TỔNG CÔNG TY ĐẦU TƯ PHÁT TRIỂN ĐƯỜNG CAO TỐC VIỆT NAM
TRUNG TÂM KHAI THÁC VẬN HÀNH ĐCT ĐÀ NẴNG – QUẢNG NGÃI
Số: 45/QĐ-TTKTVHĐNQN.HCTH

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

Đà Nẵng, ngày 16 tháng 5 năm 2024

QUYẾT ĐỊNH

Về việc ban hành Quy định An toàn bảo mật thông tin trong hoạt động tại Trung tâm khai thác vận hành đường cao tốc Đà Nẵng – Quảng Ngãi

- Căn cứ Quyết định số 292/QĐ-VEC- HĐTV ngày 28/5/2021 của Hội đồng thành viên Tổng công ty Đầu tư phát triển đường cao tốc Việt Nam về việc ban hành quy chế tổ chức và hoạt động của Trung tâm khai thác vận hành đường cao tốc Đà Nẵng – Quảng Ngãi;

- Căn cứ Quyết định số 406/QĐ-VEC ngày 03/7/2023 về việc Ban hành quy chế an toàn, bảo mật hệ thống thông tin của Tổng công ty Đầu tư phát triển đường cao tốc Việt Nam;

- Căn cứ theo Biên bản họp ngày 15/5/2024 về việc thống nhất ban hành Quy định an toàn bảo mật thông tin trong hoạt động và Quy định quản lý đăng ký và sử dụng các ứng dụng thông tin phục vụ cho công tác quản lý khai thác vận hành bảo trì tại Trung tâm khai thác vận hành đường cao tốc Đà Nẵng – Quảng Ngãi;

- Căn cứ theo đề nghị của Phòng Hành chính tổng hợp.

QUYẾT ĐỊNH

Điều 1. Ban hành "Quy định An toàn bảo mật thông tin trong hoạt động tại Trung tâm khai thác vận hành đường cao tốc Đà Nẵng – Quảng Ngãi" kèm theo Quyết định này.

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày ký.

Điều 3. Các ông (bà) Ban giám đốc, Trưởng phòng, Đội trưởng và các Phòng, Đội, cá nhân trực thuộc Trung tâm khai thác vận hành đường cao tốc Đà Nẵng - Quảng Ngãi có trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như điều 3;
- HĐTV VEC (để b/c);
- Tổng Giám đốc VEC (để b/c);
- PTGĐ Đặng Hoài Nam (để b/c);
- Ban CNTT (để b/c);
- Lưu VT, HCTH.

GIÁM ĐỐC

M.S.C.N: 0101573513 C.T.T.N.H.H
TRUNG TÂM KHAI THÁC VẬN HÀNH ĐƯỜNG CAO TỐC ĐÀ NẴNG - QUẢNG NGÃI - CHI NHÁNH TỔNG CÔNG TY ĐẦU TƯ PHÁT TRIỂN ĐƯỜNG CAO TỐC VIỆT NAM - CÔNG TY TNHH MỘT THÀNH VIÊN
THÀNH PHỐ ĐÀ NẴNG

Vương Duy Tú

TỔNG CÔNG TY ĐẦU TƯ PHÁT TRIỂN ĐƯỜNG CAO TỐC VIỆT NAM
TRUNG TÂM KHAI THÁC VẬN HÀNH ĐCT ĐÀ NẴNG – QUẢNG NGÃI

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

QUY ĐỊNH
An toàn bảo mật thông tin trong hoạt động tại Trung tâm khai thác vận hành đường cao tốc Đà Nẵng – Quảng Ngãi

CHƯƠNG I:
QUY ĐỊNH CHUNG

Điều 1: Phạm vi và đối tượng áp dụng

Quy định này áp dụng cho toàn bộ quá trình phát triển, vận hành, quản lý và sử dụng hệ thống Công nghệ thông tin nhằm đảm bảo an toàn bảo mật thông tin tại Trung tâm khai thác vận hành đường cao tốc Đà Nẵng – Quảng Ngãi.

