**QUY TRÌNH**

**ỨNG CỨU SỰ CỐ CÔNG NGHỆ THÔNG TIN**

|  |  |  |
| --- | --- | --- |
| **BIÊN SOẠN** | **KIỂM TRA** | **PHÊ DUYỆT** |
| **Nhóm SOP CNTT** | **Tổ SOP** | **Tổng giám đốc** |
| 14805feebd596e073748  **Đặng Huy Cường** | **Lê Đông** | **Nguyễn Cảnh Tĩnh** |

|  |  |  |
| --- | --- | --- |
| **Phiên bản** | **Trang** | **Nội dung thay đổi** |
| 20230710 | Tất cả | - Chuẩn hóa quy trình theo SOP |

**I. Mục tiêu**

Hướng dẫn nhân viên Trung tâm Công nghệ thông tin các bước thực hiện để ứng cứu sự cố về Công nghệ thông tin thuộc VIMC.

Đảm bảo xử lý các sự số nhanh chóng, kịp thời, để hệ thống vận hành được liên tục, an toàn và đạt hiệu suất tốt.

**II. Phạm vi**

Áp dụng cho các đối tượng là nhân viên CNTT thuộc VIMC *(các doanh nghiệp thành viên có thể vận dụng quy trình để triển khai áp dụng phù hợp với đặc thù tại doanh nghiệp).*

**III. Tài liệu liên quan**

- Bộ tài liệu ISO 9001-2015, ISO 27001.

- Các Quy định nội bộ có liên quan của VIMC.

**IV. Chú thích**

**4.1. Giải thích thuật ngữ:**

- VIMC: Tổng công ty Hàng hải Việt Nam – CTCP.

- NSD: Người sử dụng các hệ thống CNTT.

- TTCNTT Trung tâm Công nghệ thông tin.

- Lãnh đạo TTCNTT: Giám đốc/ Phó giám đốc TTCNTT.

- RACI: A: phê duyệt kết quả; R: người thực hiện; C: người tư vấn/ hỗ trợ; I: người được thông báo kết quả.

**4.2. Giải thích lưu đồ**

Các bước xử lý

Bắt đầu/Kết thúc

Kết nối các

bước xử lý

Điều kiện rẽ nhánh

Tài liệu đính kèm

Quy trình tiếp nối

**V. Nội dung quy trình**

**5.1. Lưu đồ** *(Xem trang bên)*



**5.2 Ma trận vai trò RACI & KPI quy trình**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Bước thực hiện** | **Người sử dụng** | **Nhân viên CNTT** | **Lãnh đạo TTCNTT** | **KPI** |
| 1. Tiếp nhận sự và xác minh sự cố | I | R | R | - 100% tiếp nhận  - Thông tin ghi nhận đẩy đủ. |
| 2. Thông báo sự cố | I | R | I | 5 phút |
| 3. Phân loại sự cố và triển khai phương án dự phòng | I | R | I | 5 phút giờ |
| 4. Phân tích nguyên nhân sự cố |  | R | R | 10 phút |
| 5. Tìm biện pháp và xử lý sự cố | I | R | I | Theo độ khẩn cấp |
| 6. Báo cáo & lưu hồ sơ | I | R | I | 5 phút |

**5.3 Diễn giải các bước**

**Bước 1:** Tiếp nhận và xác minh sự cố

a. TTCNTT tiếp nhận thông tin về sự cố thông qua các kênh sau:

+ Hotline 1633/1635/

+ Email [ttcntt@vimc.co](mailto:ttcntt@vimc.co)

+ Truy cập link: <https://hotro.vimc.co>

+ Phần mềm văn phòng điện tử - VIMC e-Office tại <https://portal.vimc.co> để thông báo yêu cầu hỗ trợ.

+ Thông báo sự cố từ các hệ thống giám sát của các cơ quan nhà nước có thẩm quyền (VNCERT) hoặc từ các nhà cung cấp dịch vụ viễn thông cho VIMC.

b. TTCNTT tiến hành kiểm tra, xác minh sự cố, các phương pháp như sau:

+ Kiểm tra hiện trường sự cố: cử cán bộ xuống hiện trường để xác nhận sự cố, ghi nhận bằng hình ảnh, video, gặp trực tiếp người phát hiện sự cố.

+ Kiểm tra bằng các công cụ giám sát hệ thống như: SolarWinds; Network Performance Monitor; ManageEngine OpManager; PRTG Network Monitor; WhatsUp Gold; Nagios XI hoặc các câu lệnh cơ bản như scan, ping, tracert ...

