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

Số: /QĐ-NCM	*Hà Nội, ngày tháng năm 2020*

QUYẾT ĐỊNH

BAN HÀNH QUY CHẾ CHÍNH SÁCH BẢO ĐẢM AN TOÀN, AN NINH HỆ THỐNG THÔNG TIN CÔNG TY

GIÁM ĐỐC

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Luật An ninh mạng ngày 12 tháng 6 năm 2018;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Nghị định số 15/2020/NĐ-CP ngày 03 tháng 02 năm 2020 của Chính phủ về 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;

Căn cứ Điều lệ Công ty;

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế chính sách bảo đảm an toàn, an ninh hệ thống thông tin Công ty.

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

Điều 3. Các bộ phận, chi nhánh, cá nhân trong Công ty chịu trách nhiệm đọc, hiểu rõ, cam kết, thi hành Quyết định này./.

Nơi nhận:	**CÔNG TY CP CÔNG NGHỆ THẺ**
- Như Điều 3;	**NACENCOMM**
- Lưu VT:	

QUY CHẾ CHÍNH SÁCH

BẢO ĐẢM AN TOÀN, AN NINH HỆ THỐNG THÔNG TIN CÔNG TY

(Kèm theo Quyết định số /QĐ-NCM ngày tháng năm 2020 của Giám đốc Công ty)

Chương I

QUY ĐỊNH CHUNG

Điều 4. Phạm vi, đối tượng, cấp độ và mục tiêu

1. Phạm vi điều chỉnh: Quy chế này quy định về bảo đảm an toàn, an ninh hệ thống thông tin trong các hoạt động của công ty CP Công nghệ thẻ NACENCOMM bao gồm Chi nhánh TP HCM và đối tác liên quan.

2. Đối tượng áp dụng:

a) Các bộ phận nghiệp vụ và cán bộ Công ty, Chi nhánh.

b) Đối tác, tổ chức, cá nhân tham gia và cung cấp dịch vụ liên quan.

3. Cấp độ: Cấp độ 4 theo quy định của pháp luật.

4. Mục tiêu: Duy trì là Công ty hàng đầu trong lĩnh vực ứng dụng công nghệ bảo mật xác thực, cung cấp các sản phẩm cho khách hàng vói tiêu chí Dễ dùng nhất; An toàn nhất; Hỗ trợ tốt nhất.

Điều 5. Giải thích từ ngữ

Trong Quy chế chính sách này, các từ ngữ dưới đây được hiểu như sau:

1. Hệ thống thông tin là một tập hợp các trang thiết bị phần cứng, phần mềm, cơ sở dữ liệu, hệ thống mạng, hệ thống quản lý và vận hành để tạo lập, truyền nhận, thu thập, xử lý, lưu trữ và trao đổi thông tin số phuc vụ cho một hoặc nhiều hoạt động kỹ thuật, nghiệp vụ của Công ty;

2. Bảo đảm an toàn thông tin mức vật lý là việc bảo vệ hệ thống hạ tầng kỹ thuật, phần mềm, ứng dụng và cơ sở dữ liệu khỏi các mối nguy hiểm vật lý (như: cháy, nổ; nhiệt độ, độ ẩm ngoài mức cho phép; thiên tai; mất điện; tác động cơ học) có thể gây ảnh hưởng đến hoạt động của hệ thống;

3. An toàn thông tin là sự bảo vệ thông tin số, hệ thống thông tin tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính bí mật, tính toàn vẹn và tính sẵn sàng của thông tin;

4. Rủi ro công nghệ thông tin là khả năng xảy ra tổn thất khi thực hiện các hoạt động liên quan đến hệ thống thông tin. Rủi ro công nghệ thông tin liên quan đến quản lý, sử dụng phần cứng, phần mềm, truyền thông, giao diện hệ thống, vận hành và con người;

5. Sự cố an ninh mạng (cybersecurity incident) là việc thông tin số, hệ thống thông tin bị tấn công hoặc bị gây nguy hại, ảnh hưởng tới tính bí mật, tính toàn vẹn, tính sẵn sàng;

6. Điểm yếu về mặt kỹ thuật là thành phần trong hệ thống thông tin dễ bị khai thác, lợi dụng khi bị tấn công hoặc xâm nhập bất hợp pháp;

7. Không gian mạng là mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, bao gồm mạng viễn thông, mạng internet, hệ thống máy tính, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, là nơi con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian;

8. Hạ tầng kỹ thuật là tập hợp các thiết bị tính toán, lưu trữ, thiết bị ngoại vi, thiết bị kết nối mạng, thiết bị phụ trợ, đường truyền, mạng nội bộ, mạng diện rộng;

9. Tường lửa là tập hợp các thành phần hoặc một hệ thống các trang thiết bị, phần mềm được đặt giữa hai mạng, nhằm kiểm soát tất cả các kết nối từ bên trong ra bên ngoài mạng hoặc ngược lại;

10. Mạng không tin cậy là mạng bên ngoài có kết nối vào mạng của Công ty và không thuộc sự quản lý của Công ty;

11. Phần mềm độc hại là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay toàn bộ hệ thống thông tin hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong hệ thống thông tin;

12. Dịch vụ điện toán đám mây là các dịch vụ cung cấp tài nguyên máy tính (computing resources) qua môi trường mạng cho phép nhiều đối tượng sử dụng, có thể điều chỉnh và thanh toán theo nhu cầu sử dụng;

13. Tài khoản người sử dụng (tài khoản) là một tập hợp thông tin đại diện duy nhất cho người sử dụng trên hệ thống thông tin, được sử dụng để đăng nhập và truy cập các tài nguyên được cấp phép trên hệ thống thông tin đó;

14. Bên thứ ba là các cá nhân, doanh nghiệp có thỏa thuận bằng văn bản với Công ty nhằm cung cấp dịch vụ công nghệ thông tin.

Điều 6. Nguyên tắc bảo đảm an toàn, an ninh hệ thống thông tin Công ty

1. Bảo đảm an toàn, an ninh thông tin là yêu cầu bắt buộc, thường xuyên, liên tục, có tính xuyên suốt quá trình liên quan đến thông tin và thiết kế, xây dựng, vận hành, nâng cấp, hủy bỏ hệ thống thông tin. Bảo đảm an toàn, an ninh thông tin tuân thủ các nguyên tắc chung quy định tại Điều 4 Luật An toàn thông tin mạng, Điều 4 Luật An ninh mạng và Điều 4 Nghị định số 85/2016/NĐ-CP.

2. Các bộ phận trong Công ty có trách nhiệm tham gia bảo đảm an toàn, an ninh hệ thống

thông tin của Công ty; Công ty phân công bố trí nhân sự chuyên trách chịu trách nhiệm bảo đảm an toàn, an ninh hệ thống thông tin; xác định rõ quyền hạn, trách nhiệm của Công ty, từng bộ phận, cá nhân đối với công tác bảo đảm an toàn, an ninh hệ thống thông tin.

3. Từng thành viên trong Công ty có trách nhiệm bảo đảm an toàn, an ninh hệ thống thông tin trong phạm vi xử lý công việc của mình theo quy định của Nhà nước và của Công ty.

4. Xử lý sự cố an toàn thông tin phải phù hợp với trách nhiệm, quyền hạn và bảo đảm lợi ích hợp pháp của Công ty, bộ phận, cá nhân liên quan và theo quy định của pháp luật.

Điều 7. Các hành vi bị nghiêm cấm

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

2. Tự ý đấu nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập mạng không dây của cá nhân vào mạng nội bộ; tự ý thay đổi, gỡ bỏ biện pháp an toàn thông tin cài đặt trên thiết bị công nghệ thông tin phục vụ công việc; tự ý thay thế, lắp mới, tráo đổi thành phần của máy tính phục vụ công việc.

3. Tạo ra, cài đặt, phát tán phần mềm độc hại.

4. Cản trở hoạt động cung cấp dịch vụ; ngăn chặn việc truy nhập đến dịch vụ, thông tin của Công ty.

5. Các hành vi khác làm mất an toàn, bí mật thông tin của Công ty.

Chương II

CÁC QUY ĐỊNH BẢO ĐẢM AN TOÀN, AN NINH HỆ THỐNG THÔNG TIN

Mục 1

QUẢN LÝ TÀI SẢN CÔNG NGHỆ THÔNG TIN

Điều 8. Quản lý tài sản công nghệ thông tin

1. Lập danh sách của tất cả các tài sản công nghệ thông tin gắn với từng hệ thống thông tin. Định kỳ rà soát và cập nhật danh sách tài sản công nghệ thông tin.

2. Giao, gắn trách nhiệm cho cá nhân hoặc bộ phận quản lý, sử dụng tài sản công nghệ thông tin.

3. Căn cứ theo mức độ quan trọng quy định các quy tắc sử dụng, giữ gìn bảo vệ tài sản công nghệ thông tin trong các trường hợp như: mang ra khỏi Công ty, trang thiết bị công nghệ thông tin liên quan đến dữ liệu quan trọng, cài đặt và cấu hình.

4. Tài sản có bộ phận lưu trữ hoặc thiết bị lưu trữ 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. Các bộ phận có trách nhiệm tuân thủ quy trình bảo dưỡng, bảo trì và hướng dẫn cách sử dụng, quản lý, vận hành hệ thống hạ tầng kỹ thuật; tham vấn bộ phận chuyên trách về công nghệ thông tin thực hiện quản lý, vận hành và định kỳ kiểm tra, sửa chữa, bảo trì thiết bị (bao gồm thiết bị đang hoạt động và thiết bị dự phòng).

