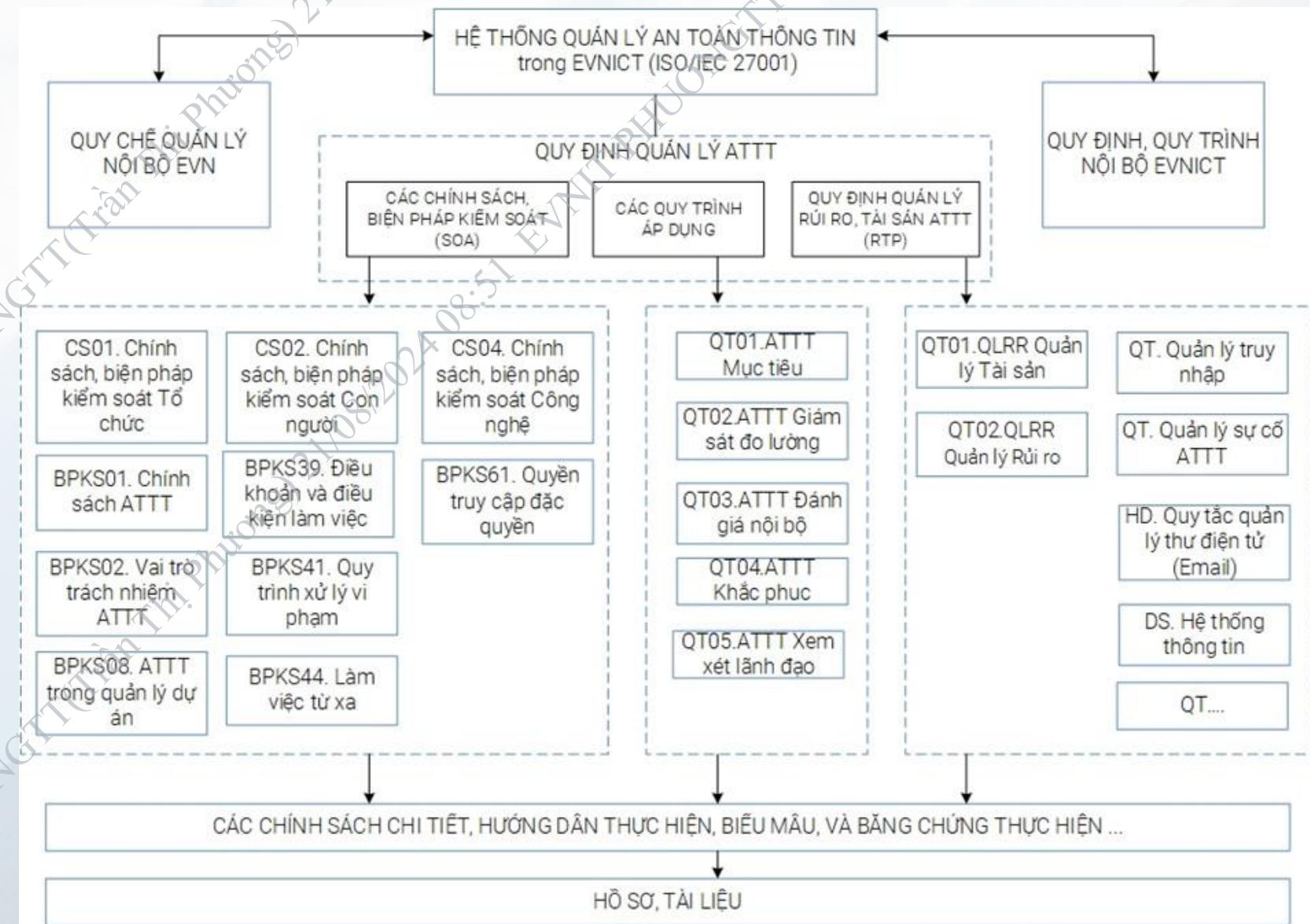
EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# HỆ THỐNG QUẢN LÝ AN TOÀN THÔNG TIN

## (Quy định số 16/QĐ-EVNICT)

2





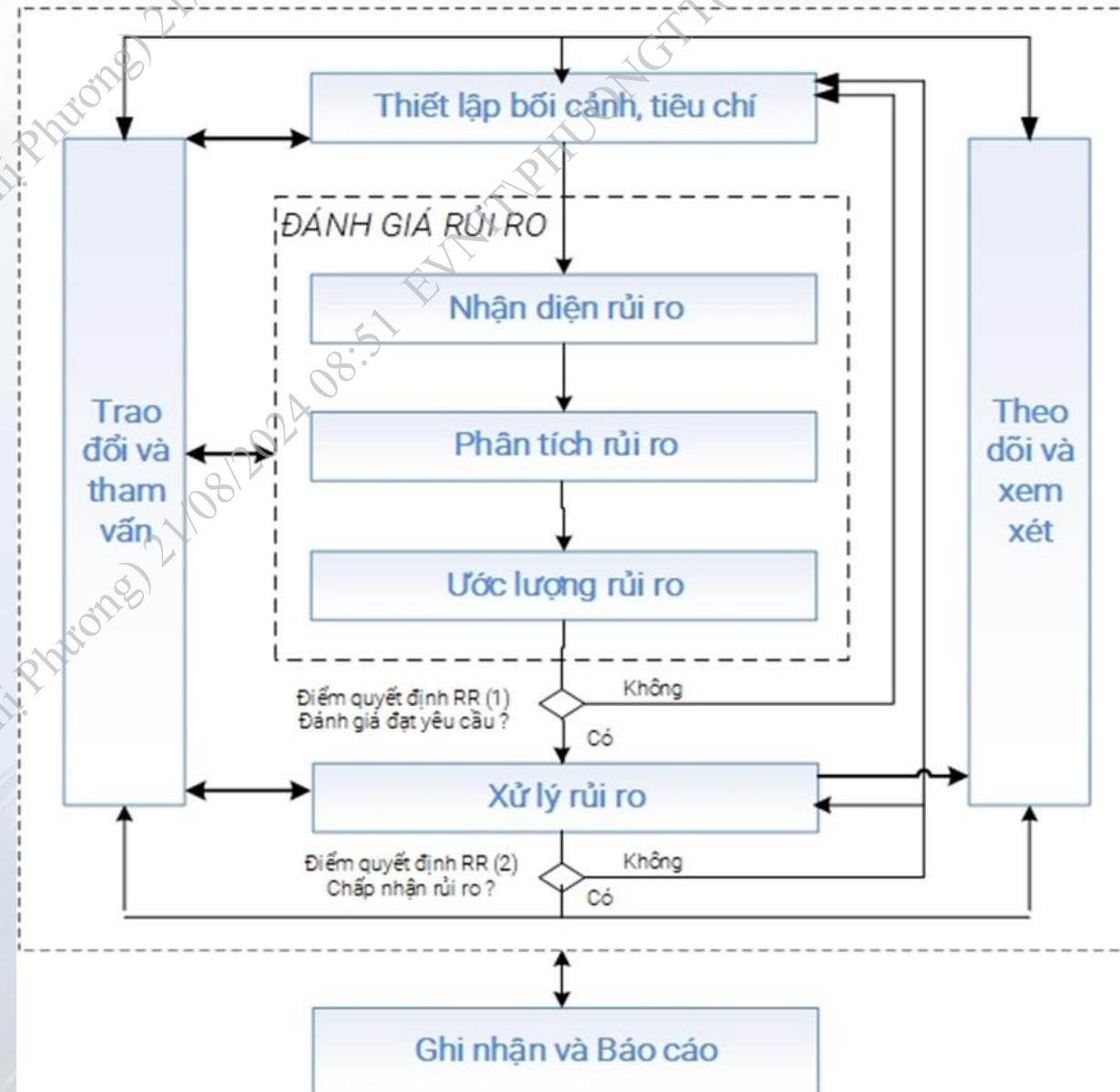
EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# QUẢN LÝ RỦI RO

## (Quy định số 16/QĐ-EVNICT)

2





EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# BIỆN PHÁP KIỂM SOÁT

## (Quy định số 16/QĐ-EVNICT)

2

### Chính sách, biện pháp kiểm soát Tổ chức (CS01.ATTT, 5.1 đến 5.37)

Stt	Biện pháp kiểm soát (BPKS)		Thuộc tính của BPKS				
	Điều khoản	Biện pháp kiểm soát	Kiểu Kiểm soát	Đặc tính ATTT	Khái niệm An ninh mạng	Khả năng vận hành	Lĩnh vực ATTT
CS01	5	<b>Kiểm soát tổ chức (Organizational controls)</b>					
1	5.1	Chính sách an toàn thông tin Policies for information security	Phòng ngừa	Bảo mật (C), Toàn vẹn (I), Sẵn sàng (A)	Xác định	Quản trị	Quản trị và hệ sinh thái, Khôi phục
2	5.2	Vai trò và trách nhiệm An toàn thông tin Information security roles and responsibility	Phòng ngừa	Bảo mật (C), Toàn vẹn (I), Sẵn sàng (A)	Xác định	Quản trị	Quản trị và hệ sinh thái, Bảo vệ, Khôi phục
3	5.3	Phân tách nhiệm vụ Segregation of duties	Phòng ngừa	Bảo mật (C), Toàn vẹn (I), Sẵn sàng (A)	Bảo vệ	Quản trị, Quản lý truy cập và xác thực	Quản trị và hệ sinh thái
4	5.4	Trách nhiệm quản lý Management responsibilities	Phòng ngừa	Bảo mật (C), Toàn vẹn (I), Sẵn sàng (A)	Xác định	Quản trị	Quản trị và hệ sinh thái
5	5.5	Liên lạc với cơ quan/ tổ chức có thẩm quyền Contact with authorities	Phòng gùra, Khắc phục	Bảo mật (C), Toàn vẹn (I), Sẵn sàng (A)	Xác định Bảo vệ, Đáp ứng, Khôi phục	Quản trị	Phòng thủ, Khôi phục
6	5.6	Liên lạc với các nhóm quan tâm đặc thù, chuyên gia Contact with special interest groups	Phòng gùra, Khắc phục	Bảo mật (C), Toàn vẹn (I), Sẵn sàng (A)	Bảo vệ, Đáp ứng, Khôi phục	Quản trị	Phòng thủ
7	5.7	Tri thức về mối đe dọa ATTT Threat intelligence	Phòng gùra, Phát hiện, Khắc phục	Bảo mật (C), Toàn vẹn (I), Sẵn sàng (A)	Xác định, Phát hiện, Đáp ứng	Quản lý mối nguy và điểm yếu	Phòng thủ
8	5.8	An toàn thông tin trong quản lý dự án Information security in project management	Phòng ngừa	Bảo mật (C), Toàn vẹn (I), Sẵn sàng (A)	Xác định, Bảo vệ	Quản trị	Quản trị và hệ sinh thái, Bảo vệ



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# BIỆN PHÁP KIỂM SOÁT

## (Quy định số 16/QĐ-EVNICT)

2

### Chính sách, biện pháp kiểm soát Con người (CS02.ATTT)

Stt	Biện pháp kiểm soát (BPKS)		Thuộc tính của BPKS				
	Điều khoản	Biện pháp kiểm soát	Kiểu Kiểm soát	Đặc tính ATTT	Khái niệm An ninh mạng	Khả năng vận hành	Lĩnh vực ATTT
CS02	6	Kiểm soát con người (People controls)					
	38	6.1 Sàng lọc Screening	Phòng ngừa	Bảo mật (C), Toàn vẹn (I), Sẵn sàng (A)	Bảo vệ	An ninh nguồn nhân lực	Quản trị và hệ sinh thái
	39	6.2 Điều khoản và điều kiện làm việc Terms and conditions of employment	Phòng ngừa	Bảo mật (C), Toàn vẹn (I), Sẵn sàng (A)	Bảo vệ	An ninh nguồn nhân lực	Quản trị và hệ sinh thái
	40	6.3 Nhận thức, giáo dục và đào tạo về an toàn thông tin Information security awareness, education and training	Phòng ngừa	Bảo mật (C), Toàn vẹn (I), Sẵn sàng (A)	Bảo vệ	An ninh nguồn nhân lực	Quản trị và hệ sinh thái
	41	6.4 Quy trình xử lý vi phạm/ kỷ luật Disciplinary process	Phòng ngừa, Khắc phục	Bảo mật (C), Toàn vẹn (I), Sẵn sàng (A)	Bảo vệ, Đáp ứng	An ninh nguồn nhân lực	Quản trị và hệ sinh thái
	42	6.5 Trách nhiệm sau khi chấm dứt hoặc thay đổi công việc Responsibilities after termination or change of employment	Phòng ngừa	Bảo mật (C), Toàn vẹn (I), Sẵn sàng (A)	Bảo vệ	An ninh nguồn nhân lực, Quản lý tài sản	Quản trị và hệ sinh thái
	43	6.6 Thỏa thuận bảo mật hoặc không tiết lộ thông tin Confidentiality or non-disclosure agreements	Phòng ngừa	Bảo mật (C)	Bảo vệ	An ninh nguồn nhân lực, Bảo vệ thông tin, An ninh nhà cung cấp	Quản trị và hệ sinh thái
	44	6.7 Làm việc từ xa Remote working	Phòng ngừa	Bảo mật (C), Toàn vẹn (I), Sẵn sàng (A)	Bảo vệ	Quản lý tài sản, Bảo vệ thông tin, An ninh vật lý, An ninh mạng và hệ thống	Bảo vệ
	45	6.8 Báo cáo sự kiện an toàn thông tin Information security event reporting	Phòng ngừa	Bảo mật (C), Toàn vẹn (I), Sẵn sàng (A)	Phát hiện	Quản lý sự kiện ATTT	Phòng thủ