+ Kiểm tra truy cập vào các ứng dụng và dữ liệu từ bên trong và ngoài hệ thống mạng.

+ Kiểm tra truy cập bằng cách sử dụng các máy tính khác nhau, trình duyệt khác nhau, kết nối khác nhau, địa chỉ IP khác nhau ...

+ Kiểm tra bằng các biện pháp nghiệp vụ khác.

c. Sau khi đã xác minh sự cố, tiến hành ghi các thông tin như sau:

+ Thời điểm sự cố: là thời điểm người phát hiện sự cố.

+ Đơn vị bị sự cố: đơn vị bị sự cố tại thời điểm phát hiện.

+ Nội dung sự cố: ghi nhận mô tả tạm thời về sự cố.

+ Loại sự cố: ghi nhận phân loại theo một số đặc điểm (tùy thuộc đặt thù từng đơn vị), theo như sau:

\*Loại 1: Cháy nổ/ hỏa hoạn/ thiên tai.

\*Loại 2: Sự cố mạng/ hệ thống CNTT (bên ngoài và nội bộ)

\*Loại 3: Phần mềm cho khách hàng (vd: e-booking, e-port, gate..)

\*Loại 4: Phần mềm vận hành khai thác (vd: tos, checkpoint, wms..)

+ Phạm vi ảnh hưởng: sự cố ảnh hưởng trong phạm vi nào? (vd: tới phòng A, phòng B, hay toàn công ty).

+ Đối tượng ảnh hưởng: đối tượng bị ảnh hưởng bởi sự cố. (vd: khách hàng, người lao động...).

+ Các bằng chứng xác thực: ghi nhận các thông tin xác thực ban đầu về sự cố. Vd: mất kết nối, ping không tới máy chủ, không truy cập được ...

*(Tham khảo Hồ sơ thông tin sự cố bên dưới, ở bước này ghi thông tin 7 cột đầu tiên – bôi vàng)*

**Hồ sơ thông tin sự cố**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Thời điểm sự cố** | **Đơn vị bị sự cố** | **Nội dung sự cố** | **Loại sự cố** | **Phạm vi ảnh hưởng** | **Đối tượng ảnh hưởng** | **Các bằng chứng xác thực** | **Độ nghiêm trọng** | **Nguyên nhân** | **Giải pháp** | **Tình trạng xử lý** | **Thời điểm hoàn thành** |
|  |  |  |  |  |  |  |  |  |  |  |  |

**Bước 2:** Thông báo sự cố

Sau khi xác nhận sự cố, người tiếp nhận sự cố có trách nhiệm thông bao sơ bộ về sự cố tới toàn thể nhân viên bộ phận CNTT, lãnh đạo thuộc Ban điều hành phụ trách lĩnh vực CNTT và các đơn vị, khách hàng có liên quan.

a. Nội dung thông báo: thông tin về sự cố đã ghi nhận ở **“Hồ sơ thông tin sự cố”.**

b. Hình thức thông báo:

+ Lãnh đạo thuộc Ban điều hành: gặp trực tiếp/ gọi điện thoại, nhắn tin, gửi email báo cáo..

+ Trung tâm CNTT: gọi điện, thông báo qua nhóm zalo chung.

+ Người sử dụng: thông báo trên phần mềm portal office và nhắn tin trên nhóm zalo đại diện phòng/ ban hoặc gửi email thông báo.

**Bước 3:** Phân loại sự cố và triển khai phương án dự phòng

a. Phân loại sự cố: sau khi xác nhận được sự cố, TTCNTT tiến hành phân loại sự cố thành các mức khẩn cấp và thời gian cần phải hoàn thành xử lý, theo bảng tiêu chí sau:

**Bảng phân loại mức sự cố khẩn cấp và thời gian xử lý**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mức ảnh Loại hưởng  sự cố | Ảnh hưởng tất cả các khách hàng | Ảnh hưởng một nhóm khách hàng | Ảnh hưởng toàn thể người dùng | Ảnh hưởng một nhóm người dùng |
| Loại 1: Cháy nổ/ hỏa hoạn/ thiên tai | Khẩn loại 1 | Khẩn loại 1 | Khẩn loại 1 | Khẩn loại 1 |
| **Xử lý: 0.5h** | **Xử lý: 0.5h** | **Xử lý: 0.5h** | **Xử lý: 0.5h** |
| Loại 2: Sự cố mạng/ Hệ thống CNTT | Khẩn loại 1 | Khẩn loại 2 | Khẩn loại 2 | Khẩn loại 3 |
| **Xử lý: 0.5h** | **Xử lý: 2h** | **Xử lý: 2h** | **Xử lý: 4h** |
| Loại 3: Phần mềm cho khách hàng (vd: e-booking, e-port, gate..) | Khẩn loại 1 | Khẩn loại 2 | Khẩn loại 2 | Khẩn loại 3 |
| **Xử lý: 0.5h** | **Xử lý: 2h** | **Xử lý: 2h** | **Xử lý: 4h** |
| Loại 4: Phần mềm vận hành khai thác (vd: tos, checkpoint, wms..) | Khẩn loại 1 | Khẩn loại 2 | Khẩn loại 2 | Khẩn loại 3 |
| **Xử lý: 0.5h** | **Xử lý: 2h** | **Xử lý: 2h** | **Xử lý: 4h** |

b. Triển khai phương án dự phòng: đối với sự cố có mức độ khẩn loại 1,2; TTCNTT tiến hành triển khai ngay các bước như sau:

+ Khoanh vùng và cách ly lây lan (đối với sự cố cháy nổ, nhiễm virus mã độc): tạm thời cách ly vùng ảnh hưởng khỏi vùng an toàn như: ngắt nguồn điện, ngắt kết nối mạng, di chuyển cách xa khu vực an toàn.

+ Tiến hành kiểm tra trạng thái các đường truyền, máy chủ, hệ thống dự phòng, chuẩn bị sẵn sàng để chuyển đổi sang hệ thống dự phòng.

+ Cấu hình tương thích với hệ thống dự phòng (IP, Port, Domain, API ...)

+ Chuyển đổi và vận hành hệ thống dự phòng.

+ Giám sát hiệu năng hoạt động của hệ thống dự phòng.

+ Ghi Log theo dõi.

**Bước 4**: Phân tích nguyên nhân sự cố

a. Thu thập thông tin phục vụ phân tích sự cố

TTCNTT triển khai phối hợp các đơn vị liên quan tiến hành thu thập các thông tin để phục vụ cho việc phân tích nguyên nhân như sau:

- Thu thập thông tin cấu hình hệ thống mạng (IP, Port, Config, Rules, Profile...)

- Thu thập chức năng của hệ thống (Function, Module...)

- Thu thập cấu hình của hệ điều hành (OS, Servise, Version …)

- Thu thập bộ nhớ trong (Memory)

- Thu thập trạng thái mạng và các kết nối (Network and Connection)

- Thu thập các tiến trình (Process) đang chạy

- Thu thập thông tin bộ nhớ lưu trữ (SSD, HDD, Removable)

- Thu thập thông tin lịch sử Log file, History file

- Và các chứng cứ có nghi ngờ khác ..

b. Phân tích nguyên nhân sự cố

TTCNTT phối hợp với các đơn vị liên quan (đơn vị cho thuê/cung cấp dịch vụ) tiến hành phân tích các thông tin sau để tìm nguyên nhân sự cố:

- Các nguyên nhân vật lý: điện nguồn, đứt dây, treo, hỏng thiết bị, đấu nối sai cách, lỏng kết nối, rơi kết nối ..

- Các nguyên nhân phần mềm: Lỗi CSDL, Source Code, Runtime…

- Thời gian bị sửa đổi, truy cập, tạo hoặc thay đổi.

- Thời gian thực hiện các cập nhật lớn đối với hệ thống (Check Last Update).

- Thời điểm mà hệ thống sử dụng ổn định lần cuối cùng (Check Restore Profile).

- Phân tích dữ liệu (Check Database).

- Kiểm tra sự thay đổi cấu hình (Check Config).

- Kiểm tra hệ thống tập tin có bị mã độc (Scan Malware, Virus...).

- Kiểm tra tập tin Internet History và các tập tin History khác.

- Kiểm tra Registry và Process.

- Quan sát các File, Process, Profile lúc khởi động.

- Phân tích Log file.