6. Các loại tài sản công nghệ thông tin bao gồm:

a) Tài sản thông tin: các dữ liệu, thông tin ở dạng số được xử lý, lưu trữ thông qua hệ thống thông tin;

b) Tài sản vật lý: các thiết bị công nghệ thông tin, phương tiện truyền thông, vật mang tin và các thiết bị phục vụ cho hoạt động của hệ thống thông tin;

c) Tài sản phần mềm: các phần mềm hệ thống, phần mềm tiện ích, phần mềm lớp giữa, cơ sở dữ liệu, chương trình ứng dụng, mã nguồn và công cụ phát triển do Công ty mua, và phát triển cùng các Hồ sơ, tài liệu kèm theo phần mềm.

d) Tài sản hồ sơ: Các hồ sơ, tài liệu dạng giấy và dạng số.

Mục 2
QUẢN LÝ NHÂN SỰ

Điều 9. Quản lý nguồn nhân lực

1. Tổ chức bộ phận chuyên trách về an toàn hệ thống thông tin có chức năng, nhiệm vụ đảm bảo an toàn hệ thống thông tin và ứng cứu sự cố an toàn an ninh hệ thống thông tin của Công ty: Bộ phận giám sát và vận hành an toàn an ninh hệ thống thông tin Công ty.

2. Tách biệt nhân sự giữa các nhiệm vụ: (i) Phát triển với quản trị hệ thống thông tin; (ii) Phát triển với vận hành hệ thống thông tin; (iii) Quản trị với vận hành hệ thống thông tin; (iv) Kiểm tra về an toàn thông tin với phát triển, quản trị, vận hành hệ thống thông tin.

3. Các bộ phận phải có các danh mục yêu cầu, trách nhiệm bảo đảm an toàn, an ninh hệ thống thông tin đối với từng vị trí công việc. Sau khi tuyển dụng, tiếp nhận nhân sự mới, bộ phận phải có trách nhiệm phổ biến cho nhân sự mới các quy định về bảo đảm an toàn, an ninh hệ thống thông tin của Công ty.

4. Bộ phận chuyên trách về an toàn hệ thống thông tin phải thường xuyên tổ chức quán triệt các quy định về an toàn, an ninh hệ thống thông tin, nhằm nâng cao nhận thức về trách nhiệm bảo đảm an toàn hệ thống thông tin của từng cá nhân trong Công ty.

5. Khi có nhân sự chấm dứt hoặc thay đổi công việc, Công ty, bộ phận phải:

a) Xác định rõ trách nhiệm của nhân sự và các bên liên quan trong quản lý, sử dụng các tài sản công nghệ thông tin được giao.

b) Lập biên bản bàn giao tài sản công nghệ thông tin.

c) Thay đổi hoặc thu hồi quyền truy cập các hệ thống thông tin.

Mục 3

ĐẢM BẢO AN TOÀN VỀ MẶT VẬT LÝ VÀ MÔI TRƯỜNG HỆ THỐNG

Điều 10. Bảo đảm an toàn hệ thống công nghệ thông tin

1. Bảo đảm an toàn thông tin đối với trung tâm dữ liệu/phòng máy chủ

a) Trung tâm dữ liệu đươc lắp đặt tại phòng riêng biêt, đảm bảo các yêu cầu về tiêu chuẩn, quy chuẩn đối với các dịch vụ Công ty cung cấp theo quy định của Nhà nước. Cửa ra vào sử dụng ít nhất hai loại khóa khác nhau, được giám sát 24/7.

b) Các thiết bị kết nối mạng, thiết bị bảo mật quan trọng như tường lửa (firewall), thiết bị định tuyến (router), hệ thống máy chủ, hệ thống lưu trữ SAN, NAS, ... phải được đặt trong trung tâm dữ liệu/phòng máy chủ và phải được thiết lập cơ chế bảo vệ, theo dõi phát hiện xâm nhập và biện pháp kiểm soát truy nhập, kết nối vật lý phù hợp với từng khu vực: máy chủ và hệ thống lưu trữ; tủ mạng và đầu nối; thiết bị nguồn điện và dự phòng điện khẩn cấp; vận hành, kiểm soát, quản trị hệ thống. Cán bộ phụ trách, bộ phận chuyên quản trung tâm dữ liệu/phòng máy chủ có trách nhiệm xây dựng nội quy hoặc hướng dẫn làm việc khu vực này.

c) Trung tâm dữ liệu/phòng máy chủ là khu vực hạn chế tiếp cận và được lắp đặt hệ thống camera giám sát. Chỉ những cá nhân có quyền, nhiệm vụ theo quy định của phụ trách bộ phận mới được phép vào trung tâm dữ liệu/phòng máy chủ. Quá trình vào, ra phòng máy chủ phải được ghi nhận vào nhật ký quản lý trung tâm dữ liệu/phòng máy chủ.

d) Trung tâm dữ liệu/phòng máy chủ phải được trang bị hệ thống lưu điện đủ công suất và duy trì thời gian hoạt động của các máy chủ ít nhất 15 phút khi có sự cố mất điện. Và có nguồn điện máy phát dự phòng nguồn điện lưới mất điện quá 5 phút.

đ) Trung tâm dữ liệu/phòng máy chủ phải có hệ thống giám sát nhiệt độ, độ ẩm để đảm bảo môi trường vận hành; hệ thống cảnh báo cháy, hệ thống chữa cháy tự động bằng khí, thiết bị phòng cháy, chữa cháy khẩn cấp; hệ thống cảnh báo hệ thống nguồn điện; hệ thống chống sét lan truyền. Tất cả các cảnh báo này phải được gửi đến các cá nhân có trách nhiệm qua tin nhắn hoặc thư điện tử. Cán bộ phụ trách, bộ phận phải cử cán bộ thường xuyên giám sát thiết bị, hạ tầng của trung tâm dữ liệu/phòng máy chủ.

e) Đảm bảo lưu trữ nhật ký độc lập và phù hợp với hoạt động của máy chủ. Dữ liệu nhật ký

phải được lưu tối thiểu 6 tháng.

f) Đảm bảo áp dụng phương pháp xác thực thực đa nhân tố khi truy cập vào các máy chủ trong hệ thống.

g) Đảm bảo việc xác thực tính toàn vẹn của các tệp tin hệ thống và tính toàn vẹn của các quyền đã được cấp trên các tài khoản hệ thống.

2. Bảo đảm an toàn thông tin khi sử dụng máy tính

a) Cá nhân chỉ cài đặt phần mềm hợp lệ và thuộc danh mục phần mềm được phép sử dụng trên máy tính được bộ phận cấp cho mình; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm khi chưa có sự đồng ý của bộ phận chuyên trách về công nghệ thông tin; thường xuyên cập nhật phần mềm và hệ điều hành.

b) Cài đặt phần mềm xử lý phần mềm độc hại và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm; khi phát hiện bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại trên máy tính phải tắt máy và báo trực tiếp cho bộ phận chuyên trách về công nghệ thông tin để được xử lý kịp thời.

c) Chỉ truy nhập vào các trang/cổng thông tin điện tử, ứng dụng trực tuyến tin cậy và các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình; có trách nhiệm bảo mật tài khoản truy nhập thông tin, không chia sẻ mật khẩu, thông tin cá nhân với người khác.

3. Bảo đảm an toàn thông tin đối với hệ thống hạ tầng mạng

a) Đảm bảo quản lý an toàn, bảo mật hệ thống mạng và quản lý các thiết bị đầu cuối của toàn bộ hệ thống mạng.

b) Lập, lưu trữ hồ sơ về sơ đồ logic và vật lý đối với hệ thống mạng, bao gồm cả mạng diện rộng (WAN/Intranet) và mạng nội bộ (LAN).

c) Chia tách thành các vùng mạng khác nhau theo đối tượng sử dụng, mục đích sử dụng và hệ thống thông tin, tối thiểu: (i) Có phân vùng mạng riêng cho máy chủ của hệ thống thông tin; (ii) Có phân vùng mạng trung gian (DMZ) để cung cấp dịch vụ trên mạng Internet; (iii) Có phân vùng mạng riêng để cung cấp dịch vụ mạng không dây.

d) Trang bị thiết bị có chức năng tường lửa để kiểm soát các kết nối, truy cập vào ra các vùng mạng quan trọng.

đ) Trang bị thiết bị có chức năng tường lửa và chức năng phát hiện phòng chống xâm nhập để kiểm soát kết nối, truy cập từ mạng không tin cậy vào hệ thống mạng của tổ chức.

e) Hỗ trợ các công nghệ mạng riêng ảo thông dụng và có phần cứng mã hóa tích hợp để tăng tốc độ mã hóa dữ liệu.

f) Đảm bảo kiểm soát, phát hiện và ngăn chặn kịp thời các kết nối, truy cập trái phép vào hệ thống mạng nội bộ của tổ chức có hệ thống thông tin.

g) Đảm bảo cân bằng tải và phương án ứng phó tấn công từ chối dịch vụ (DDoS) đối với các hệ thống cung cấp dịch vụ trên mạng Internet.

h) Thiết lập, cấu hình các tính năng theo thiết kế của các trang thiết bị an ninh mạng; thực hiện các biện pháp, giải pháp để dò tìm và phát hiện kịp thời các điểm yếu, lỗ hổng về mặt kỹ thuật của hệ thống mạng; thường xuyên kiểm tra, phát hiện những kết nối, trang thiết bị, phần mềm cài đặt bất hợp pháp vào mạng.

i) Trang bị giải pháp đảm bảo quản lý mạng không dây tập trung.

j) Đảm bảo dự phòng nóng cho các thiết bị mạng chính đảm bảo khả năng vận hành liên tục của hệ thống.

k) Đảm bảo áp dụng phương pháp xác thực thực đa nhân tố đối với các thiết bị mạng quan trọng.

l) Duy trì ít nhất 02 kết nối mạng Internet từ các ISP sử dụng hạ tầng kết nối trong nước khác nhau.