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# BIỆN PHÁP KIỂM SOÁT

## (Quy định số 16/QĐ-EVNICT)

2

### Chính sách, biện pháp kiểm soát Vật lý (CS03.ATTT)

Số thứ tự	Biện pháp kiểm soát (BPKS)		Thuộc tính của BPKS				
	Điều khoản	Biện pháp kiểm soát	Kiểu Kiểm soát	Đặc tính ATTT	Khái niệm An ninh mạng	Khả năng vận hành	Lĩnh vực ATTT
CS03	7	<b>Kiểm soát vật lý (Physical controls)</b>					
46	7.1	Vành đai an ninh vật lý Physical security perimeters	Phòng ngừa	Bảo mật (C), Toàn vẹn (I), Sẵn sàng (A)	Bảo vệ	An ninh vật lý	Bảo vệ
47	7.2	Truy nhập vật lý Physical entry	Phòng ngừa	Bảo mật (C), Toàn vẹn (I), Sẵn sàng (A)	Bảo vệ	An ninh vật lý, Quản lý truy cập và xác thực	Bảo vệ
48	7.3	An ninh khu vực cơ quan, văn phòng và thiết bị Securing offices, rooms and facilities	Phòng ngừa	Bảo mật (C), Toàn vẹn (I), Sẵn sàng (A)	Bảo vệ	Quản lý tài sản, An ninh vật lý	Bảo vệ
49	7.4	Giám sát an ninh vật lý Physical security monitoring	Phòng ngừa, Phát hiện	Bảo mật (C), Toàn vẹn (I), Sẵn sàng (A)	Bảo vệ, Phát hiện	An ninh vật lý	Bảo vệ, Phòng thủ
50	7.5	Bảo vệ chống lại các mối đe dọa vật lý và môi trường Protecting against physical and environmental threats	Phòng ngừa	Bảo mật (C), Toàn vẹn (I), Sẵn sàng (A)	Bảo vệ	An ninh vật lý	Bảo vệ
51	7.6	Làm việc trong khu vực an ninh Working in secure areas	Phòng ngừa	Bảo mật (C), Toàn vẹn (I), Sẵn sàng (A)	Bảo vệ	An ninh vật lý	Bảo vệ
52	7.7	Bàn sạch và màn hình sạch Clear desk and clear screen	Phòng ngừa	Bảo mật (C)	Bảo vệ	An ninh vật lý	Bảo vệ
53	7.8	Bảo vệ và vị trí thiết bị Equipment siting and protection	Phòng ngừa	Bảo mật (C), Toàn vẹn (I), Sẵn sàng (A)	Bảo vệ	An ninh vật lý, Quản lý tài sản	Bảo vệ



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# BIỆN PHÁP KIỂM SOÁT

## (Quy định số 16/QĐ-EVNICT)

2

### Chính sách, biện pháp kiểm soát Công nghệ (CS04.ATTT)

Stt	Biện pháp kiểm soát (BPKS)		Thuộc tính của BPKS				
	Điều khoản	Biện pháp kiểm soát	Kiểu Kiểm soát	Đặc tính ATTT	Khái niệm An ninh mạng	Khả năng vận hành	Lĩnh vực ATTT
CS04	8	<b>Kiểm soát công nghệ (Technological controls)</b>					
60	8.1	Thiết bị đầu cuối của người sử dụng User end point devices	Phòng ngừa	Bảo mật (C), Toàn vẹn (I), Sẵn sàng (A)	Bảo vệ	Quản lý tài sản, Bảo vệ thông tin	Bảo vệ
61	8.2	Quyền truy cập đặc quyền Privileged access rights	Phòng ngừa	Bảo mật (C), Toàn vẹn (I), Sẵn sàng (A)	Bảo vệ	Quản lý truy cập và xác thực	Bảo vệ
62	8.3	Hạn chế truy cập thông tin Information access restriction	Phòng ngừa	Bảo mật (C), Toàn vẹn (I), Sẵn sàng (A)	Bảo vệ	Quản lý truy cập và xác thực	Bảo vệ
63	8.4	Truy nhập mã nguồn Access to source code	Phòng ngừa	Bảo mật (C), Toàn vẹn (I), Sẵn sàng (A)	Bảo vệ	Quản lý truy cập và xác thực, An ninh ứng dụng, An ninh cấu hình	Bảo vệ
64	8.5	Xác thực an toàn Secure authentication	Phòng ngừa	Bảo mật (C), Toàn vẹn (I), Sẵn sàng (A)	Bảo vệ	Quản lý truy cập và xác thực	Bảo vệ
65	8.6	Quản lý năng lực/ dung lượng Capacity management	Phòng ngừa, Phát hiện	Toàn vẹn (I), Sẵn sàng (A)	Xác định, Bảo vệ, Phát hiện	Tính liên tục	Quản trị và hệ sinh thái, Bảo vệ
66	8.7	Bảo vệ chống mã độc Protection against malware	Phòng ngừa, Phát hiện, Khắc phục	Bảo mật (C), Toàn vẹn (I), Sẵn sàng (A)	Bảo vệ, Phát hiện	Bảo vệ thông tin, An ninh mạng và hệ thống	Bảo vệ , Phòng thủ
67	8.8	Quản lý điểm yếu kỹ thuật/ lỗ hổng bảo mật Management of technical vulnerabilities	Phòng ngừa	Bảo mật (C), Toàn vẹn (I), Sẵn sàng (A)	Xác định, Bảo vệ	Quản lý mối nguy và điểm yếu	Quản trị và hệ sinh thái, Bảo vệ , Phòng thủ



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# PHẦN 3

## TRÁCH NHIỆM QUẢN LÝ ATTT TẠI ĐƠN VỊ



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# QT01.ATTT. QUY TRÌNH XÂY DỰNG MỤC TIÊU, KẾ HOẠCH VÀ ĐÁNH GIÁ THỰC HIỆN

## (Quy định số 16/QĐ-EVNICT)

3

Stt	Trách nhiệm	Các bước thực hiện	Biểu mẫu, đầu ra	Mô tả, diễn giải
1	Đơn vị đầu mối Đơn vị áp dụng	Xây dựng mục tiêu ATTT	BM 01a/ HTQLATTT	<ul style="list-style-type: none"> <li>- Định kỳ quý 1 hàng năm,</li> <li>- Đơn vị đầu mối xây dựng mục tiêu ATTT toàn Công ty trình Lãnh đạo công ty phê duyệt.</li> <li>- Đơn vị áp dụng mục tiêu ATTT của công ty và căn cứ vào hoạt động thực tế, kết quả đánh giá và xử lý rủi ro ATTT, kết quả thực hiện mục tiêu ATTT của kỳ trước và Chính sách ATTT để bổ sung mục tiêu ATTT riêng của đơn vị và kế hoạch thực hiện, trình Lãnh đạo đơn vị phê duyệt.</li> <li>- Đơn vị áp dụng gửi mục tiêu ATTT đã được Lãnh đạo đơn vị phê duyệt đến Đơn vị đầu mối để tổng hợp đánh giá và trình Lãnh đạo công ty phê duyệt.</li> </ul>
2	Đơn vị áp dụng	Thực hiện mục tiêu ATTT		Căn cứ các mục tiêu ATTT và kế hoạch triển khai đã được phê duyệt, các đơn vị tiến hành triển khai thực hiện
3	Đơn vị áp dụng	Đánh giá và báo cáo kết quả thực hiện mục tiêu ATTT	BM 01b/ HTQLATTT	<p>Định kỳ 30/6 và 31/12 hàng năm,</p> <p>Đơn vị áp dụng đánh giá tình hình thực hiện mục tiêu ATTT trong kỳ của đơn vị mình, trình Lãnh đạo đơn vị phê duyệt và gửi về Đơn vị đầu mối tổng hợp đánh giá.</p> <p>Báo cáo kết quả thực hiện mục tiêu ATTT bao gồm các nội dung chính sau:</p> <ul style="list-style-type: none"> <li>a) Đánh giá kết quả thực hiện từng mục tiêu ATTT cụ thể.</li> <li>b) Phân tích rõ nguyên nhân đối với những mục tiêu ATTT không đạt được.</li> <li>c) Đưa ra hành động khắc phục, biện pháp thực hiện trong kỳ tới hoặc đề xuất nội dung mục tiêu ATTT kỳ tiếp theo (nếu có).</li> <li>d) Phương pháp đo lường cụ thể, bao gồm một số hoặc tất cả các yếu tố: Tần suất đo, cách thức chọn mẫu, công thức đo lường, nguồn dữ liệu...</li> </ul>
4	Đơn vị đầu mối	Tổng hợp và báo cáo		Căn cứ báo cáo kết quả thực hiện mục tiêu ATTT của các đơn vị, Đơn vị đầu mối tổng hợp báo cáo duy trì HTQLATTT toàn hệ thống để đánh giá hoàn thành mục tiêu, đồng thời là kết quả phục vụ xem xét của lãnh đạo về việc duy trì, cải tiến HTQLATTT
5	Đơn vị đầu mối Đơn vị áp dụng	Lưu hồ sơ	BM 01a, 01b/ HTQLATTT	Các đơn vị áp dụng lưu hồ sơ của đơn vị, đơn vị đầu mối lưu hồ sơ của Công ty



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# QT02.ATTT. QUY TRÌNH THỰC HIỆN GIÁM SÁT ĐO LƯỜNG CÁC QUÁ TRÌNH, BIỆN PHÁP QUẢN LÝ ATTT

**(Quy định số 16/QĐ-EVNICT)**

3

Số thứ tự	Trách nhiệm	Các bước thực hiện	Biểu mẫu, đầu ra	Mô tả, diễn giải
1	Đơn vị đầu mối Đơn vị áp dụng	Xác định nội dung cần giám sát & đo lường, phương pháp thực hiện	BM 02a/ HTQLATT	<ul style="list-style-type: none"> <li>- <b>Định kỳ, tháng 3 hàng năm,</b></li> <li>Đơn vị đầu mối xác định các nội dung quản lý ATTT cần thực hiện giám sát và đo lường, trình Lãnh đạo công ty phê duyệt và gửi về Đơn vị áp dụng để thực hiện.</li> <li>- Căn cứ các nội dung quản lý ATTT của công ty, Đơn vị áp dụng bổ sung các nội dung cần thực hiện giám sát và đo lường của đơn vị mình, trình Lãnh đạo đơn vị phê duyệt và gửi về Đơn vị đầu mối chậm nhất 30/03 hàng năm. Trong đó nêu rõ thông số cần đo và chỉ tiêu cụ thể cần đạt trong năm, phương pháp, tần suất đo lường, giám sát</li> </ul>
2	Đơn vị áp dụng	Triển khai giám sát, đo lường		<ul style="list-style-type: none"> <li>- Căn cứ theo nội dung được phê duyệt, Đơn vị áp dụng triển khai thực hiện các công việc theo dõi và đo lường, cập nhật dữ liệu giám sát, đo lường.</li> <li>- Đơn vị áp dụng phân công nhân sự/ bộ phận thực hiện đo lường, giám sát</li> </ul>
3	Đơn vị áp dụng	Đánh giá và báo cáo kết quả thực	BM 02b/ HTQLATT	<ul style="list-style-type: none"> <li>- <b>Định kỳ hàng quý,</b></li> <li>Đơn vị áp dụng tiến hành so sánh kết quả theo dõi, đo lường với các thông số và chỉ tiêu đo lường năm đã được phê duyệt; lập báo cáo trình Lãnh đạo đơn vị xem xét, phê duyệt kết quả đo lường của các biện pháp quản lý.</li> <li>- Trường hợp các quá trình/biện pháp quản lý được giám sát, đo lường không đáp ứng các thông số và chỉ tiêu đặt ra, Đơn vị áp dụng tìm nguyên nhân, tiến hành khắc phục, cải tiến và lập Phiếu đề xuất khắc phục (Mẫu số 04a/ HTQLATT).</li> <li>- Chậm nhất tuần đầu tiên quý tiếp theo, Đơn vị áp dụng gửi báo cáo đã được Lãnh đạo đơn vị phê duyệt đến Đơn vị đầu mối tổng hợp sử dụng cho hoạt động xem xét, cải tiến HTQLATT</li> </ul>
4	Đơn vị đầu mối	Tổng hợp và báo cáo		Căn cứ báo cáo kết quả giám sát, đo lường các quá trình, biện pháp quản lý của các Đơn vị áp dụng, Đơn vị đầu mối tổng hợp báo cáo duy trì HTQLATT toàn hệ thống, phục vụ xem xét của lãnh đạo và hoạt động xem xét, cải tiến HTQLATT
5	Đơn vị đầu mối Đơn vị áp dụng	Lưu hồ sơ	BM 02a, 02b/ HTQLATT	Các đơn vị áp dụng lưu hồ sơ của đơn vị, đơn vị đầu mối lưu hồ sơ của Công ty