Đối tượng áp dụng bao gồm: tất cả người lao động thuộc Trung tâm khai thác vận hành đường cao tốc Đà Nẵng - Quảng Ngãi, nhà cung cấp dịch vụ/bên thứ 3 trong việc quản lý, khai thác, sử dụng và đảm bảo an toàn, an ninh thông tin của Trung tâm.

Điều 2: Giải thích thuật ngữ, từ viết tắt

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

1. "Thông tin" là là toàn bộ các nội dung và dữ liệu được sử dụng cho mục đích sản xuất kinh doanh và các hoạt động khác của Trung tâm. Thông tin được tồn tại ở nhiều hình thức khác nhau: giấy, trang web, tệp tin máy tính, các bản fax, báo cáo, quyết định, email, video, pano áp-phích ...

2. "Hệ thống CNTT" là một tập hợp có cấu trúc các trang thiết bị phần cứng, phần mềm, cơ sở dữ liệu và hệ thống mạng v.v. để sản xuất, truyền nhận, thu thập, xử lý, lưu trữ và trao đổi thông tin phục vụ cho một hoặc nhiều hoạt động kỹ thuật, nghiệp vụ của Trung tâm, Tổng công ty.

3. "Tài sản Công nghệ thông tin (CNTT)" của Trung tâm, Tổng công ty được chia thành 03 loại sau: (i) Tài sản vật lý: là các thiết bị như máy tính (máy chủ, máy tính cá nhân, các thiết bị đi kèm máy tính), thiết bị mạng truyền thông (Router, Switch, Modem,...), máy in, và các thiết bị tin học khác (SAN, tủ rack,...) phục vụ cho hoạt động của hệ thống CNTT; (ii) Tài sản thông tin: là các dữ liệu, tài liệu liên quan đến hệ thống CNTT, được thể hiện bằng văn bản giấy hoặc dữ liệu điện tử; (iii) Tài sản phần mềm bao gồm các chương trình ứng dụng, phần mềm hệ thống, cơ sở dữ liệu và công cụ phát triển.

4. "An toàn Bảo mật Hệ thống thông tin ("ATBMHTTT") là bảo vệ thông tin và hệ thống công nghệ thông tin tránh khỏi những hành vi xâm hại đến tính bảo mật, tính toàn vẹn và tính sẵn sàng của thông tin, bao gồm nhưng không giới hạn các hành vi truy cập, sử dụng, tiết lộ, chỉnh sửa và tiêu hủy thông tin một cách trái phép. Công tác An toàn Bảo mật Thông tin là nhằm đảm bảo các đặc tính sau của thông tin: (i)Tính bảo mật: là đảm bảo thông tin không bị tiết lộ/không được phép truy cập cho các đối tượng không được phép biết hay tiếp cận thông tin; (ii) Tính toàn vẹn: là đảm bảo thông tin phải chính xác và đầy đủ; (iii) Tính sẵn sàng: là đảm bảo thông tin được truy cập và sử dụng khi cần với đúng đối tượng được cấp quyền.

5. "Quy định An toàn bảo mật hệ thống thông tin" là tài liệu cụ thể hóa việc bảo mật, bảo vệ tài sản thông tin trong quy định chung về Bảo vệ bí mật hoạt động kinh doanh của Trung tâm nhằm đảm bảo tính thống nhất và an toàn hệ thống trong quá trình quản lý, khai thác tài sản thông tin, dữ liệu.

6. "Nhà cung cấp dịch vụ / Bên thứ ba" là các tổ chức, cá nhân có chuyên môn được VEC/Trung tâm thuê hoặc hợp tác với VEC/Trung tâm nhằm cung cấp hàng hóa, dịch vụ kỹ thuật.

7. "Rủi ro CNTT" là khả năng xảy ra tổn thất khi thực hiện các hoạt động liên quan đến thông tin, hệ thống CNTT. Rủi ro liên quan đến lưu trữ, xử lý, quản lý, sử dụng phần cứng, phần mềm, truyền thông, giao diện hệ thống, vận hành và con người.

8. "Quản lý rủi ro" là các hoạt động phối hợp nhằm xác định và kiểm soát các rủi ro CNTT có thể xảy ra.