4. Bảo đảm an toàn thông tin mức ứng dụng, dịch vụ

a) Yêu cầu về bảo đảm an toàn thông tin phải được đưa vào tất cả các công đoạn thiết kế, xây dựng, triển khai và vận hành, sử dụng phần mềm, ứng dụng và dịch vụ.

b) Phần mềm, ứng dụng và dịch vụ phải đáp ứng các yêu cầu sau: cấu hình phần mềm, ứng dụng để xác thực người sử dụng; giới hạn số lần đăng nhập sai liên tiếp; giới hạn thời gian để chờ đóng phiên kết nối; mã hóa thông tin xác thực trên hệ thống; không khuyến khích việc đăng nhập tự động.

c) 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.

d) Áp dụng cơ chế xác thực đa nhân tố khi truy cập vào các tài khoản quản trị của ứng dụng. Có cơ chế yêu cầu người sử dụng thay đổi thông tin xác thực định kỳ. Có cơ chế mã hóa thông tin xác thực của người sử dụng trước khi gửi đến ứng dụng qua môi trường mạng.

đ) 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.

e) Ghi và lưu giữ bản ghi nhật ký hệ thống của phần mềm, ứng dụng trong khoảng thời gian tối thiểu 06 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.

f) 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.

g) 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.

5. Bảo đảm an toàn thông tin mức dữ liệu

a) Phải thực hiện bảo vệ thông tin, dữ liệu liên quan đến hoạt động nghiệp vụ, 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.

b) Phát hiện, cảnh báo khi có sự thay đổi.

c) 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.

Mục 4
QUẢN LÝ VẬN HÀNH

Điều 11. Trách nhiệm, quy trình quản lý vận hành

1) Ban hành đầy đủ các quy trình vận hành đối với hệ thống thông tin, tối thiểu bao gồm: quy vận hành hệ thống CNTT; quy trình sao lưu, phục hồi dữ liệu; quy trình vận hành ứng dụng; quy trình xử lý sự cố; quy trình giám sát và ghi nhật ký hoạt động của hệ thống; quy trình xử lý sự cố khi có thảm họa. Trong đó phải xác định rõ phạm vi, trách nhiệm của người sử dụng, vận hành hệ thống. Định kỳ tối thiểu mỗi năm một lần, tổ chức thực hiện rà soát, cập nhật, bổ sung các quy trình vận hành hệ thống thông tin để phù hợp thực tế.

2) Đảm bảo giám sát an toàn toàn thông tin riêng cho hệ thống theo quy định của pháp luật.

3) Tổ chức triển khai các quy trình đến toàn bộ các đối tượng tham gia vận hành và giám sát tuân thủ việc thực hiện các quy trình đã ban hành.

4) Môi trường vận hành của hệ thống dịch vụ phải tách biệt với các môi trường phát triển, kiểm tra và thử nghiệm.

5) Mọi thao tác trên hệ thống phải được lưu vết, sẵn sàng cho kiểm tra, kiểm soát khi cần thiết.

6) Lập kế hoạch và tổ chức giám sát, tối ưu hiệu suất của hệ thống thông tin; đánh giá khả năng đáp ứng, tình trạng hoạt động, cấu hình hệ thống của hệ thống thông tin để dự báo, lập kế hoạch mở rộng, nâng cấp bảo đảm khả năng đáp ứng trong tương lai.

7) Định kỳ hàng năm tổ chức diễn tập đảm bảo an toàn thông tin cho hệ thống.

8) Triển khai ứng cứu khẩn cấp đảm bảo an toàn hệ thống thông tin theo quy định của pháp luật.

Điều 12. Sao lưu dự phòng

1) Lập danh sách hệ thống thông tin cần được sao lưu, kèm theo thời gian lưu trữ, định kỳ sao lưu, phương pháp sao lưu và thời gian kiểm tra phục hồi hệ thống từ dữ liệu sao lưu.

2) Dữ liệu của các hệ thống thông tin phải có phương án tự động sao lưu phù hợp với tần suất thay đổi của dữ liệu và bảo đảm nguyên tắc dữ liệu phát sinh phải được sao lưu trong vòng 24 giờ. Dữ liệu sao lưu phải được lưu trữ ra phương tiện lưu trữ ngoài (như băng từ, đĩa cứng, đĩa quang hoặc phương tiện lưu trữ khác) và cất giữ, bảo quản an toàn tách rời với khu vực lắp đặt hệ thống thông tin nguồn.

3) Phải kiểm tra, phục hồi dữ liệu sao lưu từ phương tiện lưu trữ ngoài tối thiểu sáu tháng một lần.

Điều 13. Giám sát và ghi nhật ký hoạt động của hệ thống thông tin

Thực hiện giám sát và ghi nhật ký hoạt động của hệ thống thông tin như sau:

1. Thực hiện việc giám sát an toàn an ninh hệ thống thông tin của Công ty, các đối tượng phải được giám tối thiểu: Tường lửa; Sự truy nhập; Tuyến thông tin chủ yếu; Máy chủ quan trọng; Thiết bị quan trọng.

2. Ghi và lưu trữ nhật ký về hoạt động của hệ thống thông tin và người sử dụng, các lỗi phát sinh, các sự cố an toàn thông tin. Dữ liệu nhật ký của các hệ thống thông tin phải được lưu trữ trực tuyến tối thiểu 3 tháng theo hình thức tập trung và sao lưu tối thiểu một năm.

3. Bảo vệ các chức năng ghi nhật ký và thông tin nhật ký, chống giả mạo và truy cập trái phép; bảo đảm người quản trị hệ thống và người sử dụng không thể xóa hay sửa đổi nhật ký hệ thống ghi lại các hoạt động của chính họ.

4. Thực hiện việc đồng bộ thời gian giữa các hệ thống thông tin.

Điều 14. Phòng chống mã độc

Xây dựng và thực hiện quy định quy trình về phòng chống mã độc như sau:

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

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

3. Cập nhật mẫu mã độc và phần mềm phòng chống mã độc mới.

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

5. Kiểm soát việc cài đặt phần mềm bảo đảm tuân thủ theo quy chế an toàn thông tin của tổ chức.

6. Kiểm soát thư điện tử lạ, các tệp tin đính kèm hoặc các liên kết trong các thư lạ.

Mục 5
QUẢN LÝ TRUY CẬP

Điều 15. Quản lý truy cập

1) Kiểm soát truy cập đối với người sử dụng, nhóm người sử dụng, các thiết bị, công cụ sử dụng để truy cập hệ thống thông tin bảo đảm đáp ứng yêu cầu nghiệp vụ và yêu cầu an toàn thông tin, bao gồm các nội dung cơ bản sau:

a) Đăng ký, cấp phát, gia hạn và thu hồi quyền truy cập của người sử dụng;

b) Mỗi tài khoản truy cập hệ thống phải được gán cho một người sử dụng duy nhất; trường hợp chia sẻ tài khoản dùng chung để truy cập hệ thống thông tin thì phải được phê duyệt bởi phục trách và xác định được trách nhiệm cá nhân tại mỗi thời điểm sử dụng;

c) Phải giới hạn và kiểm soát các truy cập sử dụng tài khoản có quyền quản trị: (i) Thiết lập cơ chế kiểm soát việc tạo tài khoản có quyền quản trị để bảo đảm không một tài khoản nào sử dụng được khi chưa được cấp có thẩm quyền phê duyệt; (ii) Phải có biện pháp giám sát việc sử dụng tài khoản có quyền quản trị; (iii) Việc sử dụng tài khoản có quyền quản trị phải được giới hạn trong khoảng thời gian đủ để thực hiện công việc và phải được thu hồi ngay sau khi kết thúc công việc;

d) Quản lý, cấp phát mã khóa bí mật truy cập hệ thống thông tin;

đ) Rà soát, kiểm tra, xét duyệt lại quyền truy cập của người sử dụng.

2) Quy định về trách nhiệm của người sử dụng khi được cấp quyền truy cập bao gồm các nội dung: sử dụng mã khóa bí mật đúng quy định; giữ bí mật mã khóa bí mật; sử dụng thiết bị, công cụ để truy cập; thoát khỏi hệ thống khi không làm việc hoặc tạm thời không làm việc trên hệ thống.

3) Quản lý việc truy cập sử dụng mạng nội bộ bao gồm trách nhiệm của người quản trị, người truy cập. Kiểm soát việc quản trị, truy cập, sử dụng mạng. Và:

a) Thực hiện các biện pháp kiểm soát chặt chẽ các kết nối từ mạng không tin cậy vào mạng nội bộ của tổ chức bảo đảm an toàn thông tin;

b) Kiểm soát việc cài đặt, sử dụng các công cụ phần mềm hỗ trợ truy cập từ xa;

c) Kiểm soát truy cập các cổng dùng để cấu hình và quản trị thiết bị mạng;

d) Cấp quyền truy cập mạng và dịch vụ mạng phải bảo đảm nguyên tắc quyền vừa đủ để thực hiện nhiệm vụ được giao;

đ) Kết nối từ mạng Internet vào mạng nội bộ của tổ chức để phục vụ công việc phải sử dụng mạng riêng ảo và xác thực đa thành tố.

Điều 16. Quản lý kết nối Internet

1) Triển khai các giải pháp an ninh mạng tại các cổng kết nối Internet để bảo đảm an toàn trước các hiểm họa tấn công từ Internet vào mạng nội bộ của Công ty.