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# QT03.ATTT. QUY TRÌNH ĐÁNH GIÁ NỘI BỘ HỆ THỐNG QUẢN LÝ ATTT

**(Quy định số 16/QĐ-EVNICT)**

2

Số thứ tự	Trách nhiệm	Các bước thực hiện	Biểu mẫu đầu ra	Mô tả, diễn giải
1	Đơn vị đầu mối		Kế hoạch đánh giá nội bộ, BM01.ĐGNB	<p>Định kỳ ít nhất 1 lần/năm, trước 31/10 hàng năm, Đơn vị đầu mối lập kế hoạch đánh giá, trình Lãnh đạo công ty phê duyệt.</p> <ul style="list-style-type: none"> <li>- Hình thức ĐGNB: Trực tiếp; gián tiếp qua Elearning; rà soát báo cáo chỉ tiêu.</li> <li>- Thời gian ĐGNB: Tổ chức thực hiện ĐGNB định kỳ hoặc đột xuất theo quy định, tối thiểu 1 lần/năm với mỗi lĩnh vực (HTCNTT, VT, PM, ANTT).</li> </ul> <p>Đoàn đánh giá</p> <ul style="list-style-type: none"> <li>- Thành phần: gồm Trưởng đoàn và các thành viên (chuyên gia đánh giá).</li> <li>- Tiêu chuẩn: <ul style="list-style-type: none"> <li>+ Là chuyên gia ĐGNB đáp ứng yêu cầu: đã tham gia và hoàn thành khóa đào tạo chuyên gia ĐGNB.</li> <li>+ Có kinh nghiệm, kiến thức về các hoạt động của EVNICT (về lĩnh vực đánh giá: Hạ tầng CNTT, Viễn thông, Phần mềm, An toàn thông tin).</li> <li>+ Người đánh giá không liên quan trực tiếp đến hoạt động được đánh giá</li> </ul> </li> </ul>
2	Đơn vị đầu mối		BM01.ĐGNB	Thông báo kế hoạch đánh giá tới các bộ phận liên quan trước thời điểm đánh giá ít nhất 05 ngày làm việc. Kèm theo Phiếu khảo sát, lấy ý kiến bộ phận/ cá nhân về hoạt động thực tế so với quy trình chính sách
3	Đoàn đánh giá Các đơn vị được phân công		Danh mục kiểm tra (Checklist/ATTT) BM02.ĐGNB	<ul style="list-style-type: none"> <li>- Trưởng đoàn đánh giá tổ chức Họp, phân công các thành viên chuẩn bị các nội dung: <ul style="list-style-type: none"> <li>+ Xem xét tài liệu, tìm hiểu hoạt động của đơn vị được đánh giá.</li> <li>+ Chuẩn bị Danh mục kiểm tra.</li> <li>+ Chuẩn bị Phiếu yêu cầu khắc phục/ khuyến nghị cải tiến, ghi chép kèm theo theo.</li> </ul> </li> <li>- Đơn vị được đánh giá có trách nhiệm cung cấp tài liệu của đơn vị mình cho đoàn đánh giá nghiên cứu trước (nếu được yêu cầu); điền Phiếu khảo sát, lấy ý kiến</li> </ul>
4	Đoàn đánh giá  Đại diện lãnh đạo đơn vị được đánh giá  Thành viên Ban ATTT		Danh sách họp đánh giá nội bộ, BM03.ĐGNB  Phiếu khắc phục, khuyến nghị, BM04.ĐGNB  Biên bản kết luận đánh giá, BM05.ĐGNB	<ul style="list-style-type: none"> <li>a) Họp khai mạc/ kết thúc: đoàn đánh giá và lãnh đạo/ đại diện của đơn vị/ bộ phận được đánh giá, Danh sách tham dự họp</li> <li>b) Tiến hành đánh giá</li> <li>- Tuân thủ Quy định, Tiêu chuẩn đánh giá</li> <li>- Đánh giá được tiến hành theo nguyên tắc chọn mẫu ngẫu nhiên, nhưng cần đảm bảo xem xét hết toàn bộ các nội dung chính của lĩnh vực được đánh giá bao gồm các biện pháp quản lý (quy định, chính sách, ...) và các biện pháp kỹ thuật (quản trị, vận hành, phát triển, an toàn, bảo mật, ...).</li> <li>- Trường hợp phát hiện ra các điểm không phù hợp, Chuyên gia ĐGNB lập Phiếu yêu cầu khắc phục/ khuyến nghị cải tiến và xác nhận cùng Lãnh đạo/ đại diện bộ phận được đánh giá.</li> <li>+ Điểm yêu cầu khắc phục: bộ phận được đánh giá phải thực hiện trong vòng 30 ngày.</li> <li>+ Điểm khuyến nghị cải tiến: bộ phận được đánh giá đề xuất thời hạn thực hiện trong năm</li> <li>c) Thông qua kết quả đánh giá</li> <li>- Đoàn đánh giá và Lãnh đạo/ đại diện đơn vị được đánh giá tiến hành họp thông qua kết quả đánh giá, thống nhất thời gian gửi báo cáo tinh hình thực hiện hành động khắc phục/ cải tiến. Lập Biên bản kết luận đánh giá.</li> </ul>
5	Trưởng nhóm đánh giá		BM03, 4, 5, 6.ĐGNB	Đoàn đánh giá tổng hợp Báo cáo đánh giá nội bộ theo Mẫu số BM06.ĐGNB, kèm theo Biên bản kết luận BM05.ĐGNB và Phiếu yêu cầu khắc phục/ khuyến nghị cải tiến theo Mẫu số BM04.ĐGNB
6	Đơn vị đầu mối; Đơn vị được đánh giá		BM01-06.ĐGNB và các báo cáo khắc phục liên quan	Đơn vị/ bộ phận được đánh giá, Đơn vị đầu mối lưu hồ sơ

Lưu hành nội bộ



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# QT04.ATTT. QUY TRÌNH THỰC HIỆN HÀNH ĐỘNG KHẮC PHỤC CẢI TIẾN SỰ KHÔNG PHÙ HỢP (Quy định số 16/QĐ-EVNICT)

2

Số thứ tự	Trách nhiệm	Các bước thực hiện	Biểu mẫu, đầu ra	Mô tả, diễn giải
1	Đơn vị đầu mối Đơn vị áp dụng	<pre> graph TD     A([Đề xuất khắc phục, cải tiến]) --&gt; B{Xem xét, Phê duyệt}     </pre>	BM 04a/ HTQLATTT BM 03/ HTQLATTT	<p>a) Trường hợp nhận được yêu cầu hành động khắc phục:</p> <p>Đơn vị/bộ phận nhận được yêu cầu hành động khắc phục phải xác định nguyên nhân gây ra lỗi, đề xuất hành động khắc phục, thời hạn khắc phục và thực hiện hành động khắc phục theo Phiếu yêu cầu hành động khắc phục Mẫu số 03e/HTQLATTT trình lãnh đạo đơn vị phê duyệt.</p> <p>b) Phát sinh nhu cầu khắc phục, cải tiến:</p> <p>Trong quá trình hoạt động hoặc theo khuyến nghị của các đoàn đánh giá, đơn vị đề xuất hoạt động yêu cầu khắc phục, cải tiến theo Phiếu đề xuất Mẫu số 04a/HTQLATTT trình lãnh đạo đơn vị phê duyệt</p>
2	Lãnh đạo đơn vị	<pre> graph TD     B{Xem xét, Phê duyệt} --&gt; C[Triển khai thực hiện]     </pre>	BM 04a/ HTQLATTT BM 03/ HTQLATTT	Lãnh đạo đơn vị xem xét đề xuất hành động khắc phục, cải tiến, phê duyệt hành động khắc phục, cải tiến (nếu cần thiết), phân công trách nhiệm thực hiện và kiểm tra thực hiện hành động khắc phục, cải tiến
3	Đơn vị áp dụng	<pre> graph TD     C[Triển khai thực hiện] --&gt; D{Kiểm tra}     </pre>		<ul style="list-style-type: none"> <li>Căn cứ đề xuất được duyệt, đơn vị/bộ phận/cá nhân được phân công triển khai thực hiện các công việc theo nội dung đề xuất.</li> <li>Trong quá trình triển khai, nếu có các vướng mắc, khó khăn xảy ra cần kết hợp với các bộ phận liên quan để giải quyết theo đúng quy định về nhiệm vụ và quyền hạn được giao</li> </ul>
4	Đoàn kiểm tra, Ban ATTT	<pre> graph TD     D{Kiểm tra} --&gt; E[Báo cáo kết quả]     </pre>	BM 04a/ HTQLATTT BM 03/ HTQLATTT	<ul style="list-style-type: none"> <li>Căn cứ thời hạn được cấp có thẩm quyền phê duyệt, Đoàn kiểm tra hoặc Ban ATTT tiến hành kiểm tra hành động khắc phục, kết quả cải tiến.</li> <li>Trường hợp hành động khắc phục, cải tiến chưa được thực hiện hoặc chưa đạt yêu cầu, Đoàn kiểm tra hoặc Ban ATTT tiến hành lập lại Phiếu yêu cầu hành động khắc phục/Phiếu đề xuất (có ghi rõ số lần nhắc lại), gửi đến đơn vị/bộ phận liên quan và báo cáo lãnh đạo đơn vị. Quá trình này được lặp lại cho đến khi hành động khắc phục, cải tiến đạt yêu cầu.</li> <li>Trường hợp hành động khắc phục, cải tiến đã được thực hiện và đạt yêu cầu, tiến hành đóng Phiếu yêu cầu hành động khắc phục/Phiếu đề xuất, báo cáo tới lãnh đạo đơn vị</li> </ul>
5	Đơn vị áp dụng Đơn vị đầu mối	<pre> graph TD     E[Báo cáo kết quả] --&gt; F([Lưu hồ sơ])     </pre>		<ul style="list-style-type: none"> <li>Đối với hành động khắc phục, cải tiến sau Đánh giá nội bộ và đánh giá chứng nhận: Đơn vị báo cáo hành động khắc phục, cải tiến và kết quả khắc phục, cải tiến theo yêu cầu của Đoàn đánh giá/Tổ chức chứng nhận.</li> <li>Đối với hành động khắc phục, cải tiến khác: Châm nhặt ngày 5 tháng đầu tiên quý tiếp theo, Đơn vị thực hiện hành động khắc phục, cải tiến tổng hợp các đề xuất hành động khắc phục, cải tiến và kết quả khắc phục, cải tiến của quý trước (nếu có) theo Mẫu số 04b/HTQLATTT gửi Đơn vị đầu mối tổng hợp.</li> <li>Căn cứ báo cáo hành động khắc phục, cải tiến của các đơn vị, Đơn vị đầu mối tổng hợp báo cáo duy trì HTQLATTT toàn hệ thống, phục vụ việc xem xét của Lãnh đạo</li> </ul>
6	Đơn vị đầu mối Đơn vị áp dụng	<pre> graph TD     F([Lưu hồ sơ])     </pre>	BM 04a, 04b/ HTQLATTT	Các đơn vị áp dụng lưu hồ sơ của đơn vị, đơn vị đầu mối lưu hồ sơ của Công ty



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# QT05.ATTT. QUY TRÌNH XEM XÉT CỦA LÃNH ĐẠO VÀ CẢI TIẾN LIÊN TỤC

(Quy định số 16/QĐ-EVNICT)

2

Số thứ tự	Trách nhiệm	Các bước thực hiện	Biểu mẫu, đầu ra	Mô tả, diễn giải
1	Đơn vị đầu mối Đơn vị áp dụng	Lập kế hoạch và chuẩn bị	BM 05/HTQLATTT	<p>Định kỳ ít nhất 1 lần/năm, trước 31/10 hàng năm</p> <p>Đơn vị đầu mối chịu trách nhiệm lập kế hoạch xem xét của lãnh đạo ATTT, trình Lãnh đạo ATTT/Giám đốc thông qua và phê duyệt, trong đó nêu rõ phân công trách nhiệm chuẩn bị tài liệu, báo cáo:</p> <ul style="list-style-type: none"> <li>+ Các đơn vị áp dụng HTQLATTT chuẩn bị các nội dung liên quan đến kết quả áp dụng, duy trì HTQLATTT tại đơn vị mình và các ý kiến, đề xuất cải tiến HTQLATTT.</li> <li>+ Đơn vị đầu mối chuẩn bị các nội dung liên quan đến việc theo dõi giám sát việc triển khai áp dụng HTQLATTT của Công ty; tổng hợp báo cáo kết quả duy trì HTQLATTT toàn hệ thống</li> </ul>
2	Lãnh đạo ATTT/ Giám đốc	Xem xét hoặc Hợp xem xét và lập biên bản	Biên bản họp	<p>Nếu có tổ chức cuộc họp:</p> <ul style="list-style-type: none"> <li>- Đơn vị đầu mối báo cáo khái quát chung về tình hình áp dụng, duy trì HTQLATTT.</li> <li>- Các đơn vị/bộ phận báo cáo các nội dung được phân công.</li> <li>- Trao đổi, thảo luận.</li> <li>- Lãnh đạo công ty chỉ đạo thực hiện các hoạt động nhằm duy trì và cải tiến tính phù hợp, hiệu lực và hiệu quả của HTQLATTT và xem xét phê duyệt báo cáo kết quả áp dụng, duy trì HTQLATTT và kế hoạch cải tiến các nội dung như:</li> <li>+ Cập nhật kế hoạch đánh giá và xử lý rủi ro, mức độ rủi ro và hoặc tiêu chí chấp nhận rủi ro. + Cải tiến các thủ tục và biện pháp quản lý cần thiết có ảnh hưởng đến ATTT. + Các nhu cầu cần thiết về nguồn lực. + Các cải tiến nâng cao hiệu lực của HTQLATTT.</li> <li>- Thư ký cuộc họp ghi lại biên bản cuộc họp.</li> <li>- Thư ký cuộc họp trình bày các nội dung chính của cuộc, trong đó nhấn mạnh các vấn đề:</li> <li>+ Nhắc lại các vấn đề thảo luận và đi đến thống nhất. + Nhắc lại các quyết định/chỉ đạo của chủ trì cuộc họp.</li> </ul> <p>Nếu không tổ chức cuộc họp:</p> <ul style="list-style-type: none"> <li>- Lãnh đạo công ty xem xét các báo cáo và phê duyệt báo cáo kết quả áp dụng, duy trì HTQLATTT và các kế hoạch cải tiến tính hiệu lực và hiệu quả của HTQLATTT</li> </ul>
4	Đơn vị đầu mối	Thông báo kết luận và kế hoạch cải tiến	Kết luận họp, Giao nhiệm vụ	Căn cứ kết luận xem xét của lãnh đạo, Đơn vị đầu mối thông báo tới các đơn vị/bộ phận/cá nhân liên quan để thực hiện kế hoạch cải tiến
5	Đơn vị áp dụng Đơn vị đầu mối	Theo dõi thực hiện Kế hoạch cải tiến		Các đơn vị chịu trách nhiệm theo dõi việc thực hiện kế hoạch cải tiến đã được phê duyệt
6	Đơn vị đầu mối Đơn vị áp dụng	Lưu hồ sơ	BM 05/ HTQLATTT Biên bản Kết luận	Các đơn vị áp dụng lưu hồ sơ của đơn vị, đơn vị đầu mối lưu hồ sơ của Công ty