9. "Thiết bị lưu trữ" là thiết bị được dùng để lưu trữ dữ liệu, bao gồm nhưng không hạn chế: đĩa cứng, đĩa quang, thẻ nhớ, USB, băng từ...

10. "Mạng nội bộ" là mạng dùng trong nội bộ của Trung tâm chỉ cán bộ nhân viên mới được quyền truy cập mạng nội bộ này. Mạng nội bộ thường được sử dụng để lưu, chia sẻ, cung cấp thông tin dùng chung cho toàn tổ chức như: chính sách, thông báo..., cũng như truy cập và sử dụng các ứng dụng nghiệp vụ của Trung tâm và Tổng công ty.

11. "Trung tâm" là Trung tâm khai thác vận hành đường cao tốc Đà Nẵng – Quảng Ngãi.

12. "Đơn vị quản lý CNTT" là Phòng Ban tham mưu thuộc Tổng công ty, Phòng HCTH tại Trung tâm được giao nhiệm vụ quản lý các hệ thống CNTT phục vụ sản xuất kinh doanh.

Điều 3. Mục đích, nguyên tắc bảo đảm an toàn bảo mật thông tin

1. Mục đích

a) Đảm bảo các thông tin liên quan tới hoạt động sản xuất kinh doanh của

Tổng công ty và Trung tâm như: Hệ thống các loại dữ liệu, thông tin được lưu trữ trong các tài liệu, văn bản cứng (văn bản giấy) hoặc văn bản mềm (file văn bản điện tử), trong các cơ sở dữ liệu trên máy tính, máy chủ phục vụ việc quản lý và sản xuất của Trung tâm nên việc quản lý và khai thác phải tuân thủ theo các quy định của Tổng công ty và Trung tâm ban hành.

b) Bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

2. Nguyên tắc bảo đảm an toàn bảo mật thông tin

a) Tổ chức, cá nhân thuộc đối tượng áp dụng Quy chế này có trách nhiệm bảo đảm an toàn bảo mật thông tin trong phạm vi xử lý công việc của mình theo quy định của pháp luật, hướng dẫn của Tổng công ty và Trung tâm tại Quy chế này.

b) Bảo đảm an toàn bảo mật thông tin là yêu cầu bắt buộc, phải được thực hiện thường xuyên, liên tục trong quá trình: Thu thập, tạo lập, xử lý, truyền tải, lưu trữ và sử dụng thông tin, dữ liệu.

Điều 4. Những hành vi nghiêm cấm

Các hành vi bị nghiêm cấm quy định tại Điều 7 Luật An toàn thông tin mạng và Điều 8 Luật An ninh mạng.

CHƯƠNG II
QUẢN LÝ THÔNG TIN NGƯỜI DÙNG

Điều 5. Quy định chung quản lý thông tin người dùng

1. Thông tin người sử dụng được lưu trữ và quản lý tập trung trên domain **tctvec.vn, caotocmientrung.com.vn**

2. Các hệ thống phần mềm mới phục vụ hoạt động sản xuất của Trung tâm trước khi đưa vào sử dụng phải được sự thống nhất của Tổng công ty.

3. Khi đăng ký User truy cập các tài nguyên thông tin phải đăng ký đầy đủ các thông tin như: Họ và tên, User, IP truy cập, hệ thống truy cập, các chức năng phần mềm hệ thống cần truy cập.

4. Khi một cán bộ nhân viên nghỉ việc hoặc thay đổi vị trí công, đơn vị (cũ) quản lý cán bộ nhân viên đó phải gửi thông tin cho đơn vị quản lý CNTT tương ứng để thực hiện xóa, sửa, phân quyền lại cho User tương ứng của cán bộ nhân viên đó trên hệ thống thông tin Tổng công ty và Trung tâm trước thời điểm cán bộ chính thức chuyển khỏi Trung tâm.