2) Sử dụng các công cụ để dò tìm và phát hiện kịp thời các điểm yếu, lỗ hổng và các tấn công, truy cập bất hợp pháp vào hệ thống mạng nội bộ của Công ty thông qua cổng kết nối Internet.

Mục 6

ĐẢM BẢO HỆ THỐNG SẢN PHẨM DỊCH VỤ CÔNG TY

Điều 17. Đảm bảo an toàn hệ thống dịch vụ trực tuyến của Công ty

Phần 1

Danh sách

Danh sách các hệ thống và dịch vụ trực tuyến của Công ty:

1. Hệ thống hỗ trợ điều hành, nghiệp vụ và hồ sơ điện tử CA2
2. Hệ thống Chứng thực và xác thực chữ ký số công cộng CA2 bao gồm cả Mobile Sign.
3. Hệ thống dấu thời gian số CA2 TSA
4. Hệ thống hóa đơn điện tử CA2-eInvoice
5. Hệ thống hồ sơ cấp C/O điện tử CO-VAN-CA2
6. Các hệ thống dịch vụ khác sẽ được cập nhật khi đưa vào khai thác sử dụng.

Mỗi hệ thống dịch vụ có quy chế riêng, trên cơ sở yêu cầu chung như sau:

Phần 2

Hồ sơ căn cứ xây dựng quy chế hệ thống và dịch vụ

1) Yêu cầu chung, tài liệu mô tả, thuyết minh tổng quan đối với hệ thống thông tin cung cấp dịch vụ trực tuyến;

2) Tài liệu thiết kế về hệ thống và các tiêu chuẩn quy chuẩn bắt buộc;

3) Tài liệu thuyết minh phương án đảm bảo an toàn, sẵn sàng;

4) Hồ sơ phê duyệt các nội dung trên bao gồm các quy trình, thủ tục liên quan;

Phần 3

Yêu cầu an ninh, an toàn

1) Bảo đảm tính toàn vẹn của dữ liệu trao đổi với khách hàng trong giao dịch trực tuyến;

2) Dữ liệu trên đường truyền phải bảo đảm tính bí mật và phải được truyền đầy đủ, đúng địa chỉ và có biện pháp bảo vệ để tránh bị sửa đổi hoặc nhân bản trái phép;

3) Đánh giá mức độ rủi ro trong giao dịch trực tuyến theo đối tượng khách hàng, loại giao dịch, mức giao dịch để cung cấp giải pháp xác thực giao dịch phù hợp;

4) Cổng giao tiếp điện tử giao dịch trực tuyến phải được áp dụng các biện pháp chứng thực chống giả mạo và ngăn chặn, chống sửa đổi trái phép.

5) Hệ thống dịch vụ giao dịch trực tuyến phải được áp dụng các biện pháp để giám sát chặt chẽ và phát hiện, cảnh báo về:

a) Giao dịch đáng ngờ dựa vào các tiêu chí tối thiểu gồm: thời gian giao dịch, địa điểm giao dịch (vị trí địa lý, địa chỉ IP mạng), tần suất giao dịch, số lần xác thực sai quy định;

b) Hoạt động bất thường của hệ thống;

c) Các cuộc tấn công từ chối dịch vụ (DoS - Denial of Service attack), tấn công từ chối dịch vụ phân tán (DDoS - Distributed Denial of Service attack).

6) Tổ chức hướng dẫn các biện pháp bảo đảm an toàn thông tin và cảnh bảo rủi ro cho khách hàng trước khi tham gia sử dụng dịch vụ giao dịch trực tuyến và theo định kỳ.

7) Khi cung cấp phần mềm ứng dụng giao dịch trực tuyến trên Internet phải áp dụng các biện pháp bảo đảm tính toàn vẹn của phần mềm.

Phần 4

Quy chế tối thiểu gồm các nội dung cơ bản sau

1) Chính sách hệ thống, dịch vụ, cấp độ an toàn an ninh và mục tiêu hệ thống, dịch vụ tham chiếu cơ sở Quy chế chính sách này;

2) Phương thức và hình thức phổ biến công bố các quy định đối với hệ thống và dịch vụ;

3) Yêu cầu về hồ sơ định danh, thẩm định xác thực, quản lý sử dụng, lưu trữ thông tin thuê bao;

4) Nghĩa vụ và trách nhiệm pháp lý;

5) Các yêu cầu về quy trình, thủ tục hoạt động quản lý và vận hành hệ thống, dịch vụ;

6) Quản lý tài sản công nghệ thông tin;

7) Quản lý nguồn nhân lực;

8) Đảm bảo an ninh an toàn cơ sở vật chất, quản lý và vận hành hệ thống;

9) Quản lý sự cố, bảo đảm hoạt động liên tục;

10) Giám sát, kiểm tra nội bộ và chế độ báo cáo.

Mục 7

QUẢN LÝ SỬ DỤNG DỊCH VỤ HỆ THỐNG CỦA BÊN THỨ BA

Điều 18. Các nguyên tắc chung về sử dụng dịch vụ của bên thứ ba

Khi sử dụng dịch vụ công nghệ thông tin của bên thứ ba, phải bảo đảm các nguyên tắc sau đây:

1. Không làm suy giảm khả năng cung cấp dịch vụ liên tục của Công ty cho khách hàng.
2. Không làm suy giảm việc kiểm soát quy trình nghiệp vụ của Công ty.
3. Không làm thay đổi trách nhiệm của Công ty trong việc bảo đảm an toàn thông tin.
4. Dịch vụ công nghệ thông tin của bên thứ ba phải đáp ứng các quy định về bảo đảm an toàn thông tin của Công ty.

Điều 19. Các yêu cầu khi sử dụng dịch vụ của bên thứ ba

Trước khi sử dụng dịch vụ của bên thứ ba, phải thực hiện:

1. Đánh giá rủi ro công nghệ thông tin, rủi ro hoạt động tối thiểu bao gồm các nội dung sau:

a) Nhận diện rủi ro, phân tích, ước lượng mức độ tổn hại, mối đe dọa đến an toàn thông tin;

b) Khả năng kiểm soát các quy trình nghiệp vụ, khả năng cung cấp dịch vụ liên tục cho khách hàng, khả năng thực hiện nghĩa vụ cung cấp thông tin cho các cơ quan nhà nước;

c) Xác định rõ vai trò, trách nhiệm của các bên liên quan trong việc bảo đảm chất lượng dịch vụ;

d) Xây dựng các biện pháp nhằm giảm thiểu rủi ro, biện pháp phòng ngừa, ứng cứu, khắc phục sự cố;

đ) Rà soát và điều chỉnh chính sách quản lý rủi ro (nếu có).

2. Trong trường hợp sử dụng dịch vụ điện toán đám mây, ngoài các yêu cầu tại khoản 1 Điều này, phải thực hiện:

a) Phân loại hoạt động, nghiệp vụ dự kiến triển khai trên điện toán đám mây dựa trên đánh giá tác động của hoạt động, nghiệp vụ đó với hoạt động của Công ty;

b) Xây dựng phương án dự phòng đối với các cấu phần của hệ thống thông tin. Phương án dự phòng phải được kiểm thử và đánh giá sẵn sàng thay thế cho các hoạt động, nghiệp vụ triển

khai trên điện toán đám mây;

c) Xây dựng các tiêu chí lựa chọn bên thứ ba đáp ứng yêu cầu;

d) Rà soát, bổ sung, áp dụng các biện pháp bảo đảm an toàn thông tin của Công ty, giới hạn truy cập từ điện toán đám mây đến các hệ thống thông tin của Công ty.

3. Trường hợp thuê bên thứ ba thực hiện toàn bộ công việc quản trị hệ thống thông tin, phải thực hiện đánh giá rủi ro theo quy định tại khoản 1 Điều này.

Điều 20. Hợp đồng sử dụng dịch vụ với bên thứ ba

Hợp đồng sử dụng dịch vụ ký kết với bên thứ ba phải có tối thiểu những nội dung sau:

1. Cam kết của bên thứ ba về bảo đảm an toàn thông tin bao gồm:

a) Đáp ứng yêu cầu theo quy định;

b) Không sao chép, thay đổi, sử dụng hay cung cấp dữ liệu của Công ty sử dụng dịch vụ cho cá nhân, tổ chức khác, trừ trường hợp có yêu cầu của cơ quan Nhà nước có thẩm quyền theo quy định của pháp luật; trong trường hợp này, bên thứ ba phải thông báo cho tổ chức sử dụng dịch vụ trước khi cung cấp dữ liệu, trừ khi việc thông báo sẽ vi phạm pháp luật Việt Nam;

c) Phổ biến cho nhân sự của bên thứ ba tham gia thực hiện hợp đồng các quy định về bảo đảm an toàn thông tin của tổ chức, thực hiện các biện pháp giám sát bảo đảm tuân thủ.

2. Quy định cụ thể thời gian tối đa có thể gián đoạn dịch vụ và thời gian khắc phục sự cố, các yêu cầu liên quan đến bảo đảm hoạt động liên tục (dự phòng tại chỗ, sao lưu dữ liệu, dự phòng thảm họa), các yêu cầu liên quan đến năng lực xử lý, tính toán, lưu trữ, các biện pháp thực hiện khi chất lượng dịch vụ không được bảo đảm.

3. Trường hợp bên thứ ba sử dụng nhà thầu phụ không làm thay đổi trách nhiệm của bên thứ ba đối với dịch vụ mà tổ chức sử dụng.