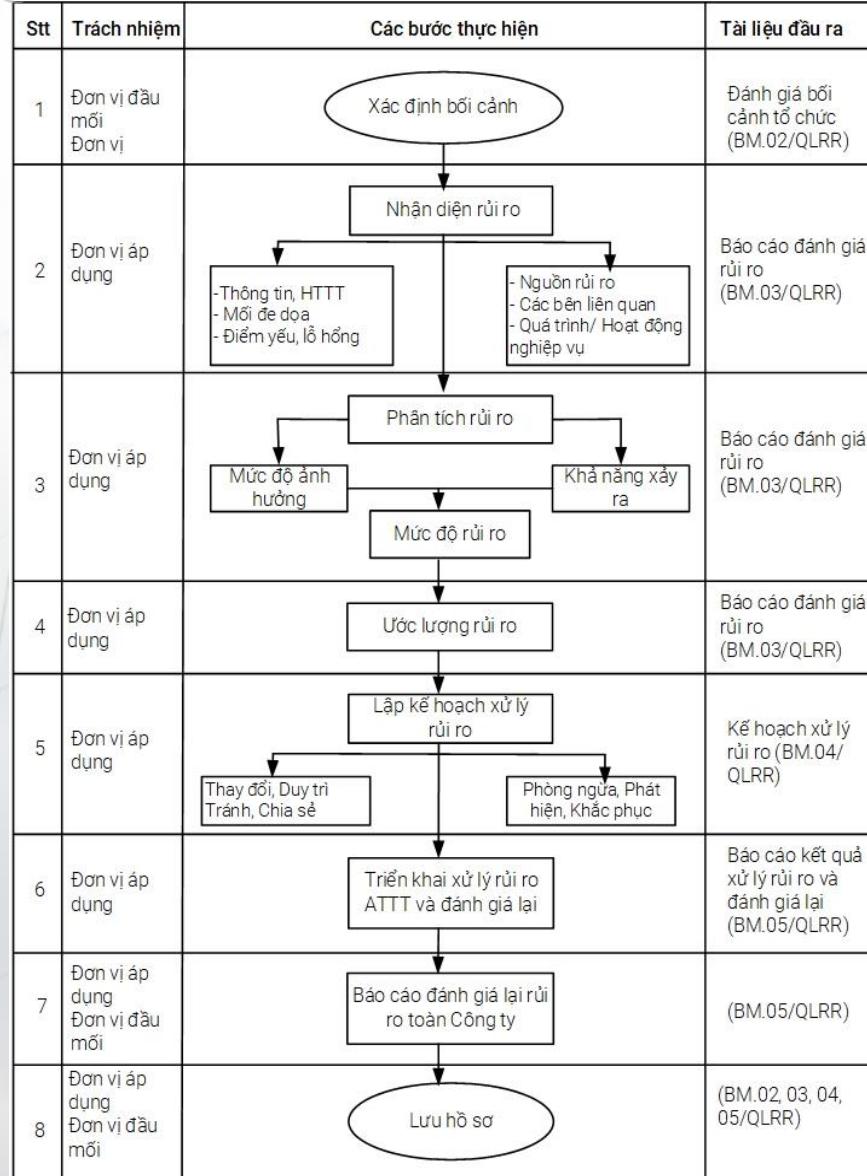
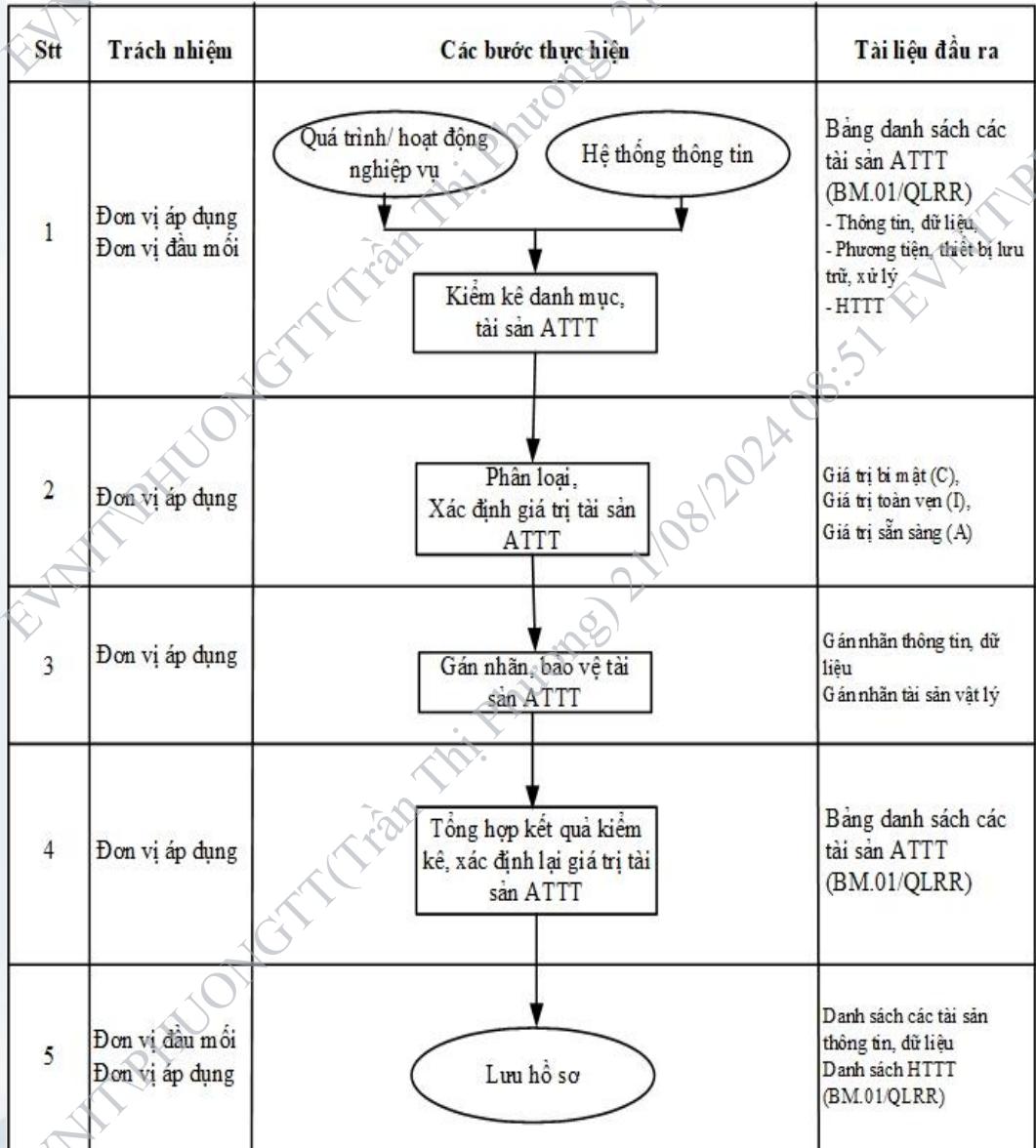
EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# QT01.QLRR. QUY TRÌNH QUẢN LÝ TÀI SẢN THÔNG TIN,

## QT02.QLRR. QUẢN LÝ RỦI RO ATTT (Quy định số 16/QĐ-EVNICT)

2





EVN

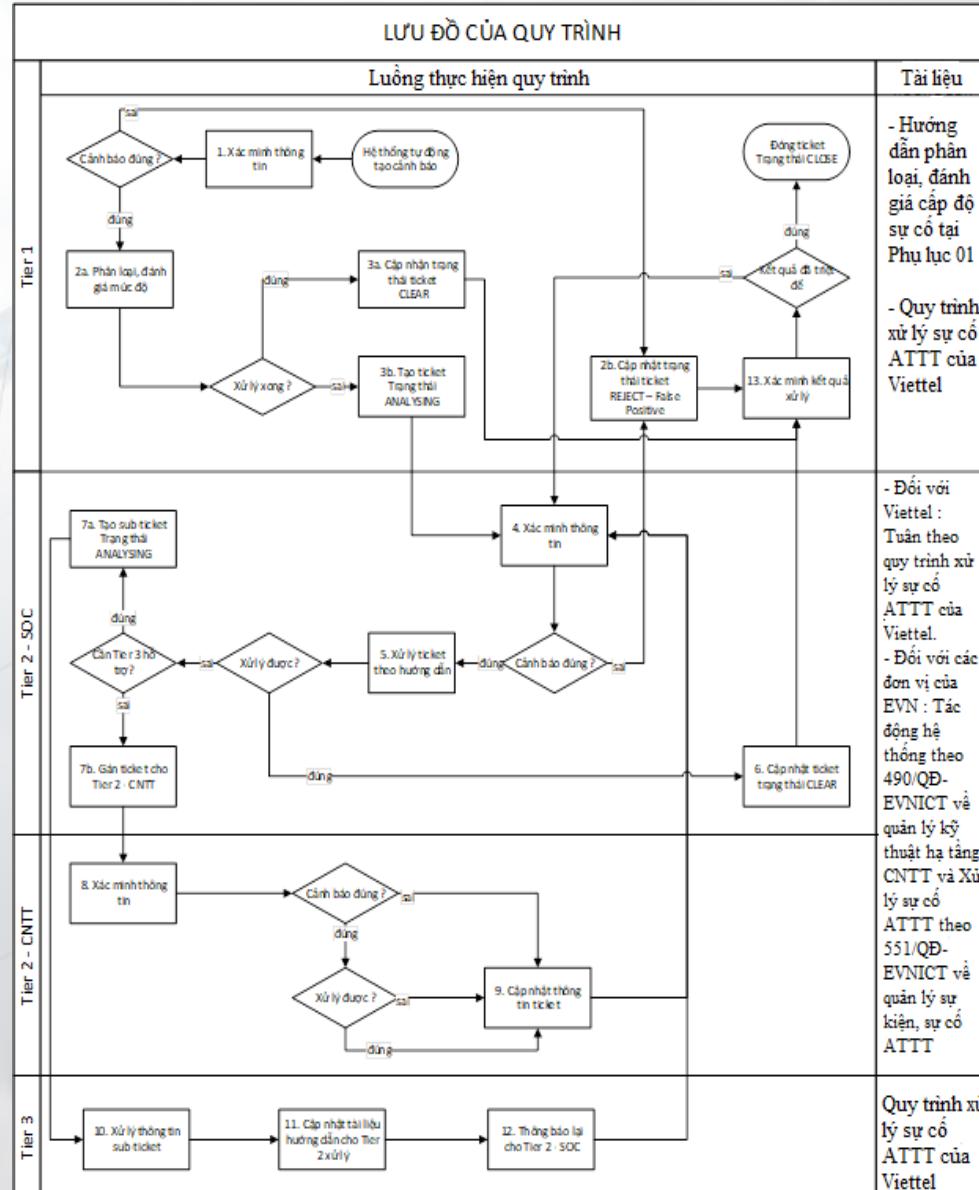
CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# Quy trình tổ chức diễn tập nội bộ EVNICT (Quy định số 101/QĐ-EVNICT)