Điều 6. Quy định mật khẩu người dùng truy cập các hệ thống thông tin của Trung tâm

1. Thời gian sử dụng mật khẩu tối đa không quá 180 ngày.

2. Mật khẩu phải đặt bắt buộc có cả chữ thường và chữ hoa (a-z, A-Z) và chữ số (0-9), tùy chọn có thêm ký hiệu đặc biệt có trên bàn phím máy tính, có số ký tự tối thiểu đảm bảo an toàn tùy theo từng hệ thống. Mật khẩu mới không được đặt giống một trong số các mật khẩu đã đặt trong 2 lần gần nhất và cũng không được giống tên đăng nhập gắn liền với mật khẩu.

3. Mật khẩu đặt lần đầu tiên hoặc được thiết lập lại do người quản trị/người vận hành phải được gửi trực tiếp đến cá nhân quản lý tài khoản đó kèm thông báo là cần đổi ngay sau khi đăng nhập lần đầu tiên.

4. Người sử dụng có trách nhiệm bảo vệ mật khẩu của mình, định kỳ chủ động thay đổi mật khẩu, không chia sẻ mật khẩu cho bất kỳ ai trong mọi trường hợp.

CHƯƠNG III
TRÁCH NHIỆM QUẢN LÝ, SỬ DỤNG ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

Điều 7. Quản lý thiết bị công nghệ thông tin

Thiết bị CNTT trang bị tại các phòng, đội, đơn vị là tài sản của Trung tâm được Tổng công ty Đầu tư phát triển đường cao tốc Việt Nam giao quản lý và sử dụng trong công tác khai thác vận hành bảo trì dự án đường cao tốc Đà Nẵng – Quảng Ngãi. Các đơn vị, cán bộ nhân viên và người lao động có trách nhiệm quản lý trang thiết bị được giao theo đúng quy định của Trung tâm, Tổng công ty.

Điều 8. Quy định về an toàn Cơ sở dữ liệu (CSDL)

Các phần mềm ứng dụng trong hệ thống mạng máy tính tại Trung tâm phải tuân thủ các quy định quản lý của VEC và tuân theo quy định của Nhà nước.

Điều 9. Quy định về bảo mật đối với phần mềm phục vụ sản xuất kinh doanh

1. Các phần mềm phục vụ sản xuất kinh doanh phải có các chức năng bảo mật thông tin, tối thiểu phải có các chức năng sau:

a) Quản lý mật khẩu người sử dụng theo quy định của VEC và Trung tâm.

b) Phải có chức năng chống dò quét mật khẩu tự động;

c) Phân quyền người sử dụng đến từng chức năng của chương trình;

d) Cho phép sử dụng nhiều hình thức xác thực tập trung, xác thực đa nhân tố đối với các chức năng yêu cầu bảo mật cao.

2. Gán User riêng biệt cho từng người dùng và phân quyền cụ thể cho từng User.

3. Định định kỳ kiểm tra và xác nhận phần mềm đáp ứng điều kiện bảo mật

thông tin để tiếp tục sử dụng theo quy định.

Điều 10. Phòng chống virus máy tính, bảo mật cơ sở dữ liệu hoạt động

- Bảo mật số liệu, thông tin hoạt động: Cán bộ nhân viên, người lao động tại Trung tâm phải có trách nhiệm bảo mật số liệu thông tin hoạt động trong công việc được phân công.

- Bảo mật truy cập: Các chương trình ứng dụng, phân chia sử dụng trên máy tính phải được đặt mật khẩu, mã khoá bảo mật.

- An toàn trong sử dụng: Khi không làm việc với máy vi tính trong thời gian dài, phải tắt máy tính hoặc đặt chế độ bảo vệ để đảm bảo an toàn cho dữ liệu của cá nhân.

- Phòng, chống virus: Cán bộ nhân viên, người lao động thuộc Trung tâm có trách nhiệm tuân thủ các biện pháp phòng và chống virus cho máy tính, đảm bảo an toàn dữ liệu thuộc cá nhân quản lý. Mọi dữ liệu từ các thiết bị lưu trữ bên ngoài đều phải được quét, diệt virus mỗi khi đưa vào máy. Không truy cập vào các link liên kết không rõ ràng; không click vào các link, tải về các file tài liệu từ các địa chỉ thư không nắm rõ thông tin, địa chỉ người gửi.