4. Dữ liệu phát sinh trong quá trình sử dụng dịch vụ là tài sản của Công ty. Khi chấm dứt sử dụng dịch vụ:

a) Bên thứ ba thực hiện trả lại toàn bộ dữ liệu triển khai và dữ liệu phát sinh trong quá trình sử dụng dịch vụ;

b) Bên thứ ba cam kết hoàn thành việc xoá toàn bộ dữ liệu của Công ty trong một khoảng thời gian xác định.

5. Bên thứ ba phải thông báo cho Công ty khi phát hiện nhân sự vi phạm quy định về an toàn thông tin đối với dịch vụ mà Công ty sử dụng.

6. Hợp đồng sử dụng dịch vụ điện toán đám mây, ngoài các nội dung quy định tại các khoản 1, 2, 3, 4, 5 Điều này, phải bổ sung thêm những nội dung sau:

a) Bên thứ ba phải cung cấp báo cáo kiểm toán tuân thủ công nghệ thông tin do tổ chức kiểm toán độc lập thực hiện hàng năm trong thời gian thực hiện hợp đồng;

b) Bên thứ ba phải cung cấp: công cụ kiểm soát chất lượng dịch vụ đám mây; quy trình giám sát, kiểm soát chất lượng dịch vụ đám mây;

c) Bên thứ ba phải minh bạch các vị trí (thành phố, quốc gia) đặt trung tâm dữ liệu bên ngoài lãnh thổ Việt Nam triển khai dịch vụ cho tổ chức;

d) Trách nhiệm bảo vệ dữ liệu, chống truy cập dữ liệu trái phép trên kênh phân phối dịch vụ từ bên thứ ba đến Công ty;

đ) Bên thứ ba phải hỗ trợ, hợp tác điều tra trong trường hợp có yêu cầu từ các cơ quan nhà nước có thẩm quyền theo quy định của pháp luật;

e) Dữ liệu của Công ty phải được tách biệt với dữ liệu của khách hàng khác sử dụng trên cùng nền tảng kỹ thuật do bên thứ ba cung cấp.

Điều 21. Trách nhiệm của Công ty trong quá trình sử dụng dịch vụ của bên thứ ba

1. Cung cấp, thông báo và yêu cầu bên thứ ba thực hiện các quy định về an toàn thông tin của Công ty.

2. Có quy trình và bố trí nguồn lực để giám sát, kiểm soát các dịch vụ do bên thứ ba cung cấp bảo đảm chất lượng dịch vụ theo thỏa thuận đã ký kết. Đối với dịch vụ điện toán đám mây, phải giám sát, kiểm soát chất lượng dịch vụ.

3. Áp dụng các quy định về an toàn thông tin của Công ty đối với trang thiết bị, dịch vụ do bên thứ ba cung cấp được triển khai trên hạ tầng do Công ty quản lý, sử dụng.

4. Quản lý các thay đổi đối với dịch vụ do bên thứ ba cung cấp bao gồm: thay đổi nhà cung cấp, thay đổi giải pháp, thay đổi phiên bản, thay đổi các nội dung quy định tại Điều 26; đánh giá đầy đủ tác động của việc thay đổi, bảo đảm an toàn khi được đưa vào sử dụng.

5. Áp dụng các biện pháp giám sát chặt chẽ và giới hạn quyền truy cập của bên thứ ba khi cho phép bên thứ ba truy cập vào hệ thống thông tin của Công ty.

6. Giám sát nhân sự của bên thứ ba trong quá trình thực hiện hợp đồng. Trường hợp phát hiện nhân sự bên thứ ba vi phạm quy định về an toàn thông tin phải thông báo và phối hợp với bên thứ ba áp dụng biện pháp xử lý kịp thời.

7. Thu hồi quyền truy cập hệ thống thông tin đã được cấp cho bên thứ ba, thay đổi các khoá, mã khóa bí mật nhận bàn giao từ bên thứ ba ngay sau khi hoàn thành công việc hoặc kết thúc hợp đồng.

8. Đối với hệ thống thông tin hoặc hệ thống thông tin sử dụng dịch vụ điện toán đám mây,

phải đánh giá sự tuân thủ các quy định về bảo đảm an toàn thông tin của bên thứ ba theo đúng thỏa thuận đã ký kết. Thực hiện đánh giá sự tuân thủ định kỳ hàng năm hoặc đột xuất khi có nhu cầu. Việc đánh giá tuân thủ có thể sử dụng kết quả kiểm toán công nghệ thông tin của tổ chức kiểm toán độc lập.

Mục 8

QUẢN LÝ TIẾP NHẬN, PHÁT TRIỂN, DUY TRÌ HỆ THỐNG THÔNG TIN

Điều 22. Yêu cầu về an toàn, bảo mật các hệ thống thông tin

Khi xây dựng mới hoặc nâng cấp hệ thống thông tin phải thực hiện:

1. Xây dựng tài liệu thiết kế, mô tả về các phương án bảo đảm an toàn hệ thống thông tin. Trong đó các yêu cầu về an toàn, bảo mật được xây dựng đồng thời với việc xây dựng các yêu cầu kỹ thuật, nghiệp vụ.

2. Xây dựng phương án kiểm tra, xác minh hệ thống được triển khai tuân thủ theo đúng tài liệu thiết kế và yêu cầu bảo đảm an toàn thông tin trước khi nghiệm thu. Kết quả kiểm tra phải lập thành hồ sơ báo cáo và được phê duyệt trước khi đưa vào vận hành chính thức.

3. Giám sát, quản lý chặt chẽ việc thuê mua phần mềm bên ngoài. theo quy định tại Điều 21.

Điều 23. Bảo đảm an toàn, bảo mật ứng dụng nghiệp vụ

Các chương trình ứng dụng nghiệp vụ phải đáp ứng các yêu cầu tối thiểu sau:

1. Kiểm tra tính hợp lệ của dữ liệu nhập vào các ứng dụng, bảo đảm dữ liệu được nhập vào chính xác và hợp lệ.

2. Kiểm tra tính hợp lệ của dữ liệu cần được xử lý tự động trong các ứng dụng nhằm phát hiện thông tin sai lệch do các lỗi trong quá trình xử lý hoặc các hành vi sửa đổi thông tin có chủ ý.

3. Có các biện pháp bảo đảm tính xác thực và bảo vệ sự toàn vẹn của dữ liệu được xử lý trong các ứng dụng.

4. Kiểm tra tính hợp lệ của dữ liệu xuất ra từ các ứng dụng, bảo đảm quá trình xử lý thông tin của các ứng dụng là chính xác và hợp lệ.

5. Mã khóa bí mật của người sử dụng trong các hệ thống thông tin phải được mã hóa ở lớp ứng dụng.

Điều 24. Quản lý mã hóa

Tổ chức quản lý mã hóa như sau:

1. Quy định và đưa vào sử dụng các biện pháp mã hóa theo quy chuẩn kỹ thuật quốc gia về mã hóa dữ liệu sử dụng trong giao dịch điện tử hoặc tiêu chuẩn quốc tế đã được công nhận.

2. Có biện pháp quản lý khóa mã hóa để bảo vệ thông tin của Công ty.

Điều 25. An toàn, bảo mật trong quá trình phát triển phần mềm

1. Tổ chức thực hiện quản lý quá trình phát triển phần mềm như sau:

a) Quản lý, kiểm soát chương trình nguồn. Việc truy cập, tiếp cận chương trình nguồn phải được sự phê duyệt của BGĐ;

b) Quản lý, bảo vệ tệp tin cấu hình hệ thống.

2. Tổ chức lựa chọn, kiểm soát đối với dữ liệu kiểm tra, thử nghiệm. Không sử dụng dữ liệu thật của hệ thống thông tin vận hành chính thức cho hoạt động kiểm thử khi chưa thực hiện các biện pháp che giấu hoặc thay đổi đối với dữ liệu chứa thông tin khách hàng và thông tin bí mật.

Điều 26. Quản lý sự thay đổi hệ thống thông tin

Tổ chức ban hành quy trình, biện pháp quản lý và kiểm soát sự thay đổi hệ thống thông tin, tối thiểu bao gồm:

1. Thực hiện ghi chép lại các thay đổi; lập kế hoạch thay đổi; thực hiện kiểm tra, thử nghiệm sự thay đổi, báo cáo kết quả; phê duyệt kế hoạch thay đổi trước khi áp dụng chính thức thay đổi phiên bản phần mềm, cấu hình phần cứng, tham số phần mềm hệ thống, quy trình vận hành. Có phương án dự phòng cho việc phục hồi hệ thống trong trường hợp thực hiện thay đổi không thành công hoặc gặp các sự cố không có khả năng dự tính trước.

2. Kiểm tra, đánh giá tác động để bảo đảm hệ thống thông tin hoạt động ổn định, an toàn trên môi trường mới đối với hệ thống thông tin khi thay đổi phiên bản hoặc thay đổi hệ điều hành, cơ sở dữ liệu, phần mềm lớp giữa phải.

Điều 27. Đánh giá an ninh bảo mật hệ thống thông tin

1. Nội dung đánh giá hệ thống thông tin về an ninh bảo mật phải bao gồm các nội dung sau:

a) Đánh giá về kiến trúc hệ thống để xác định tính phù hợp của các thiết bị lắp đặt với kiến trúc hệ thống tổng thể và yêu cầu về an ninh bảo mật;

b) Kiểm tra cấu hình các thiết bị bảo mật, các hệ thống cấp quyền truy cập tự động, hệ thống quản lý thiết bị đầu cuối, danh sách tài khoản;

c) Kiểm tra thử nghiệm mức độ an toàn mạng (Penetration Test), bắt buộc phải thực hiện đối với các hệ thống thông tin có kết nối và cung cấp thông tin, dịch vụ ra Internet, kết nối với khách hàng và bên thứ ba.