## Quy trình vận hành giám sát xử lý an toàn thông tin ((Quy định số 06/QĐ-EVNICT))

2

Trách nhiệm	Nội dung	Tài liệu liên quan
	<pre> graph TD     Start([Bắt đầu]) --&gt; Prep[Đề xuất tổ chức diễn tập]     Prep --&gt; Build[Xây dựng kịch bản]     Build --&gt; Prepare[Chuẩn bị trước khi tổ chức diễn tập]     Prepare --&gt; Execute[Tổ chức diễn tập]     Execute --&gt; End([Kết thúc])     </pre>	
Đơn vị chủ trì công tác diễn tập	<pre> graph TD     Start --&gt; Prep     Prep --&gt; Build     Build --&gt; Prepare     Prepare --&gt; Execute     Execute --&gt; End     </pre> <p>- Kế hoạch diễn tập đã được phê duyệt - Tình hình thực tế</p>	
Đơn vị chủ trì công tác diễn tập	<pre> graph TD     Start --&gt; Prep     Prep --&gt; Build     Build --&gt; Prepare     Prepare --&gt; Execute     Execute --&gt; End     </pre> <p>- Đề xuất được duyệt</p>	
Đơn vị theo phân công tại kịch bản	<pre> graph TD     Start --&gt; Prep     Prep --&gt; Build     Build --&gt; Prepare     Prepare --&gt; Execute     Execute --&gt; End     </pre> <p>- Kịch bản diễn tập được duyệt - Hồ sơ hệ thống liên quan - Quy trình quản trị vận hành hệ thống liên quan - phương án phòng ngừa, xử lý và khắc phục sự cố</p>	
Đơn vị theo phân công tại kịch bản	<pre> graph TD     Start --&gt; Prep     Prep --&gt; Build     Build --&gt; Prepare     Prepare --&gt; Execute     Execute --&gt; End     </pre> <p>- Kịch bản diễn tập được duyệt - Quy trình quản trị vận hành hệ thống liên quan - phương án phòng ngừa, xử lý và khắc phục sự cố</p>	
Đơn vị chủ trì	<pre> graph TD     Start --&gt; Prep     Prep --&gt; Build     Build --&gt; Prepare     Prepare --&gt; Execute     Execute --&gt; End     </pre> <p>- Báo cáo, đúc rút kinh nghiệm - Giám sát các đơn vị liên quan cập nhật, hồ sơ tài liệu (nếu có)</p>	





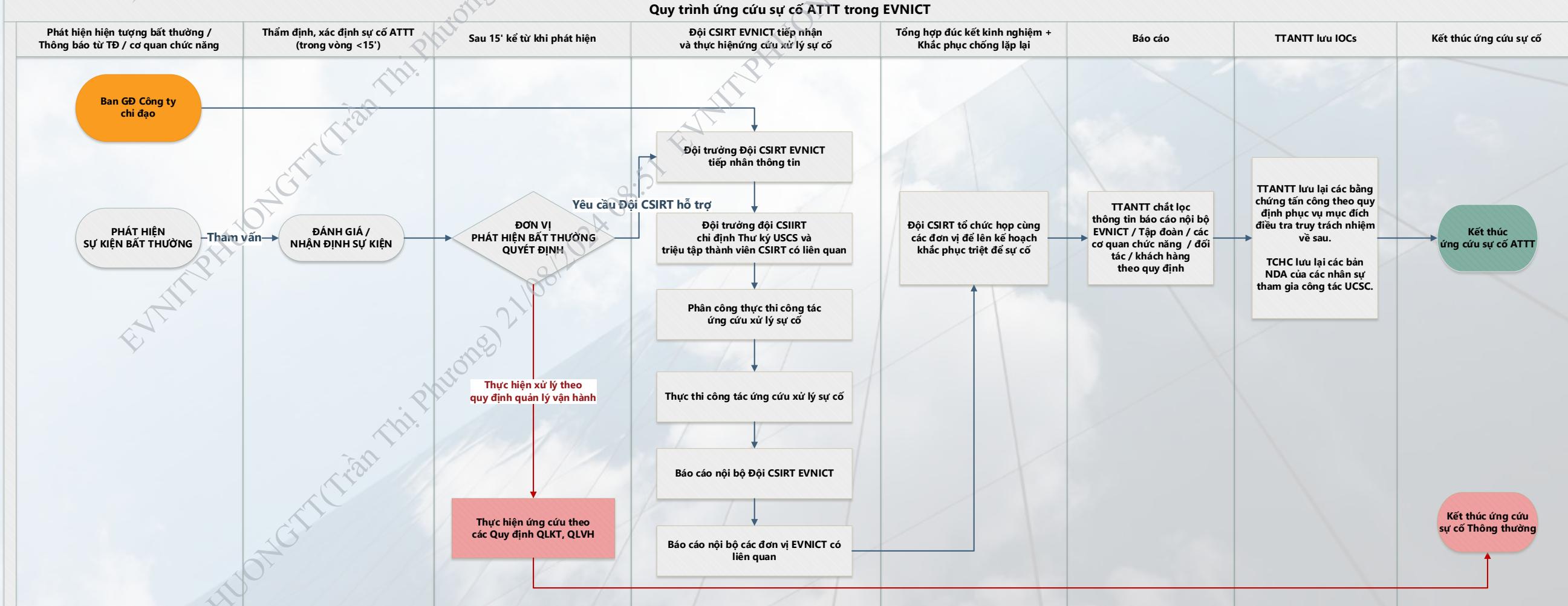
EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# SƠ ĐỒ QUY TRÌNH ỨNG CỨU XỬ LÝ SỰ CỐ ATTT

## (Quy định số 101/QĐ-EVNICT)

3





EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# TRÁCH NHIỆM ĐẢM BẢO ATTT

## Thành viên BCĐ ATTT (QĐ 1087/QĐ-EVNICT)

3

### 1. Lãnh đạo về Hệ thống quản lý ATTT

- Chịu trách nhiệm trực tiếp về việc chỉ đạo, tổ chức triển khai áp dụng, duy trì và cải tiến liên tục hệ thống quản lý ATTT đảm bảo an toàn thông tin trong các hoạt động thuộc phạm vi hệ thống quản lý ATTT của Công ty.

### 3. Phụ trách TTTT chính sách, quy định và kiểm tra đánh giá

- Tiến hành theo dõi, kiểm tra và đánh giá các đơn vị/ cá nhân trong việc tuân thủ thực hiện. Tập hợp thông tin và lập báo cáo kết quả đánh giá, lưu trữ hồ sơ, tài liệu theo việc thực thi các chính sách quy định biện pháp kiểm soát được phân công. Căn cứ kế hoạch hoạt động ATTT hàng năm, chủ trì hoặc phối hợp triển khai áp dụng các chính sách quy định, biện pháp kiểm soát được phân công.
- Xây dựng, đề xuất cải tiến, hiệu chỉnh các chính sách/ quy định ATTT trong quá trình triển khai áp dụng và phù hợp với thực tế hoạt động của EVNICT.
- Xây dựng kế hoạch duy trì, áp dụng HTQL ATTT của công ty hằng năm.
- Điều phối, hướng dẫn mạng lưới PTATTT hoạt động trong công ty
- Đầu mối phụ trách về pháp chế trong ban ATTT.

### 2. Thành viên chỉ đạo An toàn thông tin

- Đề nghị lên Giám đốc phê duyệt ban hành các chính sách ATTT, các văn bản cần thiết cho hoạt động triển khai áp dụng, duy trì và cải tiến hệ thống quản lý ATTT.
- Chịu trách nhiệm trực tiếp về việc chỉ đạo, tổ chức triển khai áp dụng, duy trì và cải tiến liên tục hệ thống quản lý ATTT đảm bảo an toàn thông tin, xử lý các vấn đề an ninh bảo mật trong các hoạt động thuộc phạm vi của Đơn vị quản lý.

### 4. Phụ trách ATANTT tại đơn vị/bộ phận

- Đầu mối triển khai áp dụng hệ thống quản lý ATTT và các chính sách, quy định, quy trình về ATTT mà Công ty đã ban hành.
- Đánh giá, đề xuất cải tiến, hiệu chỉnh các chính sách, biện pháp kiểm soát ATTT trong quá trình triển khai áp dụng và phù hợp với thực tế hoạt động của EVNICT.
- Phối hợp với các Đoàn đánh giá thực hiện đánh giá nội bộ, đánh giá giám sát, đánh giá cấp nhứng nhận.
- Đôn đốc, nhắc nhở, hướng dẫn CBCNV trong đơn vị chấp hành nghiêm chỉnh các quy định về an toàn thông tin, bảo quản các phương tiện lưu trữ và xử lý thông tin an toàn, bảo vệ thông tin cá nhân.



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# TRÁCH NHIỆM ĐẢM BẢO ATTT

3

## 1. TCHC:

- ✓ Hướng dẫn, nguyên tắc quản lý văn bản mật (tiếp nhận và soạn thảo, phát hành)
- ✓ Xây dựng kế hoạch đào tạo, tập huấn về an toàn thông tin hàng năm: a) CBCNV/Người dung, b) Cán bộ quản lý, c) Cán bộ công nghệ thông tin, d) Cán bộ chuyên trách công tác ATTT;
- ✓ Xây dựng yêu cầu, trách nhiệm bảo đảm an toàn, an ninh thông tin đối với từng **vị trí chức danh công việc** và phổ biến đến toàn thể CBCNV.
- ✓ Trong **Quyết định giao nhiệm vụ** hoặc **Hợp đồng lao động** phải có các điều khoản về trách nhiệm đảm bảo an toàn, bảo mật thông tin của người được giao nhiệm vụ trong và sau khi làm việc tại đơn vị
- ✓ Thực hiện ký **Cam kết đảm bảo an toàn thông tin (NDA)**: a) đội ngũ quản trị hệ thống thông tin, b) toàn thể cán bộ CNV, c) nhân viên của đối tác, nhà thầu, nhà cung cấp.

- ✓ Khi chấm dứt hợp đồng phải thực hiện:
  - Yêu cầu cá nhân bàn giao và lập biên bản bàn giao tài sản CNTT.
  - Thu hồi ngay quyền truy cập HTTT của cá nhân nghỉ việc. Thay đổi kịp thời quyền truy cập HTTT của cá nhân thay đổi công việc bảo đảm nguyên tắc quyền vừa đủ để thực hiện nhiệm vụ được giao.
  - Rà soát, kiểm tra đối chiếu định kỳ tối thiểu ba (03) tháng một lần giữa bộ phận quản lý nhân sự và bộ phận quản lý cấp phát, thu hồi quyền truy cập HTTT.
- ✓ Đảm bảo không kết nối mạng đối với máy tính sử dụng để đọc, soạn thảo, lưu trữ, in ấn văn bản thuộc bí mật Nhà nước;
- ✓ Quy định thời gian lưu trữ **dữ liệu camera** là 30 ngày, hoạt động kiểm tra giám sát vận hành của hệ thống camera nhằm đảm bảo an ninh dữ liệu khi cần truy xuất
- ✓ **Con dấu** phải được giao bằng văn bản của người có thẩm quyền cho cán bộ văn thư quản lý và sử dụng

# TRÁCH NHIỆM ĐẢM BẢO ATTT

3

## 2. KT:

- ✓ Chủ trì, **đầu mối** tổ chức triển khai áp dụng, duy trì và cải tiến Hệ thống quản lý an toàn thông tin trong công ty (tiêu chuẩn ISO/IEC 27001, tiêu chuẩn liên quan)
- ✓ Căn cứ trên các văn bản pháp quy có liên quan, thực hiện **thẩm định** các nội dung của Kế hoạch ứng phó sự cố ATTT mạng theo các tiêu chí.
- ✓ **Thẩm định** toàn bộ việc mở kết nối đến các hệ thống như mở tường lửa thế hệ mới (NGFW), cổng truy nhập web an toàn (SWG), tường lửa ứng dụng web (WAF), bảo mật cơ sở dữ liệu (DBS)...
- ✓ Phối hợp TCHC xây dựng yêu cầu **bài giảng đào tạo, tập huấn về an toàn thông tin** hàng năm.
- ✓ Phòng Kỹ thuật chịu trách nhiệm về các **rủi ro** thuộc về công tác thiết kế, quy hoạch, lựa chọn công nghệ tồn tại quá ba (03) tháng.
- ✓ Tham gia ứng cứu sự cố, thành viên đội CSIRT.

## 3. GPCN

- Tham gia ứng cứu sự cố, thành viên đội CSIRT
- Xây dựng Kế hoạch ứng phó sự cố ATTT mạng cho hệ thống do mình quản lý vận hành (bao gồm RTO, RPO)
- Đảm bảo cách ly Internet đối với các máy tính người sử dụng của các hệ thống thông tin quan trọng của Tập đoàn: Hệ thống thu thập và xử lý dữ liệu công tơ điện tử EVNHES.
- Đảm bảo ATTT hệ thống EVNHES/ hệ thống do phòng quản lý tương tự như các dự án của TPM mục “6. TPM”
- Đơn vị vận hành chịu trách nhiệm về các rủi ro về an toàn bảo mật thông tin tồn tại trong hệ thống quá ba (03) tháng kể từ thời điểm có bản vá khắc phục, có văn bản hướng dẫn khắc phục từ các đơn vị, có thông báo bằng văn bản từ EVN/ cơ quan chức năng,
- Chịu trách nhiệm về các rủi ro thuộc về công tác thiết kế, quy hoạch, lựa chọn công nghệ tồn tại quá ba (03) tháng.