Việc quản lý phòng chống virus và phần mềm độc hại được thực hiện theo các yêu cầu sau:

1. Không mở các thư từ địa chỉ lạ hoặc các thư có đính kèm file mà không rõ nguồn gốc, website không phục vụ công việc trên hệ thống máy tính, hệ thống mạng nội bộ của Trung tâm.
2. Nghiêm cấm mọi hành động tạo lập, phân phối virus, chương trình nguy hiểm trên hệ thống máy tính, hệ thống mạng nội bộ của Trung tâm.
3. Không chia sẻ thư mục/file trực tiếp với chế độ truy cập đọc/ghi khi không có sự cho phép của người quản trị hệ thống của Trung tâm.
4. Quét virus trên các đĩa CD, USB hoặc thiết bị lưu trữ di động khác (nếu máy tính đó được cấp quyền) trước khi đưa vào sử dụng trên hệ thống máy tính của Trung tâm.

Điều 11. Đảm bảo an toàn truy cập, đăng nhập hệ thống thông tin

- Trách nhiệm, quyền hạn người dùng khi truy cập, đăng nhập các hệ thống thông tin, đảm bảo mỗi người dùng khi sử dụng hệ thống thông tin phải được cấp và sử dụng tài khoản truy cập với định danh duy nhất gắn với người dùng đó. Trường hợp sử dụng tài khoản dùng chung cho một nhóm người hay một đơn vị, bộ phận phải có cơ chế xác định các cá nhân có trách nhiệm quản lý tài khoản. Người dùng chỉ được truy cập các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình và có trách nhiệm bảo mật tài khoản truy cập được cấp.

Điều 12. Đảm bảo an toàn thông tin, dữ liệu

Thông tin, dữ liệu khi được lưu trữ, khai thác, trao đổi phải được đảm bảo tính toàn vẹn, tính tin cậy, tính sẵn sàng và phải có cơ chế lưu trữ dự phòng.

Trong trao đổi thông tin, dữ liệu phục vụ công việc tại Trung tâm phải đảm bảo bảo mật thông tin.

Điều 13. Những điều không được làm

Không được lợi dụng việc sử dụng Internet nhằm mục đích: Chống lại nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam, gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội; kích động bạo lực, đồi trụy, tệ nạn xã hội, mê tín dị đoan; phá hoại thuần phong mỹ tục của dân tộc.

Không được chơi các trò chơi trực tuyến (game online) hoặc các trò chơi khác trên Internet trong giờ làm việc.

Không được truy cập hoặc tải các trang website có nội dung đồi trụy, phản động, các chương trình không rõ nguồn gốc, các thông tin quảng cáo hấp dẫn.

Khi sử dụng hệ thống thư điện tử (Email) không được kích chuột vào bất cứ thư điện tử, tệp đính kèm, đường link, thư rác, thư quảng cáo nào không rõ nguồn gốc và không xác định được người gửi.

CHƯƠNG IV
QUẢN LÝ TRUY CẬP

Điều 14. Quy định chung quản lý truy cập

Xây dựng và thực hiện các quy định về quản lý truy cập đối với người sử dụng, nhóm người sử dụng để đảm bảo đáp ứng yêu cầu nghiệp vụ và yêu cầu an toàn bảo mật. Quy định về quản lý truy cập bao gồm các nội dung cơ bản sau:

1. Phân quyền truy cập
2. Quy tắc thiết lập mã truy cập, mật khẩu
3. Đăng ký, cấp phát, gia hạn và thu hồi quyền truy cập của người sử dụng
4. Giới hạn và kiểm soát các truy cập đặc quyền
5. Quản lý, cấp phát mật khẩu
6. Rà soát, kiểm tra, xét duyệt lại quyền truy cập của người sử dụng
7. Kiểm soát quyền truy cập đối với người dùng hệ thống trong thời gian nghỉ dài ngày
8. Quản lý việc truy cập từ xa.

Điều 15. Quản lý kết nối Internet

1. Không cung cấp, gửi và nhận các nội dung từ Internet không liên quan tới công việc, các tập tin, liên kết không có nguồn gốc rõ ràng.