2. Tổ chức thực hiện đánh giá an ninh bảo mật đối với hệ thống thông tin theo các nội dung quy định tại khoản 1 Điều này trước khi đưa vào vận hành chính thức.

3. Trong quá trình vận hành hệ thống thông tin, định kỳ thực hiện đánh giá an ninh bảo mật tối thiểu như sau:

a) Sáu tháng một lần đối với các thành phần hệ thống thông tin quan trọng theo các nội dung tại khoản 1 Điều này;

b) Một năm một lần đối với các hệ thống thông tin và các trang thiết bị giao tiếp trực tiếp với môi trường bên ngoài như Internet, kết nối với khách hàng và bên thứ ba theo các nội dung tại khoản 1 Điều này;

4. Kết quả đánh giá phải được lập thành văn bản báo cáo BGĐ. Đối với các nội dung chưa tuân thủ quy định về an toàn thông tin (nếu có) phải đề xuất biện pháp, kế hoạch, thời hạn xử lý, khắc phục.

Điều 27. Quản lý các điểm yếu về mặt kỹ thuật

Tổ chức quản lý các điểm yếu về mặt kỹ thuật như sau:

1. Xây dựng quy trình về việc đánh giá, quản lý và kiểm soát các điểm yếu về mặt kỹ thuật của các hệ thống thông tin đang sử dụng.

2. Chủ động phát hiện các điểm yếu về mặt kỹ thuật thông qua các hoạt động:

a) Thường xuyên cập nhật thông tin liên quan đến lỗ hổng, điểm yếu về mặt kỹ thuật;

b) Thực hiện dò quét, phát hiện các mã độc, lỗ hổng, điểm yếu về mặt kỹ thuật của các hệ thống thông tin đang sử dụng định kỳ tối thiểu như sau: (i) Ba tháng một lần đối với hệ thống thông tin quan trọng hoặc các hệ thống thông tin có kết nối với mạng Internet; (ii) Sáu tháng một lần đối với các hệ thống thông tin còn lại.

3. Đánh giá mức độ tác động, rủi ro của từng lỗ hổng, điểm yếu về mặt kỹ thuật được phát hiện của các hệ thống thông tin đang sử dụng và đưa ra phương án, kế hoạch xử lý.

4. Xây dựng, tổ chức triển khai các quy trình, giải pháp xử lý, khắc phục và báo cáo kết quả xử lý.

Điều 28. Quản lý bảo trì hệ thống thông tin

Tổ chức quản lý bảo trì hệ thống thông tin như sau:

1. Ban hành quy định bảo trì hệ thống thông tin ngay sau khi đưa vào hoạt động chính thức. Quy định bảo trì tối thiểu bao gồm các nội dung sau:

a) Phạm vi, các đối tượng được bảo trì;

b) Thời điểm, tần suất bảo trì;

c) Quy trình, kịch bản kỹ thuật để thực hiện bảo trì của từng cấu phần và toàn bộ hệ thống thông tin;

d) Khi thực hiện bảo trì nếu phát hiện, phát sinh sự cố phải báo cáo BGĐ để xử lý;

đ) Phân công và xác định trách nhiệm của bộ phận thực hiện bảo trì và giám sát bảo trì.

2. Thực hiện bảo trì theo quy định tại khoản 1 Điều này.

3. Rà soát quy định bảo trì tối thiểu một năm một lần hoặc khi hệ thống thông tin có sự thay đổi.

Mục 9
QUẢN LÝ SỰ CỐ AN TOÀN THÔNG TIN

Điều 29. Quy trình xử lý sự cố

Tổ chức quản lý sự cố như sau:

1. Ban hành quy trình xử lý sự cố an toàn thông tin bao gồm những nội dung tối thiểu sau:

a) Tiếp nhận thông tin về sự cố phát sinh;

b) Đánh giá mức độ, phạm vi ảnh hưởng của sự cố đến hoạt động của hệ thống thông tin. Tùy theo mức độ, phạm vi ảnh hưởng của sự cố phải báo cáo đến các cấp quản lý tương ứng để chỉ đạo xử lý;

c) Thực hiện các biện pháp xử lý, khắc phục sự cố;

d) Ghi nhận hồ sơ và báo cáo kết quả xử lý sự cố.

2. Quy định trách nhiệm của cá nhân, tập thể trong việc báo cáo, tiếp nhận, xử lý các sự cố an toàn thông tin.

3. Xây dựng các mẫu biểu để ghi nhận, lưu trữ hồ sơ xử lý sự cố.

Điều 30. Kiểm soát và khắc phục sự cố

Tổ chức kiểm soát và khắc phục sự cố như sau:

1. Lập danh sách sự cố an toàn thông tin và phương án xử lý sự cố đối với các hệ thống thông tin; tối thiểu 6 tháng một lần thực hiện rà soát, cập nhật danh sách, phương án ứng cứu sự cố.

2. Lập tức báo cáo đến cấp quản lý tương ứng và những người có liên quan khi phát sinh sự cố an toàn thông tin để có biện pháp khắc phục trong thời gian sớm nhất.

3. Trong quá trình kiểm tra, xử lý, khắc phục sự cố thu thập, ghi chép, bảo vệ chứng cứ và lưu trữ tại Công ty.

4. Đánh giá xác định nguyên nhân và thực hiện các biện pháp phòng ngừa tránh sự cố tái diễn sau khi khắc phục sự cố,.

5. Trong trường hợp sự cố an toàn thông tin có liên quan đến các vi phạm pháp luật, phải có trách nhiệm thu thập và cung cấp chứng cứ cho cơ quan có thẩm quyền đúng theo quy định của pháp luật.

Điều 31. Bộ phận giám sát, điều hành an toàn an ninh hệ thống thông tin Công ty

Bộ phận giám sát, điều hành an toàn an ninh hệ thống thông tin Công ty thực hiện các nhiệm

vụ sau:

1. Chủ động theo dõi, thu thập, tiếp nhận các thông tin, cảnh báo về các nguy cơ, rủi ro an toàn thông tin từ bên trong và bên ngoài.

2. Xây dựng hệ thống quản lý và phân tích sự kiện an toàn thông tin (SIEM), thực hiện thu thập và lưu trữ tập trung tối thiểu các thông tin: nhật ký của các hệ thống thông tin; cảnh báo, nhật ký của trang thiết bị an ninh mạng (tường lửa, IPS/IDS).

3. Phân tích thông tin để phát hiện và cảnh báo về các rủi ro và các nguy cơ tấn công mạng, sự cố an ninh mạng và phải gửi cảnh báo đến người quản trị hệ thống khi phát hiện sự cố liên quan đến các hệ thống: (i) Hệ thống thông tin phục vụ khách hàng yêu cầu hoạt động 24/7; (ii) Hệ thống cung cấp giao dịch trực tuyến; (iii) Hệ thống thông tin mức độ 3.

4. Tổ chức điều phối ứng cứu sự cố và khoanh vùng, ngăn chặn, giảm thiểu tác động, thiệt hại đến hệ thống thông tin khi sự cố phát sinh.

5. Điều tra, xác định nguồn gốc, cách thức, phương pháp tấn công và thực hiện các biện pháp phòng ngừa tránh sự số tái diễn.

Mục 10

BẢO ĐẢM HOẠT ĐỘNG LIÊN TỤC CỦA HỆ THỐNG THÔNG TIN

Điều 32. Nguyên tắc bảo đảm hoạt động liên tục

1. Thực hiện các yêu cầu tối thiểu sau:

a) Phân tích tác động và đánh giá rủi ro đối với việc gián đoạn hoặc ngừng hoạt động của hệ thống thông tin;

b) Xây dựng quy trình và kịch bản bảo đảm hoạt động liên tục hệ thống thông tin theo quy định tại Điều 34;

c) Tổ chức triển khai bảo đảm hoạt động liên tục theo quy định tại Điều 35.

2. Trên cơ sở phân tích tác động và đánh giá rủi ro tại điểm a khoản 1 Điều này, lập danh sách các hệ thống thông tin cần bảo đảm hoạt động liên tục tối thiểu bao gồm:

a) Hệ thống thông tin phục vụ hoạt động nội bộ hàng ngày của Công ty và không chấp nhận ngừng vận hành quá 4 giờ làm việc;

b) Hệ thống phục vụ khách hàng yêu cầu hoạt động 24/7;

c) Hệ thống cung cấp giao dịch trực tuyến cho khách hàng;

3. Các hệ thống cần bảo đảm hoạt động liên tục tại Khoản 2 Điều này phải bảo đảm tính sẵn sàng cao và có hệ thống dự phòng thảm họa.

Điều 33. Hệ thống dự phòng thảm họa

Hệ thống dự phòng thảm họa đáp ứng các yêu cầu sau:

1) Đánh giá rủi ro và xem xét khả năng xảy ra các thảm họa ảnh hưởng đồng thời tới cả hệ thống thông tin chính và hệ thống thông tin dự phòng thảm họa khi lựa chọn địa điểm đặt hệ thống dự phòng thảm họa như: thảm họa tự nhiên như động đất, lũ lụt, bão, đại dịch; thảm họa do yếu tố con người và công nghệ như các sự cố về mạng lưới điện, hỏa hoạn, giao thông, tấn công an ninh mạng;

2) Địa điểm đặt hệ thống dự phòng phải đáp ứng các yêu cầu theo quy định;

3) Hệ thống dự phòng phải bảo đảm khả năng thay thế hệ thống chính trong khoảng thời gian: (i) 4 giờ đồng hồ đối với: hệ thống thông tin phục vụ hoạt động nội bộ hàng ngày của tổ chức và không chấp nhận ngừng vận hành quá 4 giờ làm việc, hệ thống phục vụ khách hàng yêu cầu hoạt động 24/7, hệ thống cung cấp giao dịch trực tuyến cho khách hàng; (ii) 24 giờ đồng hồ đối với các hệ thống khác.