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# TRÁCH NHIỆM ĐẢM BẢO ATTT

3

## 4. TT ANTT:

- ✓ TTANTT là đơn vị tổng hợp, chắt lọc thông tin, lập **báo cáo** Tập đoàn, đơn vị thuê vận hành, các cơ quan nhà nước có thẩm quyền (nếu EVN yêu cầu xây dựng dự thảo) theo quy định có trong QĐ 1828 và QĐ 99.
- ✓ Thực hiện giám sát công tác quản lý rủi ro toàn bộ các điểm yếu kỹ thuật/ lỗ hổng bảo mật (Vul/ CVE) trên hệ thống thông tin. Xây dựng quy trình hướng dẫn kiểm soát, khắc phục Vul/CVE.
- ✓ Thông tin tình báo/ tri thức về **mối đe dọa, nguy cơ** cung cấp sớm thông tin về các mối đe dọa để chuẩn bị các phương án xử lý, ứng phó.
- ✓ Vận hành giám sát, xử lý ATTT theo mô hình **SOC** (SECURITY OPERATION CENTER).
- ✓ TTANTT chịu trách nhiệm về **các rủi ro** về an toàn bảo mật thông tin tồn tại trong hệ thống quá ba (03) tháng kể từ thời điểm có các dấu hiệu cảnh báo trên hệ thống giám sát, hoặc có cảnh báo của EVN/ các cơ quan chức năng, hoặc có thông báo về hiện tượng bất thường từ phía các đơn vị.
- ✓ Tiếp nhận yêu cầu hỗ trợ và thực hiện **điều tra** phát hiện sự cố trong trường hợp Ban Giám đốc Công ty, Đơn vị chủ trì dịch vụ, Đơn vị vận hành, người dùng cuối phát hiện các hiện tượng bất thường trong hệ thống.

- ✓ TTANTT trình Giám đốc Công ty phê duyệt **kế hoạch diễn tập** cho năm kế tiếp trong tháng 10 hàng năm.
- ✓ **Sử dụng các công cụ** được trang bị giám sát liên tục nhằm phát hiện kịp thời các hiện tượng bất thường trong hệ thống nghi ngờ là sự cố ATTT.
- ✓ Lập và cập nhật tối thiểu một năm một lần các kế hoạch và danh mục kiểm tra đánh giá **tính sẵn sàng và tuân thủ** về an toàn thông tin và năng lực sẵn sàng ứng cứu sự cố vào tháng 10 hàng năm.
- ✓ Toàn bộ các trang thiết bị (như: máy tính, thiết bị mạng, thiết bị an ninh bảo mật...) được huy động tham gia điều tra phân tích, ứng cứu, xử lý sự cố đều phải được TTANTT **kiểm tra, đánh giá, đảm bảo** không tồn tại mã độc, đảm bảo không đưa thêm rủi ro vào hệ thống.
- ✓ Toàn bộ phần mềm được cài đặt thêm, chạy trực tiếp, chạy từ xa phục vụ cho mục đích phân tích mã độc, rà soát mã độc, rà soát lỗ hổng, kiểm thử xâm nhập, trích xuất dữ liệu... phải được TTANTT **kiểm tra đánh giá** và giám sát liên tục quá trình thực hiện.



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# TRÁCH NHIỆM ĐẢM BẢO ATTT

3

## 5. TTHT:

- ✓ Xây dựng Kế hoạch ứng phó sự cố ATTT mạng cho hệ thống do mình quản lý vận hành (bao gồm RTO, RPO)
- ✓ TTHT xây dựng các nội dung liên quan đến sự cố do lỗi của hệ thống phần cứng, phần mềm hạ tầng CNTT, điều kiện môi trường, do người quản trị vận hành.
- ✓ Thực thi ngay các biện pháp đã có sẵn trong Kế hoạch ứng phó sự cố ATTT mạng nếu nghi ngờ có sự cố ATTT
- ✓ Phối hợp TCHC: Thu hồi, thay đổi ngay **quyền truy cập HTTT** của cá nhân nghỉ việc, thay đổi công việc. Rà soát, kiểm tra đổi chiếu định kỳ tối thiểu ba (03) tháng một lần.
- ✓ Tham gia **diễn tập** đánh giá phương án phòng ngừa, xử lý và khắc phục sự cố.
- ✓ Văn bản hóa và thực hiện các quy tắc về update hệ thống, cập nhật bản vá, các quy tắc về đặt mật khẩu, thiết lập chính sách log, antivirus (để nâng cao tính bảo mật cho một hệ thống bằng các quy tắc, các thiết lập bảo mật, (**System Hardening**).
- ✓ Tài khoản hệ thống phải được giao đích danh cá nhân làm công tác quản trị. Hạn chế tối đa dùng chung tài khoản quản trị
- ✓ Phải **rà soát hệ thống tài khoản** hàng năm, đảm bảo các tài khoản và quyền truy cập hệ thống được cấp phát đúng. Các tài khoản không sử dụng/truy cập trong thời gian 06 tháng phải bị khóa hoặc xóa bỏ (sau khi có thông báo với đơn vị/người sử dụng).
- ✓ Đảm bảo cách ly Internet đối với toàn bộ các máy chủ, máy tính quản trị của các HTTT.
- ✓ Vô hiệu hóa các chức năng truy cập từ xa không an toàn đối với HTTT từ Cấp độ 3 trở lên.
- ✓ Cập nhật bản vá HĐH, ứng dụng cho các máy chủ các HTTT, khắc phục Vul/CVE.
- ✓ Đơn vị vận hành chịu trách nhiệm về các rủi ro về an toàn bảo mật thông tin tồn tại trong hệ thống quá ba (03) tháng kể từ thời điểm có bản vá khắc phục, có văn bản hướng dẫn khắc phục từ các đơn vị, có thông báo bằng văn bản từ EVN/ cơ quan chức năng, ...



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# TRÁCH NHIỆM ĐẢM BẢO ATTT

3

## 6. TPM:

- Xây dựng **Kế hoạch ứng phó sự cố ATTT** mạng cho hệ thống do mình quản lý vận hành (bao gồm RTO, RPO)
- *TPM xây dựng các nội dung liên quan đến sự cố do các lỗi của phần mềm/dịch vụ do TPM chủ trì phát triển, phục vụ cho công tác phát triển phần mềm, chăm sóc khách hàng sử dụng phần mềm.*
- Thực thi ngay các biện pháp đã có sẵn trong Kế hoạch ứng phó sự cố ATTT mạng nếu nghi ngờ có sự cố ATTT.
- Tham gia **diễn tập** đánh giá phương án phòng ngừa, xử lý và khắc phục sự cố.
- **Tài khoản hệ thống** phải được giao đích danh cá nhân làm công tác quản trị. Hạn chế tối đa dùng chung tài khoản quản trị
- Phải rà soát hệ thống tài khoản hàng năm, đảm bảo các tài khoản và quyền truy cập hệ thống được cấp phát đúng. Các tài khoản không sử dụng/truy cập trong thời gian 06 tháng phải bị khóa hoặc xóa bỏ (sau khi có thông báo với đơn vị/người sử dụng).
- ✓ Phải tiến hành **phân tích, xác định rủi ro** có thể xảy ra, đánh giá phạm vi tác động và phải chuẩn bị các biện pháp hạn chế, loại trừ các rủi ro này khi tiếp nhận, phát triển, nâng cấp, bảo trì HTTT
  - Đảm bảo cách ly Internet đối với toàn bộ các máy chủ, máy tính quản trị của các HTTT
  - Vô hiệu hóa các chức năng truy cập từ xa không an toàn đối với HTTT từ Cấp độ 3 trở lên.
  - Phải có **biên bản đánh giá ATTT** sau khi kết thúc mỗi công đoạn thiết kế, xây dựng, kiểm thử, triển khai và vận hành sử dụng phần mềm.
  - Tách biệt cổng giao tiếp quản trị phần mềm ứng dụng với cổng giao tiếp cung cấp dịch vụ; đóng các cổng giao tiếp không sử dụng.
  - Chỉ cho phép sử dụng các giao thức mạng có hỗ trợ chức năng mã hóa thông tin như SSH, SSL, VPN hoặc tương đương khi truy nhập, quản trị phần mềm, ứng dụng từ xa trên môi trường mạng;
  - Phần mềm, ứng dụng cần được kiểm tra phát hiện và **khắc phục các điểm yếu về an toàn, an ninh thông tin** trước khi đưa vào sử dụng và trong quá trình sử dụng.
  - Đơn vị vận hành chịu trách nhiệm về các rủi ro về an toàn bảo mật thông tin tồn tại trong hệ thống quá ba (03) tháng kể từ thời điểm có bản vá khắc phục, có văn bản hướng dẫn khắc phục từ các đơn vị, có thông báo bằng văn bản từ EVN/ cơ quan chức năng, ...



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# TRÁCH NHIỆM ĐẢM BẢO ATTT

3

## 7. QLĐTXD:

Bổ sung nội dung xem xét **đánh giá ANBM** trong Biên bản nghiệm thu hoàn thành công trình.

**Thuyết minh đề xuất cấp độ**, lồng ghép vào nội dung của báo cáo nghiên cứu khả thi, dự án khả thi ứng dụng công nghệ thông tin hoặc báo cáo đầu tư của dự án, thẩm định, trình phê duyệt báo cáo nghiên cứu khả thi.

Thực hiện **xem xét lại các vấn đề về ATTT** trong tất cả các hợp đồng, dự án định kì 1 lần/ 1 năm.

**Thỏa thuận bảo mật, không tiết lộ thông tin** với từng đối tác, nhà cung cấp.

Quản lý hồ sơ liên quan đến các gói thầu.

## 8. TKDV

Định kỳ kiểm tra **cam kết chất lượng dịch vụ (SLA)** trong các hợp đồng, lưu hồ sơ, báo cáo đánh giá.

Thực hiện đo lường và **giám sát thời gian xử lý** các issue trên Sdp đúng với cam kết trong HD

Thường xuyên công tác **tuyên truyền, phổ biến nâng cao nhận thức** cho người dùng tại đơn vị về bảo đảm ATTT: phát hành sổ tay ATTT, bảng tin, hội thảo

# TRÁCH NHIỆM ĐẢM BẢO ATTT

## 9. TCKT:

- Các **hồ sơ, tài liệu** quan trọng phục vụ hoạt động nghiệp vụ cần được **bảo vệ** khỏi bị mất mát, phá hủy, giả mạo, truy nhập và công bố trái phép. Để đảm bảo tuân thủ quy định của pháp luật, quy định của EVN, hợp đồng.
- Quản lý trong suốt vòng đời phương tiện lưu trữ thông tin dữ liệu, kể từ khi **mua sắm**, sử dụng, vận chuyển và **hủy bỏ**.
- Tất cả các dữ liệu nhạy cảm, license phần mềm chứa trong các thiết bị xử lý thông tin trước khi **thanh lý** hoặc tái sử dụng phải được xóa triệt để. để phòng ngừa việc lộ lọt thông tin quan trọng khi thực hiện loại bỏ hoặc tái sử dụng thiết bị.

## 10. KH:

- **Giao các nhiệm vụ triển khai ATTT** vào kế hoạch thực hiện của các đơn vị.
- Đánh giá hoàn thành nhiệm vụ về thực hiện công tác ATTT các đơn vị.
- Đảm bảo ATTT trong quá trình thanh lý, hủy bỏ thiết bị, phương tiện lưu trữ và xử lý thông tin, dữ liệu.
- Phối hợp TCHC lập biên bản bàn giao tài sản CNTT.
- Giao, gắn trách nhiệm cụ thể cho cá nhân hoặc tập thể **quản lý, sử dụng tài sản, trang thiết bị công nghệ thông tin**.



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# PHẦN 4

## QUY TẮC ĐẢM BẢO ATTT ĐỐI VỚI NGƯỜI SỬ DỤNG



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# QUY TẮC ĐẢM BẢO ATTT

## Sử dụng tài khoản và mật khẩu đúng cách

4



### NGUY CƠ VÀ RỦI RO

- Kẻ gian có thể mạo danh người dùng để lấy cắp thông tin nếu sử dụng mật khẩu quá đơn giản (ví dụ: 123456, abc123,...) hoặc quản lý chúng một cách cẩu thả (ví dụ: ghi lại mật khẩu trên giấy và dán vào máy tính, bàn làm việc,...)
- Sử dụng cùng một tài khoản/mật khẩu cho nhiều trang Web khác nhau sẽ làm tăng nguy cơ trở thành nạn nhân cho tấn công mạng vào các trang khác, nếu một trang bị lộ lọt thông tin



### BIỆN PHÁP BẢO VỆ

- Đặt mật khẩu mạnh, có đủ độ phức tạp. Thường xuyên thay đổi mật khẩu, ít nhất 3 tháng đổi mật khẩu một lần.
- Không chia sẻ mật khẩu cho người khác, không sử dụng cùng một mật khẩu cho nhiều ứng dụng khác nhau.
- Không lưu mật khẩu khi truy cập các trang Web tại các máy tính công cộng hoặc các máy tính của người khác.
- Không đặt chế độ lưu giữ mật khẩu hoặc tự động đăng nhập trong các ứng dụng, trình duyệt khi làm việc với các hệ thống thông tin quan trọng, trọng yếu.
- Nếu bắt buộc phải đăng nhập vào ứng dụng trên các máy tính công cộng hoặc máy tính của người khác thì nên sử dụng bàn phím ảo để nhập mật khẩu hoặc các thông tin quan trọng.