2. Việc gửi nhận các thông tin quan trọng (hợp đồng, tài liệu hệ thống,..) trong công ty ra ngoài phải qua kênh Email của Trung tâm và phải được được đảm

bảo an toàn bảo mật cho nội dung. Các trường hợp ngoại lệ không thể gửi qua email cần có sự phê duyệt của Ban giám đốc.

3. Không sử dụng các công cụ phần mềm và các biện pháp kỹ thuật nhằm chiếm dụng băng thông đường truyền, gây tắc nghẽn mạng Internet của Tổng công ty cho các mục đích riêng khi không có sự cho phép của Lãnh đạo Tổng công ty và Trung tâm.

4. Nghiêm cấm mọi hành vi sử dụng mạng Internet Tổng công ty, Trung tâm vào các trang web phản động hoặc website có nội dung không lành mạnh, đưa các thông tin xuyên tạc, vu khống, xúc phạm uy tín của tổ chức, danh dự nhân phẩm công dân, gửi nhận các thông tin đồi trụy vi phạm pháp luật Việt Nam.

5. Nghiêm cấm việc sao chép, chuyển, hay lưu trữ dữ liệu từ hệ thống nội bộ sang ổ cứng gắn theo máy, hay thiết bị lưu trữ di động khi thực hiện truy cập từ xa đến các dữ liệu đó.

6. Người sử dụng tuân thủ các quy định về sử dụng Internet và tự chịu trách nhiệm trước Tổng công ty, Trung tâm và pháp luật về thông tin trao đổi trên Internet được kết nối từ mạng Tổng công ty, Trung tâm.

Điều 16. Kiểm soát truy cập thông tin và ứng dụng

1. Quản lý và phân quyền truy cập thông tin ứng dụng phù hợp với chức năng nhiệm vụ của người sử dụng:

a) Phân quyền truy cập đến từng thư mục, chức năng của chương trình;

b) Phân quyền đọc, ghi, xóa, thực thi đối với thông tin, dữ liệu, chương trình.

2. Các hệ thống thông tin quan trọng phải đặt trong môi trường mạng máy tính riêng. Neu các hệ thống thông tin cùng sử dụng nguồn tài nguyên chung thì phải được người quản trị hệ thống chấp nhận.

CHƯƠNG V
QUY ĐỊNH BẢO MẬT VỚI NHÀ CUNG CẤP DỊCH VỤ/ BÊN THỨ 3

Điều 17. Nguyên tắc sử dụng dịch vụ của nhà cung cấp dịch vụ/ bên thứ 3

Việc sử dụng CNTT của Nhà cung cấp dịch vụ/ Bên thứ 3 phải đảm bảo các nguyên tắc sau:

1. Tuân thủ các quy định của VEC trong việc sử dụng dịch vụ CNTT không làm suy giảm khả năng cung cấp dịch vụ liên tục của Tổng công ty, Trung tâm tới khách hàng.

2. Việc sử dụng dịch vụ CNTT không làm suy giảm việc kiểm soát quy trình nghiệp vụ của Tổng công ty, Trung tâm.

3. Việc sử dụng dịch vụ CNTT không làm thay đổi trách nhiệm Tổng công ty, Trung tâm trong việc đảm bảo an toàn, bảo mật thông tin.

Điều 18. Quy định bảo mật khi sử dụng dịch vụ của nhà cung cấp dịch vụ/bên thứ 3

Cần thực hiện các nội dung về bảo mật sau để đánh giá các rủi ro công nghệ thông tin, rủi ro hoạt động trước khi sử dụng dịch vụ CNTT của Nhà cung cấp dịch vụ/ bên thứ 3.

1. Trước khi ký hợp đồng nhà thầu phải:

a) Phân quyền và trách nhiệm, an ninh bảo mật thông tin cho nhân viên, các bên cung cấp dịch vụ và các bên thứ ba cần phải được định nghĩa về lập thành tài liệu tương ứng với chính sách an ninh bảo mật của Tổng công ty, Trung tâm.

b) Hợp đồng ký kết phải bao gồm các điều khoản về việc xử phạt trong trường hợp vi phạm quy định an toàn bảo mật thông tin và trách nhiệm trong trường hợp có thiệt hại do hành vi vi phạm của bên thứ ba gây ra.