Điều 34. Xây dựng quy trình, kịch bản bảo đảm hoạt động liên tục

Xây dựng quy trình, kịch bản bảo đảm hoạt động liên tục như sau:

1. Xây dựng quy trình xử lý các tình huống mất an toàn, gián đoạn hoạt động của từng cấu phần trong hệ thống thông tin.

2. Xây dựng kịch bản chuyển đổi hệ thống dự phòng thay thế cho hoạt động của hệ thống chính, bao gồm nội dung công việc, trình tự thực hiện, dự kiến thời gian hoàn thành đáp ứng các nội dung sau:

a) Có các nguồn lực, phương tiện và các yêu cầu cần thiết để thực hiện;

b) Có các mẫu biểu ghi nhận kết quả;

c) Bố trí và phân công trách nhiệm cho nhân sự tham gia với các vai trò: chỉ đạo thực hiện, giám sát, thực hiện chuyển đổi, vận hành chính thức và kiểm tra kết quả;

d) Áp dụng biện pháp bảo đảm an toàn thông tin;

đ) Có phương án bảo đảm hoạt động liên tục khi việc chuyển đổi không thành công.

3. Quy trình, kịch bản chuyển đổi phải được kiểm tra và cập nhật khi có sự thay đổi của hệ thống thông tin, cơ cấu tổ chức, nhân sự và phân công trách nhiệm của các bộ phận có liên quan trong Công ty.

Điều 35. Tổ chức triển khai bảo đảm hoạt động liên tục

Xây dựng kế hoạch và tổ chức triển khai bảo đảm hoạt động liên tục hệ thống thông tin theo các yêu cầu sau:

1) Tối thiểu sáu tháng một lần, tiến hành kiểm tra, đánh giá hoạt động của hệ thống dự phòng;

2) Định kỳ hàng năm, thực hiện chuyển hoạt động chính thức từ hệ thống chính sang hệ thống dự phòng tối thiểu 1 ngày làm việc của từng hệ thống thông tin theo danh sách tại khoản 2 Điều 32; đánh giá kết quả và cập nhật các quy trình, kịch bản chuyển đổi (nếu có).

Mục 11

KIỂM TRA NỘI BỘ VÀ CHẾ ĐỘ BÁO CÁO

Điều 36. Kiểm tra nội bộ

Thực hiện kiểm tra nội bộ như sau:

1. Xây dựng quy định kiểm tra nội bộ về công tác bảo đảm an toàn thông tin của tổ chức.

2. Xây dựng kế hoạch và thực hiện công tác tự kiểm tra việc tuân thủ các quy định tại Quy chế này và các quy định nội bộ của tổ chức về bảo đảm an toàn thông tin tối thiểu mỗi năm một lần.

3. Kết quả kiểm tra về công tác bảo đảm an toàn thông tin phải được lập thành báo cáo gửi người đại diện theo pháp luật và cấp quản lý tương ứng, trong đó các vấn đề còn tồn tại chưa bảo đảm tuân thủ các quy định về an toàn thông tin (nếu có) phải có phương án xử lý, kế hoạch thực hiện.

4. Tổ chức thực hiện và báo cáo kết quả khắc phục các tồn tại nêu trong báo cáo theo quy định tại khoản 3 Điều này.

Điều 37. Kiểm tra, đánh giá an toàn thông tin

1. Kiểm tra việc tuân thủ quy định của pháp luật về đảm bảo an toàn hệ thống thông tin.

2. Đánh giá hiệu quả của biện pháp đảm bảo an toàn hệ thống thông tin.

3. Đánh giá phát hiện mã độc, lỗ hổng, điển yếu, thử nghiệm xâm nhập hệ thống.

4. Kiểm tra đánh giá định kỳ hoặc đột xuất theo yêu cầu.

Điều 38. Ứng cứu sự cố an toàn thông tin mạng

1. Quy trình ứng cứu sự cố an toàn thông tin mạng

a) Khi phát hiện dấu hiệu tấn công hoặc sự cố an toàn thông tin mạng cần nhanh chóng báo cho bộ phận giám sát, điều hành an toàn an ninh hệ thống thông tin Công ty.

b) Bộ phận giám sát, điều hành an toàn an ninh hệ thống thông tin Công ty khi phát hiện, tiếp nhận xác minh, xử lý ban đầu và phân loại sự cố an toàn thông tin mạng theo quy định.

c) Quy trình ứng cứu sự cố an toàn thông tin mạng theo quy định tại Phụ Lục Quy trình của Quy chế chính sách này.

2. Diễn tập ứng cứu sự cố an toàn thông tin mạng

Bộ phận giám sát, điều hành an toàn an ninh hệ thống thông tin Công ty theo dõi và tham

gia các khóa diễn tập ứng cứu sự cố do Bộ TTTT tổ chức và phổ biến lại trong Công ty

Điều 39. Đào tạo, bồi dưỡng nghiệp vụ, tuyên truyền, phổ biến nâng cao nhận thức về an toàn thông tin mạng

1. Trung tâm Công nghệ thông tin, bộ phận giám sát điều hành an toàn an ninh hệ thống thông tin Công ty tích cực tham gia đào tạo nâng cấp và cập nhật chuyên môn.

2. Bộ phận giám sát, điều hành an toàn an ninh hệ thống thông tin Công ty định kỳ tổ chức đào tạo, bồi dưỡng nghiệp vụ về an toàn thông tin cho cán bộ công nghệ thông tin, cán bộ chuyên trách an toàn thông tin mạng; đào tạo cơ bản về an toàn thông tin cho cán bộ quản lý, người sử dụng máy tính trong Công ty.

3. Hành chính, công đoàn, bộ phận chuyên trách thường xuyên tổ chức các hoạt động tuyên truyền, phổ biến nâng cao nhận thức về bảo đảm an toàn, an ninh thông tin mạng đến toàn thể Công ty.

Chương III
TRÁCH NHIỆM

Điều 40. Trách nhiệm của Trung tâm nghệ thông tin

1. Thực hiện trách nhiệm quản lý vận hành hệ thống thông tin theo quy định của Quy chế chính sách này.

2. Hướng dẫn triển khai Quy chế chính sách này và các quy định liên quan của Nhà nước.

3. Tổ chức triển khai thực hiện Quy chế chính sách.

4. Xây dựng kế hoạch, báo cáo về an toàn, an ninh hệ thống thông tin của Công ty.

5. Bảo đảm an toàn, an ninh thông tin cho các hệ thống thông tin của Công ty.

6. Chỉ đạo, phân công các bộ phận kỹ thuật (quản lý ứng dụng; quản lý dữ liệu; vận hành hệ thống; triển khai và hỗ trợ kỹ thuật) triển khai công tác bảo đảm an toàn thông tin trong tất cả các công đoạn liên quan đến hệ thống thông tin , bao gồm xây dựng, cập nhật đầy đủ các hồ sơ tài liệu kỹ thuật trong quá trình thực hiện Quy chế này.

Điều 41. Trách nhiệm của các bộ phận Công ty

1. Thực hiện các trách nhiệm nêu trong Quy chế chính sách này.

2. Tổ chức triển khai thực hiện Quy chế chính sách bảo đảm an toàn, an ninh thông tin phù hợp với các yêu cầu cụ thể của từng bộ phận.

3. Phối hợp và thực hiện các báo cáo theo yêu cầu.

4. Thực hiện việc quản lý trang thiết bị công nghệ thông tin và nhân sự theo Quy chế chính sách này.

Điều 42. Trách nhiệm của bộ phận giám sát và điều hành an toàn an ninh hệ thống thông tin Công ty

1. Thực hiện trách nhiệm của bộ phận chuyên trách về an toàn thông tin theo quy định tại Quy chế chính sách này và các nhiệm vụ do cấp quản lý tương ứng giao.

2. Phối hợp chặt chẽ với các bộ phận và kỹ thuật vận hành hệ thống thông tin trong việc bảo đảm an toàn thông tin trong tất cả các công đoạn liên quan đến hệ thống thông tin.

Điều 42. Trách nhiệm cá nhân

1. Cấp quản lý và phụ trách bộ phận có trách nhiệm: phổ biến tới từng nhân sự; thường xuyên kiểm tra việc thực hiện Quy chế chính sách này; chịu trách nhiệm trước pháp luật và Lãnh đạo Công ty về các vi phạm, thất thoát thông tin, dữ liệu do không tổ chức, chỉ đạo, kiểm tra nhân sự của bộ phận thực hiện đúng quy định.

2. Toàn thể nhân sự Công ty, Chi nhánh Công ty và các bên khác thuộc đối tượng áp dụng của quy chế chính sách có trách nhiệm: tuân thủ Quy chế chính sách; thông báo các vấn đề bất thường liên quan tới an toàn thông tin cho Công ty, bộ phận chuyên trách về an toàn thông tin mạng của Công ty; chịu trách nhiệm trước pháp luật và Lãnh đạo Công ty về các vi phạm, thất thoát dữ liệu do không tuân thủ Quy chế chính sách.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 43. Công tác kiểm tra

1. Các bộ phận phải thường xuyên kiểm tra, theo dõi và đánh giá công tác bảo đảm an toàn, an ninh hệ thống thông tin.

2. Bộ phận hành chính định kỳ hàng năm hoặc đột xuất thực hiện kiểm tra, rà soát, đánh giá và báo cáo BGĐ việc thực hiện và cập nhật Quy chế chính sách.