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# QUY TẮC ĐẢM BẢO ATTT

## Thiết lập máy tính cá nhân an toàn

4



### NGUY CƠ VÀ RỦI RO

- Các máy tính mới mua hay mới được cài đặt lại thường chưa được cập nhật các bản vá lỗi, cũng như chưa được thực hiện các thiết lập an toàn cần thiết, kẻ xấu có thể lợi dụng các lỗ hổng để tấn công khai thác thông tin.
- Việc truy cập trái phép vào máy tính có thể làm thất thoát thông tin cá nhân hoặc bị lợi dụng làm bước đệm để tấn công vào máy tính khác



### BIỆN PHÁP BẢO VỆ

- Tất cả máy tính phải được đặt mật khẩu truy cập và đổi mật khẩu thường xuyên.
- Nên gỡ bỏ các chương trình không cần thiết được cài đặt sẵn đối với máy tính mới.
- Kích hoạt tính năng tường lửa bảo vệ cá nhân trên máy tính trước khi kết nối đến bất kỳ mạng máy tính nào.
- Cài đặt phần mềm diệt virus và cập nhật thường xuyên.
- Nâng cấp phần mềm ứng dụng và hệ điều hành máy tính, các trình duyệt Web để được cập nhật các bản vá lỗi bảo mật mới nhất.
- Không dùng các công cụ, phần mềm bẻ khóa do chúng thường chứa virus/mã độc.
- Nên đăng xuất khỏi tài khoản đã truy cập hoặc khóa màn hình làm việc trước khi rời khỏi máy tính. Thiết lập chế độ màn hình chờ có mật khẩu bảo vệ sau 5 đến 10 phút không sử dụng máy tính.



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# QUY TẮC ĐẢM BẢO ATTT

## Sử dụng email, nhận biết và phòng chống thư rác, thư giả mạo

4



### NGUY CƠ VÀ RỦI RO

- Việc mở tệp đính kèm hay nhập chuột vào một đường dẫn gửi kèm trong thư điện tử giả mạo có thể làm máy tính bị nhiễm virus hay bị dẫn tới một trang Web giả mạo nhằm đánh cắp thông tin hoặc bị lợi dụng là nơi để phát tán thư rác.
- Địa chỉ email bị lợi dụng để phát tán thư rác, do được thu thập từ việc tham gia dịch vụ tặng quà giả mạo trên mạng hoặc qua các thông báo không có thật về việc cắt các dịch vụ dùng thử trên mạng.



### BIỆN PHÁP BẢO VỆ

- Chỉ sử dụng email của EVN để trao đổi nội dung liên quan đến công việc. Không sử dụng địa chỉ mail EVN và các email quan trọng để đăng ký trên các trang web/dịch vụ không rõ nguồn gốc.
- Cẩn trọng với các email có tiêu đề nhạy cảm (như: thanh toán hóa đơn, tiền lương, bổ nhiệm cán bộ,...).
- Cần kiểm tra kỹ địa chỉ email nhận được để đảm bảo rằng tên hiển thị người gửi đúng với địa chỉ email của người mà mình biết.
- Khi nhận được email nghi ngờ giả mạo: Không mở các tập tin hay đường liên kết đáng ngờ gửi kèm. Cẩn thận, cân nhắc khi tải về các file đính kèm trong email: các file đính kèm lạ có phần mở rộng bất thường như .exe, .dll, .bat... Nếu đã chót mở các tập tin hay đường liên kết đáng ngờ, hãy ngắt kết nối mạng và liên hệ với bộ phận hỗ trợ của EVNICT để được hỗ trợ.
- Nhận diện các email spam - email quảng cáo: Nếu gặp các email này thì thực hiện chặn người gửi (Block sender) và xóa vĩnh viễn khỏi hộp thư; hoặc báo cho bộ phận hỗ trợ của EVNICT.



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

## QUY TẮC ĐẢM BẢO ATTT

# An toàn khi sử dụng mạng không dây (wifi) tại nơi công cộng

4



### NGUY CƠ VÀ RỦI RO

1. Các hoạt động trên Internet của người dùng tại các mạng không dây thiếu an toàn có thể bị kẻ xấu theo dõi, đánh cắp các thông tin quan trọng (mật khẩu, các thông tin cá nhân, thông tin thẻ tín dụng...)
2. Một số trường hợp có thể bị lợi dụng để thực thi những hành động bất hợp pháp hoặc làm bước đệm để tấn công vào các hệ thống khác.



### BIỆN PHÁP BẢO VỆ

1. Khi sử dụng mạng không dây ở nơi công cộng, cần tắt tính năng chia sẻ file trước khi sử dụng dịch vụ. Khi cần truy cập vào các hệ thống ứng dụng riêng của EVN thì nên sử dụng VPN.
2. Tắt bỏ chức năng tự động kết nối mạng không dây. Khi chức năng này được bật, mỗi khi thiết bị ở trong phạm vi của mạng không dây, thiết bị đó sẽ tự động kết nối, tạo cơ sở để kẻ xấu lợi dụng lấy cắp dữ liệu người dùng.



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# QUY TẮC ĐẢM BẢO ATTT

## Sử dụng mạng xã hội an toàn

4



### NGUY CƠ VÀ RỦI RO

- Thông tin cá nhân dễ dàng bị lộ một cách vô ý thức, bị kẻ xấu lợi dụng làm ảnh hưởng tới hình ảnh, uy tín của bản thân
- Kẻ xấu giả danh bạn bè lừa đảo (mượn tiền, nạp thẻ di động ...).
- Việc vô tình đăng tin sai sự thật trên các trang mạng xã hội có thể dẫn đến hậu quả phải bồi thường thiệt hại, bị phạt, thậm chí bị bắt giữ vì vi phạm luật pháp.



### BIỆN PHÁP BẢO VỆ

- Bảo mật thông tin cá nhân trên mạng: không tiết lộ số điện thoại, địa chỉ, lịch công tác, thông tin liên quan tới công việc ở cơ quan; đặt chế độ cá nhân hoặc chỉ bạn bè thân thiết và tin cậy mới có thể xem để tránh trường hợp bị kẻ xấu lợi dụng những thông tin đó để uy hiếp, đe dọa.
- Hạn chế chia sẻ thông tin cá nhân lên mạng xã hội (MXH), cố gắng hạn chế công khai các thông tin có tính liên kết, xâu chuỗi với nhau.
- Chỉ kết bạn với những người thân, quen biết ở ngoài đời. Xác minh với bạn bè, người thân qua điện thoại hoặc gặp mặt trước khi kết bạn trên MXH.
- Kiểm tra kỹ yêu cầu của bạn bè gửi trên MXH khi liên quan đến tài chính (mượn tiền, nạp thẻ di động ...).
- Không nhấn vào bất kỳ một đường link nào có dấu hiệu bất thường hoặc được gửi từ một người mà bạn không quen biết.
- Xin phép bạn bè mình trước khi đăng những bức ảnh và câu chuyện của họ.



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# QUY TẮC ĐẢM BẢO ATTT

## Sử dụng Internet truy cập vào các trang Web

4



### NGUY CƠ VÀ RỦI RO

1. Máy tính bị nhiễm các mã độc hại, virus, trojan
2. Bị nghe lén trên mạng
3. Mất cảnh giác và cung cấp thông tin lên mạng Internet
4. Bạn có thể trở thành nạn nhân của những lừa đảo trực tuyến.
5. Bị làm phiền khi lướt web, popup, banner quảng cáo



### BIỆN PHÁP BẢO VỆ

1. Thận trọng khi truy cập Internet: Thông thường các trang Web bắt đầu bằng https (có biểu tượng khóa) là trang web an toàn.
2. Nhận biết website, link an toàn: Rê chuột vào đường link nhưng không bấm để xem trước đường link. Nếu đường link này lạ lẫm, bạn không nên click vào.
3. Không truy cập các trang Web có nội dung nhạy cảm, không lành mạnh, câu view.
4. Không chia sẻ thông tin cá nhân, tổ chức (các tài liệu nội bộ của EVN, hướng dẫn chuyên môn, văn bản...) lên Internet.
5. Đối với các trang web cần tài khoản truy cập, đặt mật khẩu đủ mạnh.
6. Không cài các phần mềm lạ, Toolbar quảng cáo
7. Lướt Web an toàn ở các điểm truy cập Internet công cộng: Sử dụng bàn phím ảo khi gõ mật khẩu. Để mở bàn phím ảo có sẵn của Windows, bạn mở hộp thoại Run (hoặc bấm phím Windows + R), gõ OSK và Enter để mở bàn phím ảo.



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# QUY TẮC ĐẢM BẢO ATTT

## Sử dụng ổ cứng di động, USB

4



### NGUY CƠ VÀ RỦI RO

- Bị lây nhiễm mã độc
- Bị virus/malware mã hóa dữ liệu để tống tiền
- Bị lộ thông tin nhạy cảm



### BIỆN PHÁP BẢO VỆ

- Quét virus thiết bị lưu trữ di động như ổ cứng di động, USB, thẻ nhớ SD... trước khi sử dụng.
- Đối với các dữ liệu quan trọng nên sử dụng biện pháp để mã hóa dữ liệu.
- Hạn chế mượn hoặc cho mượn thiết bị lưu trữ di động. Nếu cần phải cho mượn thì nên xóa sạch dữ liệu (format) trước khi cho người khác mượn sử dụng.
- Đối với các dữ liệu quan trọng, nên sao lưu dự phòng các dữ liệu trên nhiều thiết bị khác nhau.



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# QUY TẮC ĐẢM BẢO ATTT

## Phòng chống virus, mã độc

4



### NGUY CƠ VÀ RỦI RO

1. Mã độc xâm nhập vào máy tính có thể đánh cắp dữ liệu người dùng như các thông tin nhạy cảm, riêng tư, thông tin của cơ quan...
2. Nhiều mã độc thực hiện phá hoại dữ liệu, mã hóa dữ liệu người dùng, đòi hỏi người dùng phải trả chi phí để lấy lại dữ liệu
3. Tạo bàn đạp để tấn công vào máy tính khác



### BIỆN PHÁP BẢO VỆ

1. Sử dụng thư điện tử thận trọng. Mã độc thường được lây nhiễm qua các tệp tin đính kèm trong thư điện tử.
2. Thận trọng khi truy cập trang Web lạ được gửi từ những người không quen biết hoặc người quen nhưng có các hành vi bất thường.
3. Không sử dụng các phần mềm bẻ khóa (crack), không bản quyền



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# QUY TẮC ĐẢM BẢO ATTT

## Đảm bảo an toàn thông tin khi truy cập các hệ thống thông tin của EVN/EVNICT

4



### NGUY CƠ VÀ RỦI RO

1. Bị khai thác, rò rỉ các thông tin quan trọng gây thiệt hại, ảnh hưởng đến uy tín, danh dự, hình ảnh của EVN



### BIỆN PHÁP BẢO VỆ

1. Tuyệt đối Không sử dụng các thiết bị găng ngoài như USB, đầu đọc thẻ nhớ, thẻ nhớ trên các máy tính kết nối mạng OT.
2. Khi cần truy cập vào các hệ thống ứng dụng riêng của EVN/EVNICT thì nên sử dụng VPN.



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# QUY TẮC ĐẢM BẢO ATTT

## Đảm bảo an toàn khi sử dụng các ứng dụng họp trực tuyến

4



### NGUY CƠ VÀ RỦI RO

1. Ứng dụng có tồn tại các lỗ hổng bảo mật cho phép tin tặc đánh cắp thông tin cá nhân, chèn các liên kết độc hại, chiếm quyền điều khiển, chèn các nội dung không phù hợp, tấn công kiểm soát micro, camera, đánh cắp video trực tuyến...
2. Ứng dụng tự động thu thập thông tin và bí mật chia sẻ dữ liệu của người dùng cho các bên thứ ba mà không có sự cho phép của người dùng.
3. Các tin tặc đăng ký các tên miền giả mạo các ứng dụng họp trực tuyến nhằm phát tán các tệp tin độc hại, giả mạo ứng dụng của chính hãng để lừa người dùng tải và cài đặt trên thiết bị của mình. Ví dụ room.us, zoom.xyz ...



### BIỆN PHÁP BẢO VỆ

1. Nghiên cứu kỹ trong lựa chọn sử dụng các ứng dụng, tránh cài đặt, sử dụng các ứng dụng đang bị cảnh báo tồn tại lỗ hổng, điểm yếu bảo mật;
2. Tải và cài đặt ứng dụng từ các nguồn chính thống; thường xuyên cập nhật bản vá lỗ hổng của các ứng dụng và hệ điều hành.
3. Khi sử dụng các ứng dụng trực tuyến cần sử dụng các kênh, phòng riêng, có mật khẩu bảo vệ, xác thực người tham gia; không chia sẻ các thông tin về phòng họp (ID, mật khẩu, thời gian họp...) trên không gian mạng; không tải, mở các tệp tin, đường dẫn lạ không rõ nguồn gốc...
4. Không sử dụng các ứng dụng trực tuyến để trao đổi, gửi nhận các dữ liệu bí nhặt nhà nước, dữ liệu nội bộ của đơn vị.



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# QUY TẮC ATTT: NHỚ VÀ TUÂN THỦ

## Quy định an toàn thông tin trong quản lý nhân sự, người dùng

4



### Quản lý nhân sự, người dùng

- Việc thẩm định thông tin của ứng viên và nhân viên đối tác được tiến hành trước thời điểm bắt đầu làm việc, phù hợp với các yêu cầu đảm bảo ATTT của EVNICT.
- Các cán bộ, nhân viên của EVNICT và các nhân viên đối tác khi tham gia vào hoạt động của EVNICT phải ký cam kết bảo mật an toàn thông tin.
- Tất cả các cán bộ, nhân viên được đào tạo, nâng cao nhận thức về chính sách và quy định ATTT của EVNICT. Tất cả các nhân viên mới khi được tiếp nhận đều phải tham gia và đạt yêu cầu của khóa đào tạo hội nhập trong đó có đào tạo về an toàn thông tin trong EVNICT.
- Cán bộ, nhân viên EVNICT/ đối tác nào vi phạm chính sách ATTT thì bị xử lý vi phạm theo quy định.
- Thu hồi quyền sử dụng tài sản thông tin (máy tính, điện thoại, tài liệu, tài khoản, thẻ nhân viên...) khi một nhân sự bị buộc thôi việc, nghỉ việc hoặc thuyên chuyển công tác.
- Khi cán bộ, nhân viên đã chấm dứt hợp đồng lao động với EVNICT thì thỏa thuận/cam kết về ATTT trong hợp đồng, thỏa thuận lao động đã ký với EVNICT vẫn còn hiệu lực.
- Đeo thẻ nhân viên trong văn phòng và phòng máy của EVNICT.
- Đóng cửa sau khi ra/vào, khi không có ai trong phòng.