2. Trước khi triển khai công việc

a) Yêu cầu Nhà thầu phải cung cấp danh sách nhân sự của bên thứ ba sẽ tham gia công việc.

b) Mỗi nhân sự tham gia phải được kiểm tra tư cách pháp lý và năng lực chuyên môn đảm bảo phù hợp với công việc.

c) Đại diện pháp lý của của bên thứ ba phải ký cam kết không tiết lộ thông tin của Tổng công ty ra ngoài.

d) Các nhân sự của bên thứ ba phải được phổ biến về quy định an toàn bảo mật thông tin hiện hành của Tổng công ty có liên quan đến công việc trước khi bắt đầu.

3. Trong khi triển khai không việc

a) Cung cấp và yêu cầu bên thứ ba tuân thủ đầy đủ các quy định, quy chế về an toàn, bảo mật CNTT của Tổng Công ty, Trung tâm.

b) Trong trường hợp phát hiện dấu hiệu vi phạm hoặc vi phạm quy định an toàn bảo mật thông tin của bên thứ ba, đơn vị cần:

- Tạm dừng hoặc đình chỉ hoạt động của bên thứ ba tùy theo mức độ vi phạm;
- Thông báo chính thức các vi phạm về an toàn, bảo mật CNTT của nhân sự cho bên thứ ba;
- Kiểm tra xác định, lập báo cáo mức độ vi phạm và thông báo cho bên thứ ba thiệt hại xảy ra;
- Thu hồi quyền truy cập hệ thống CNTT đã được cấp cho bên thứ ba.
- Đơn vị giám sát, quản lý hợp đồng phải thực hiện quản lý nhà thầu để đảm

bảo không được phát sinh các vấn đề về an toàn bảo mật thông tin.

4. Khi kết thúc công việc:

a) Yêu cầu bên thứ ba bàn giao tất cả tài sản sử dụng của VEC, Trung tâm trong quá trình triển khai công việc;

b) Thu hồi, khóa tài khoản khách hoặc các tài khoản truy cập khác đã cấp cho nhân sự của bên thứ ba ngay sau khi kết thúc công việc;

c) Thay đổi các khóa và mật khẩu nhận bàn giao từ đối tác hoặc tạo/ đặt bởi đối tác.

d) Trách nhiệm của đơn vị quản lý, giám sát nhà thầu phải đảm bảo nhà thầu tuân thủ các yêu cầu về bảo mật thông tin của hệ thống.

CHƯƠNG VI
TỔ CHỨC THỰC HIỆN

Điều 19. Điều khoản thi hành

Cán bộ nhân viên và người lao động tại các phòng, đội, đơn vị trực thuộc Trung tâm có trách nhiệm thực hiện nghiêm túc Quy định này.

Mọi hành vi vi phạm các điều khoản trong Quy định, tùy theo tính chất, mức độ sẽ bị xử lý kỷ luật, xử phạt vi phạm hành chính, bồi thường vật chất, khắc phục hậu quả hoặc truy cứu trách nhiệm theo quy định của VEC và pháp luật hiện hành.

Trong quá trình thực hiện, nếu có vấn đề phát sinh hoặc khó khăn, vướng mắc cần phản ánh kịp thời về phòng Hành chính tổng hợp để tổng hợp báo cáo Giám đốc Trung tâm xem xét quyết định điều chỉnh, bổ sung cho phù hợp./.

GIÁM ĐỐC

M.S.C.N: 0101573511-004 - C.T.T.N.H.H
TRUNG TÂM KHAI THÁC VẬN HÀNH ĐƯỜNG CAO TỐC ĐÀ NẴNG - QUẢNG NGÃI - CHI NHÁNH TỔNG CÔNG TY ĐẦU TƯ PHÁT TRIỂN ĐƯỜNG CAO TỐC VIỆT NAM - CÔNG TY TNHH MỘT THÀNH VIÊN
THÀNH PHỐ ĐÀ NẴNG

Vương Duy Tú