3. Hoạt động kiểm tra, rà soát, đánh giá bảo đảm an toàn hệ thống thông tin cho các sản phẩm, dịch vụ của Công ty phải gồm: Hệ thống thông tin; Máy chủ; Máy trạm; Thiết bị mạng; phần cứng; phần mềm hệ thống; Phần mềm ứng dụng; Hệ thống quản lý, vận hành.

Điều 44. Khen thưởng, kỷ luật

1. Kết quả thực hiện Quy chế chính sách này là một trong những tiêu chí đánh giá kết quả thực hiện hàng năm của cá nhân, bộ phận.

2. Bộ phận, cá nhân vi phạm Quy chế này và các quy định khác của pháp luật về bảo đảm an toàn, an ninh thông tin mạng, tùy theo tính chất, mức độ vi phạm sẽ bị xử lý kỷ luật hoặc các hình thức xử lý khác theo quy định của pháp luật; nếu vi phạm gây thiệt hại đến tài sản, thiết bị, thông

tin, dữ liệu thì chịu trách nhiệm bồi thường theo pháp luật hiện hành.

Điều 45. Trách nhiệm thi hành

1. Cấp quản lý và phụ trách bộ phận có trách nhiệm phổ biến, quán triệt đến toàn bộ nhân sự trong Công ty thực hiện các quy định của Quy chế chính sách này.

2. Trong quá trình thực hiện, nếu có những vấn đề khó khăn, vướng mắc, các bộ phận phản ảnh về hành chính để tổng hợp, trình BGĐ xem xét, sửa đổi, bổ sung quy chế chính sách ./.

Phụ lục1

Các quy trình thủ tục

- Các quy trình vận hành hệ thống

  + Chi tiết theo tài liệu của từng hệ thống

- Các quy trình vận hành ứng dụng, nghiệp vụ

  + Chi tiết theo quy chế của từng hệ thống

- Quy trình kiểm tra, rà soát, đánh giá bảo đảm an toàn hệ thống thông tin
- Quy trình test hệ thống dự phòng
- Quy trình giám sát an toàn hệ thống, quản trị hệ thống từ xa
- Quy trình sao lưu, phục hồi dữ liệu
- Quy trình xử lý sự cố
- Quy trình giám sát và ghi nhật ký hoạt động của hệ thống
- Quy trình xử lý sự cố khi có thảm họa
- Quy trình ứng cứu sự cố an toàn hệ thống thông tin
- Quy trình diễn tập an toàn hệ thống thông tin

Phụ lục 2

Các mẫu báo cáo

NACENCOMM SCT	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**
	Độc lập – Tự do – Hạnh phúc
Số: ...../.....	*……, ngày tháng năm*

BÁO CÁO SỰ CỐ AN TOÀN AN NINH HỆ THỐNG THÔNG TIN CÔNG TY

Mẫu 01 - Báo cáo tiếp nhận sự cố

Kính gửi:

I. THÔNG TIN NGƯỜI BÁO CÁO

- Họ và tên: …… Chức vụ: .....
- Phòng ban:.....
- Địa chỉ: .....
- Điện thoại: …… Email:.....

II. NỘI DUNG BÁO CÁO

1. Hệ thống thông tin gặp sự cố:……

2. Mức độ quan trọng của hệ thống thông tin gặp sự cố:……

3. Thời điểm phát hiện sự cố: …… giờ.... phút ngày …../…../……

4. Mức độ ảnh hưởng ban đầu của sự cố:

- Hệ thống cung cấp dịch vụ cho khách hàng bị tác động ☐

  + Ảnh hưởng đến toàn bộ khách hàng ☐

  + Ảnh hưởng đến một số khách hàng ☐ … / … < *Số lượng khách hàng bị ảnh hưởng/Tổng khách hàng của Hệ thống thông tin*>

- Hệ thống thông tin nội bộ của đơn vị bị tác động ☐

  + Ảnh hưởng đến toàn bộ đơn vị ☐

  + Ảnh hưởng đến một số bộ phận ☐

- Các hệ thống thông tin liên quan bị ảnh hưởng:……

- Mô tả chi tiết:

.....

.....

5. Loại sự cố (theo đánh giá ban đầu)

☐ Tấn công từ chối dịch vụ (DoS/DDoS)
☐ Virus/Worm/Trojan/Malware
☐ Xâm nhập/Tấn công/Truy cập trái phép
☐ Thay đổi giao diện web
☐ Sử dụng/khai thác hệ thống không phù hợp
☐ Tấn công Zero day/APT
☐ Tấn công Phishing/Social engineering
☐ Những sự cố khác (mô tả rõ):

.....

.....

6. Sự cố đã được báo cáo với bất kỳ cơ quan thực thi pháp luật nào chưa (cung cấp rõ tên cơ quan thực thi pháp luật đã được đơn vị báo cáo)**:**

.....

III. KIẾN NGHỊ, ĐỀ XUẤT

.....

.....

.....

……., ngày …. tháng …. năm……

Người báo cáo

(ký, ghi rõ họ tên)

NACENCOMM SCT

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

Độc lập – Tự do – Hạnh phúc

Số: ...../.....

……., ngày tháng năm

BÁO CÁO SỰ CỐ AN TOÀN AN NINH HỆ THỐNG THÔNG TIN CÔNG TY

Mẫu 02 - Báo cáo hoàn thành khắc phục sự cố

Kính gửi:

I. THÔNG TIN NGƯỜI BÁO CÁO

- Họ và tên: …… Chức vụ: .....
- Bộ phận công tác:.....
- Địa chỉ: .....
- Điện thoại: …… Email:.....

II. NỘI DUNG BÁO CÁO

1. Báo cáo cập nhật sự cố (điền đầy đủ thông tin bên dưới) ☐

+ Số văn bản báo cáo (trước đó) về sự cố: .....

+ Ngày báo cáo (trước đó): .....

2. Mức độ ảnh hưởng của sự cố:

- Hệ thống cung cấp dịch vụ cho khách hàng bị tác động ☐

+ Ảnh hưởng đến toàn bộ khách hàng ☐

+ Ảnh hưởng đến một số khách hàng ☐ … / … < *Số lượng khách hàng bị ảnh hưởng/Tổng khách hàng của Hệ thống thông tin*>.

- Hệ thống thông tin nội bộ của đơn vị bị tác động ☐

+ Ảnh hưởng đến toàn bộ đơn vị ☐

+ Ảnh hưởng đến một số bộ phận ☐

- Các hệ thống thông tin liên quan bị ảnh hưởng:……

- Mô tả chi tiết:

.....

.....

3. Sự cố này có liên quan với những sự cố khác đã được báo cáo trước đó ?

☐ Không

☐ Có

- Cung cấp thông tin cụ thể hơn về sự cố trước đó:

.....

.....

.....

- Văn bản báo cáo liên quan đến sự cố đã được báo cáo trước đó: .....

4. Loại sự cố

☐ Tấn công từ chối dịch vụ (DoS/DDoS)

☐ Virus/Worm/Trojan/Malware

☐ Xâm nhập/Tấn công/Truy cập trái phép

☐ Thay đổi giao diện web

☐ Sử dụng/khai thác hệ thống không phù hợp

☐ Tấn công Zero day/APT

☐ Tấn công Phishing/Social engineering

☐ Những sự cố khác (mô tả rõ):

.....

.....

5. Thông tin về hệ thống gặp sự cố:

- Hệ điều hành ..... Version:…..…….

- Các dịch vụ có trên hệ thống *(Đánh dấu những dịch vụ được sử dụng trên hệ thống)*

☐ Hệ thống a ☐ Hệ thống b ☐ Hệ thống n

☐ Dịch vụ khác, đó là.....

- Cổng UDP hoặc TCP nào liên quan đến sự cố ☐ :.....
- Địa chỉ IP Public của những hệ thống bị ảnh hưởng ☐ :.....
- Địa chỉ IP tấn công ☐ :.....

6. Các biện pháp an toàn thông tin đã triển khai (trước khi hệ thống gặp sự cố)**:**

☐ Antivirus ☐ Firewall ☐ Hệ thống phát hiện xâm nhập

☐ Khác:

7. Sự cố đã được báo cáo với bất kỳ cơ quan thực thi pháp luật nào chưa (cung cấp rõ tên cơ quan thực thi pháp luật đã được đơn vị báo cáo)**:**

.....

8. Các hoạt động bảo lưu bằng chứng có được triển khai:

.....

9. Các hoạt động ngăn ngừa, cô lập sự cố có được triển khai:

.....

10. Phương án khắc phục sự cố

(Cung cấp thông tin chi tiết về sự cố: tóm tắt nguyên nhân; các biện pháp đã thực hiện để ngăn chặn, khắc phục và phòng ngừa; thiệt hại liên quan đến sự cố)

.....

III. KIẾN NGHỊ, ĐỀ XUẤT

.....

.....

……., ngày …. tháng …. năm…….

Người báo cáo

(ký, ghi rõ họ tên)

Phụ lục 3

Hệ thống khung tài liệu kỹ thuật

- Tài liệu mô tả, thuyết minh tổng quan về hệ thống, ứng dụng
- Tài liệu thiết kế xây dựng đã được ký duyệt
- Tài liệu thuyết minh phương án đảm bảo an toàn thông tin theo mức độ đã duyệt

+ Đảm bảo an toàn hệ thống

+ Đảm bảo an toàn vận hành

Phụ lục 4

Các biểu mẫu

(danh sách các hạng mục tài sản, tên, tuổi, địa chỉ)

STT	Hệ thống	địa chỉ	Nhân sự	TG / Xác nhận
Tài sản thông tin				
Tài sản vật lý				
Tài sản phần mềm				
Tài sản tài liệu				

Phụ lục 5

Dashboard