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# QUY TẮC ATTT: NHỚ VÀ TUÂN THỦ

## Quy định an toàn thông tin về quản lý tài sản và trang thiết bị

4



### Quản lý tài sản và trang thiết bị

1. Từng cán bộ nhân viên được giao tài sản thông tin có trách nhiệm bảo quản, sử dụng đúng mục đích, đảm bảo an toàn thông tin cho tài sản thông tin đó.
2. Tất cả các cán bộ nhân viên cũng như những người dùng tài sản thông tin phải bàn giao tài sản thông tin khi chấm dứt công việc, hợp đồng lao động hoặc hết thỏa thuận với đơn vị.
3. Các máy tính xách tay cấp cho cá nhân quản lý, sử dụng phải đảm bảo được bàn giao theo đúng biên bản bàn giao thiết bị, sử dụng đúng mục đích, hiệu quả và có các biện pháp bảo vệ thông tin phù hợp như sử dụng tường lửa cá nhân và Antivirus, đặt mật khẩu, ...
4. Khóa thiết bị một cách thích hợp khi chất dứt phiên làm việc.
5. Thoát khỏi các ứng dụng hoặc dịch vụ mạng nếu không cần thiết.
6. Phải bật chế độ khóa màn hình và yêu cầu mật khẩu khi đăng nhập nếu như rời khỏi vị trí làm việc sau một khoảng thời gian 5, 10 phút.
7. Khi in/photo các tài liệu quan trọng phải kiểm soát và đảm bảo không thất thoát hay lộ ra ngoài: đếm trang, hủy bản lõi bằng máy hủy giấy.
8. Khi thay hoặc chuyển nhượng thiết bị cần sao lưu lại toàn bộ dữ liệu quan trọng để đưa vào thiết bị mới. Sau đó xóa toàn bộ các thông tin trên các ứng dụng làm việc và các dữ liệu công việc được lưu trên thiết bị



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# QUY TẮC ATTT: NHỚ VÀ TUÂN THỦ

## Quy định an toàn thông tin về quản lý truy nhập

4



### Quản lý truy nhập

1. Mỗi người dùng hệ thống thông tin trong EVNICT phải có tài khoản và được quản lý, cấp quyền truy nhập tương ứng với các yêu cầu nghiệp vụ:

- Đăng ký tài khoản truy cập vào các hệ thống máy chủ, các hệ thống lưu trữ và xử lý thông tin quan trọng, nhạy cảm phải được sự phê duyệt của các cấp có thẩm quyền.
- Người dùng phải ký thỏa thuận đảm bảo giữ bí mật các thông tin xác thực cá nhân (trong cam kết bảo mật ATTT hay thỏa thuận không tiết lộ thông tin trong hợp đồng).

2. Đảm bảo an toàn thông tin khi sử dụng mật khẩu:

- Người dùng phải đảm bảo giữ bí mật cho mật khẩu cá nhân và mật khẩu hệ thống, ứng dụng mà mình quản lý.
- Không lưu lại mật khẩu lên giấy, tệp tin hoặc thiết bị cầm tay.
- Mật khẩu phải được thay đổi ngay lập tức khi nghi ngờ bị lộ.
- Đặt mật khẩu cần đảm bảo có một mật khẩu mạnh.
- Phải đổi mật khẩu ngay khi nhận được tài khoản cá nhân và mật khẩu tạm thời.
- Mật khẩu là tài sản cá nhân và không được chia sẻ với người khác.
- Tất cả các tài khoản trên máy tính để bàn và máy tính xách tay đều phải đặt mật khẩu; Các cá nhân phải thay đổi mật khẩu 3 tháng/1 lần để đảm bảo an toàn; Không lưu mật khẩu tự động trong quá trình đăng nhập



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# QUY TẮC ATTT: NHỚ VÀ TUÂN THỦ

## Quy định an toàn thông tin trong vận hành

4



### An toàn thông tin trong vận hành

- Trên mặt bàn làm việc trong văn phòng, phòng làm việc khi không có sự kiểm soát của con người thì không được để các giấy tờ, tài liệu quan trọng, các phương tiện lưu trữ thông tin trên mặt bàn.
- Cán bộ, nhân viên EVNICT cần được đào tạo và nhận thức về an toàn vệ sinh lao động, PCCN, PCLB.
- Các vật liệu dễ cháy, nổ, các chất độc hại, văn phòng phẩm phải được đặt đúng nơi quy định, không được phép đặt tại các khu vực có chứa các trang thiết bị xử lý thông tin và các hệ thống thông tin.
- Người bên ngoài EVNICT làm việc trong phòng máy viễn thông, trung tâm dữ liệu phải có cán bộ của EVNICT giám sát trong suốt quá trình làm việc.
- Không sử dụng máy ảnh, máy quay phim, các thiết bị ghi âm trong khu vực an ninh cao (DC, DR/ phòng máy VT, ...) khi không được phép của cấp có thẩm quyền



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# QUY TẮC ATTT: NHỚ VÀ TUÂN THỦ

## Quy định an toàn mạng và trao đổi thông tin

4



### An toàn mạng và trao đổi thông tin

1. Xóa các thông tin quan trọng được lưu trong bộ nhớ của các thiết bị in ấn như máy in, máy photocopy, máy fax ngay sau khi in xong.
2. Người dùng phải chịu trách nhiệm trước Pháp luật và EVNICT về nội dung của những thư được gửi đi từ hộp thư điện tử của mình.
3. Nghiêm cấm Tạo ra và cài đặt các chương trình virus máy tính, phần mềm gây hại vào thiết bị số của người khác.
4. Nghiêm cấm sử dụng các tài nguyên, tài sản thông tin của EVNICT cho các hoạt động trái quy định của pháp luật; nghiêm cấm mua bán, trao đổi thông tin của EVNICT.
5. Hạn chế sử dụng mạng dịch vụ xã hội trực tuyến, trang thông tin điện tử cá nhân không đúng mục đích trong giờ làm việc. Không được phép sử dụng mạng dịch vụ xã hội trực tuyến, trang thông tin điện tử cá nhân thông qua hệ thống Internet vào các mục đích xấu hoặc vi phạm pháp luật.
6. Phải thực hiện quét kiểm tra virus các file tải từ internet trước khi sử dụng.
7. Không được sử dụng các thiết bị thu phát sóng làm ảnh hưởng (nhiều tần số, gián đoạn, giảm chất lượng...) đến mạng wifi của EVNICT.
8. Nghiêm cấm sử dụng công cụ để vượt qua Proxy hoặc Firewall (ví dụ: Free Gate, Ultrasurf,...), giả mạo địa chỉ MAC, IP dưới mọi hình thức, kể cả để phục vụ mục đích công việc.



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# QUY TẮC ATTT: NHỚ VÀ TUÂN THỦ

## Quy định đối với sự cố an toàn thông tin

4



### Sự cố an toàn thông tin

- Phải thông báo kịp thời với bộ phận quản lý sự cố ATTT về việc xảy ra sự kiện an toàn thông tin:
  - Mất mát thiết bị CNTT;
  - Dịch vụ bị ngắt, dịch vụ không hoạt động đúng chức năng;
  - Hệ thống bị quá tải, hệ thống hoạt động không đúng chức năng thông thường;
  - Lỗi sinh ra khi thao tác;
  - Các hành vi không tuân thủ các chỉ dẫn hoặc chính sách an toàn thông tin;
  - Các sơ hở, các lỗi gây mất an toàn vật lý có liên quan đến hệ thống thông tin như: ngập nước, dột, hở điện, hỏng khóa, hỏng thiết bị an ninh, ...
  - Các hoạt động bất thường của mạng, các lỗi của phần mềm gây mất an toàn thông tin.

- Người dùng không được tự ý xử lý, khắc phục sự cố, cho dù có khả năng thao tác thực hiện việc đó.  
Nếu xuất hiện nghi ngờ nhiễm mã độc hại hoặc lỗi phần mềm, người dùng phải làm theo các bước sau:
  - Chú ý đến bất kỳ dấu hiệu nào xuất hiện trên màn hình;
  - Hạn chế sử dụng máy tính và tránh sử dụng ứng dụng nếu có thể;
  - Ngay lập tức thông báo với bộ phận quản lý sự cố CNTT;
  - Không cố gắng đọc dữ liệu trong các thiết bị lưu trữ di động đã bị hư hỏng trên các máy tính khác nhau;
  - Không được phép thử khôi phục lại hệ điều hành, ứng dụng khi không có trách nhiệm.



EVN

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# QUY TẮC ATTT: NHỚ VÀ TUÂN THỦ

## Quy định với thiết bị di động và làm việc từ xa

4



### Thiết bị di động và làm việc từ xa

1. Một số các lưu ý sau phải được thực hiện đối với thiết bị di động:

- Phải sử dụng các biện pháp xác thực khi đăng nhập vào thiết bị làm việc di động tránh việc bất kỳ ai cũng có thể sử dụng thiết bị đó;
- Không cài đặt phần mềm không phục vụ cho các hoạt động nghiệp vụ;
- Phải thực hiện cập nhật và cài đặt các bản vá liên tục;
- Thường xuyên sao lưu các thông tin quan trọng và lưu trữ ở những nơi an toàn;
- Luôn luôn đặt thiết bị trong tầm quan sát khi dự hội thảo, hội nghị hoặc khi làm việc bên ngoài cơ quan;
- Phải cài đặt các biện pháp bảo vệ truy nhập mạng như tường lửa cá nhân, phần mềm phòng chống virus.

2. Tất cả các thiết bị lưu trữ di động được phép sử dụng phải được quét virus trước khi sử dụng.

Bất cứ thiết bị lưu trữ di động nào có chứa bất kỳ thông tin gì của EVNICT đều phải được giữ trong nội bộ và không được mang ra khỏi phạm vi EVNICT trừ khi được cho phép của lãnh đạo đơn vị hoặc cấp cao hơn vì mục đích công việc.

3. Chỉ cho phép truy cập từ xa (như remote desktop, remote assistance) đối với các hệ thống cung cấp dịch vụ thuộc quyền người quản trị theo định danh, IP, mật khẩu .... phục vụ cho công tác xử lý sự cố, sau khi khắc phục xong phải dừng ngay truy cập từ xa.

4. Đối tác của EVNICT được phép sử dụng truy cập từ xa:

- Đối tác đang trong quá trình triển khai các dự án CNTT tại EVNICT cần xử lý, giải quyết các vướng mắc phát sinh theo yêu cầu của EVNICT hoặc theo đề nghị của đối tác.
- Các đối tượng này được cung cấp account/mật khẩu bảo mật từng lần và sẽ phải thu hồi ngay sau khi kết thúc công việc.

5. Chỉ được truy cập vào những phân vùng mạng được phép thông qua việc phân quyền truy cập thông tin của người có thẩm quyền. Không được sử dụng các công cụ hay các biện pháp giả mạo địa chỉ, định danh để truy cập vào các máy chủ, thiết bị vùng mạng không được phép.

6. Không được phép tiết lộ cũng như sử dụng chung các account/password đã được quản trị hệ thống cung cấp.

## Quy định về quản lý đối tác, nhà cung cấp và bên thứ 3



### Quản lý đối tác, nhà cung cấp và bên thứ 3

1. Các vấn đề về bảo mật cần phải được thảo luận và làm rõ với đối tác, nhà cung cấp trước khi ký hợp đồng/biên bản thoả thuận/biên bản ghi nhớ hoặc trước khi cho phép đối tác, nhà cung cấp truy cập tài sản của EVNICT.
2. Cán bộ nhân viên liên quan trong từng vụ việc có trách nhiệm xác định thông tin tài sản cung cấp cho đối tác, bên thứ ba thông qua ràng buộc trong hợp đồng.
2. Không đưa khách cá nhân vào trong khu vực làm việc của EVNICT. Nghiêm cấm cho khách đi nhờ, đi ké qua các cổng, cửa kiểm soát khi không có người phụ trách đi kèm.
3. Tất cả khách đến làm việc tại EVNICT phải được hướng dẫn và qua đăng ký tại quầy lễ tân tòa nhà Tầng 1, đeo thẻ khách và sử dụng thang máy đến tầng 16 để đăng ký làm việc với bộ phận Lễ tân EVNICT.
4. Khách đến làm việc với bộ phận nào, bộ phận đó có trách nhiệm quản lý, không để khách đi lại tự do trong EVNICT. Khách đến làm việc phải đeo thẻ khách trong suốt thời gian làm việc tại EVNICT.



**EVN**

CÔNG TY VIỄN THÔNG ĐIỆN LỰC  
VÀ CÔNG NGHỆ THÔNG TIN

# TRÂN TRỌNG CẢM ƠN !