**Bước 5:** Tìm biện pháp và xử lý sự cố

TTCNTT tiến hành các biện pháp xử lý sự cố bao gồm các bước:

- Khoanh vùng, cách ly, gỡ bỏ sự cố

- Sử dụng các nguồn lực sẵn có hoặc tiến hành bổ sung nguồn lực bằng các hình thức thuê, đầu tư, mua sắm... để khắc phục sự cố theo thời gian cam kết

- Thực hiện khôi phục các tổn thất gây ra bởi sự cố (thiết bị, dữ liệu, hình ảnh, tập tin, Email ...)

- Kiểm tra giám sát vận hành của hệ thống sau khi phục hồi.

- Đối với sự cố đã sử dụng phương án dự phòng, cần tiến hành chạy song song 2 hệ thống (chính và dự phòng) đảm bảo 2 hệ thống hoạt động ổn định ít nhất 24h, sau đó mới tiến hành chuyển hoàn toàn sang hệ thống chính.

**Bước 6:** Báo cáo & Lưu hồ sơ

TTCNTT tiến hành cập nhật đầy đủ thông tin vào “Hồ sơ thông tin sự cố” và báo cáo lãnh đạo “Ban Điều hành”, thông báo tới các đơn vị liên quan và khách hàng về thông tin khôi phục hệ thống, đồng thời gửi báo cáo tới các DNTV để đơn vị tham khảo, rút kinh nghiệm trong hoạt động xử lý sự cố và đề xuất các biện pháp áp dụng cho các sự cố tương tự.

**VI. Rủi ro và kiểm soát**

|  |  |  |  |
| --- | --- | --- | --- |
| **Bước thực hiện** | **Mối nguy** | **Rủi ro** | **Kiểm soát** |
| 1. Tiếp nhận sự và xác minh sự cố | NSD Chậm thông báo.  Xác minh sai sót về sự cô | - Hỏng hệ thống.  - Mất dữ liệu  - Thảm họa về môi trường, xã hội.  - Khách hàng chờ đợi, không sử dụng được dịch vụ. | - NSD cần thông báo ngay cho TTCNTT khi gặp sự cố.  - TTCNTT thực hiện giám sát cảnh bảo sớm sự cố bằng hệ thống.  - Xây dựng bảng tiêu chí để dễ dàng phân loại. |
| 2. Thông báo sự cố | Nhân viên CNTT thông báo sai, không thông báo, thông báo chậm | - Chậm trễ khắc phục.  - Ùn tắc trong và ngoài cảng. | - Nhân viên CNTT phối hợp đồng nghiệp cùng thực hiện.  - Lãnh đạo TTCNTT kiểm tra chéo. |
| 3. Phân loại sự cố và triển khai phương án dự phòng | - Chậm trễ thực hiện.  - Phân loại sai  - Chưa có phương án dự phòng. | - Chậm trễ khắc phục.  - Ùn tắc trong và ngoài cảng. | - Xây dựng bảng tiêu chí phân loại,  - Nhân viên CNTT phối hợp đồng nghiệp cùng thực hiện.  - Yêu cầu xây dựng các phương án dự phòng khi đầu tư các hệ thống CNTT quan trọng (hệ thống khách hàng sử dụng và hệ thống vận hành khai thác) |
| 4. Phân tích nguyên nhân sự cố | Nhân viên CNTT phân tích sai nguyên nhân, thiếu nguyên nhân | - Chậm trễ khắc phục.  - Hỏng hệ thống.  - Mất dữ liệu.  - Đưa ra biện pháp sai, thiếu, thừa. | - Thu thập đủ thông tin phục vụ phân tích.  - Xây dựng bảng tiêu chí kiểm tra/ phân loại vấn đề.  - Nhân viên CNTT phối hợp đồng nghiệp cùng thực hiện. |
| 5. Tìm biện pháp và xử lý sự cố | Chậm trễ thực hiện. | - Chậm trễ khắc phục. | - Tuân thủ KPI quy trình thời gian cam kết khắc phục sự cố. |
| 6. Báo cáo & lưu hồ sơ | Nhân viên CNTT quên không ghi hồ sơ. | - Không theo dõi được lịch sử sự cố.  - Không tham khảo được giải pháp đã thực hiện. | - Lãnh đạo TTCNTT thường xuyên kiểm tra và yêu cầu cập nhật đầy đủ. |

**VII. Hồ sơ lưu**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| STT | Tên Hồ sơ | Người lưu | Nơi lưu | Thời gian lưu |
| 1 | Hồ sơ theo dõi CNTT | Nhân viên TTCNTT | VIMC-Cloud | Không xác định |

**VIII. Biểu mẫu/ phụ lục**