



QUY TRÌNH

Xử lý sự cố

ISO/IEC 27001:2013& ISO 9001:2015	
Mã hiệu	2-504
Ngày hiệu lực	2023/11/09
Lần ban hành	01

LỊCH SỬ SỬA ĐỔI TÀI LIỆU

STT	Mục sửa đổi	Nội dung sửa đổi	Ngày sửa đổi	Phiên bản sửa đổi
1	Toàn bộ	Ban hành	2023/11/09	01

MỤC LỤC

I.	MỤC ĐÍCH	4
II.	PHẠM VI ÁP DỤNG.....	4
III.	TÀI LIỆU VIỆN DẪN.....	4
IV.	THUẬT NGỮ & CÁC TỪ VIẾT TẮT	4
1.	Các từ viết tắt	4
2.	Thuật ngữ	4
1.	Sự cố	5
2.	Nguồn phát hiện sự cố	5
3.	Thiệt hại tài chính	5
4.	Chứng cứ liên quan đến sự cố.....	6
4.1.	Định nghĩa	6
4.2.	Yêu cầu	6
5.	Phân loại sự cố.....	7
5.1.	Mức độ nghiêm trọng của sự cố (Severity)	8
5.2.	Mức độ khẩn cấp của sự cố (Urgency)	9
VI.	QUY TRÌNH	10
	Bước 1: Phát hiện và báo cáo nhanh về sự cố - Incident detection and quick report..	10
	Bước 2: Hành động khắc phục tức thời - Incident immediate action	11
	Bước 3: Phân tích và báo cáo sự cố - Incident analysis and report	12
	Bước 4: Đưa ra biện pháp dài hạn - Permanent action	12
	Bước 5: Theo dõi và đánh giá - Follow up action	13
	PHỤ LỤC: DANH SÁCH BIỂU MẪU ÁP DỤNG.....	14

I. MỤC ĐÍCH

Văn bản này quy định về quy trình xử lý các sự cố liên quan đến hoạt động vận hành của công ty, nằm ngoài phạm vi dự án phát triển phần mềm, nhằm hạn chế, giảm thiểu tác động tiêu cực của sự cố đến hoạt động vận hành và kinh doanh của Công ty; đồng thời góp phần cải tiến liên tục chất lượng và an ninh thông tin của hệ thống quy trình, quy định liên quan đến vận hành và kinh doanh của công ty.

II. PHẠM VI ÁP DỤNG

Áp dụng cho tất cả các phòng ban tại Công ty TNHH Sun Asterisk Việt Nam (sau đây gọi tắt là “Sun*”).

III. TÀI LIỆU VIỆN DẪN

- Tiêu chuẩn ISO/IEC 27001:2013
- Tiêu chuẩn ISO/IEC 27001:2022
- Tiêu chuẩn ISO/IEC 27035: 2016 Công nghệ thông tin - Kỹ thuật bảo mật - Quản lý sự cố an toàn thông tin

IV. THUẬT NGỮ & CÁC TỪ VIẾT TẮT

1. Các từ viết tắt

- UM: Unit Manager (trưởng ban)
- LM: Line Manager (trưởng phòng)
- PIC: Person in charge (người phụ trách)
- LRM: Legal & Risk Management (phòng Pháp chế & Quản trị rủi ro)
- F&A: Finance & Accounting (phòng Tài chính kế toán)

2. Thuật ngữ

- Hành động khắc phục sự cố tức thời (Immediate action): là các biện pháp tạm thời được thực hiện ngay sau khi sự cố phát sinh nhằm kiểm soát sự cố, giảm thiểu tác động của sự cố, ngăn chặn tình huống trở nên tồi tệ hơn và giữ cho hoạt động được duy trì khi tình huống khẩn cấp xảy ra.
- Biện pháp dài hạn (Permanent action): là các biện pháp mang tính lâu dài để xử lý triệt để nguồn gốc phát sinh sự cố và phòng ngừa sự cố lặp lại trong tương lai.
- Nguyên nhân gốc rễ của vấn đề (Root cause): là nguyên nhân cốt lõi chính và cơ bản dẫn đến việc xảy ra sự cố mà nếu loại bỏ hoặc khắc phục sẽ có thể ngăn chặn sự cố tái diễn trong tương lai.

V. ĐỊNH NGHĨA

1. Sự cố

- Sự cố là lỗi xảy ra trong hoạt động vận hành, trong dự án hoặc bất kỳ tình huống nào gây ảnh hưởng, thiệt hại hoặc làm gián đoạn đến hoạt động vận hành, dịch vụ, uy tín, hình ảnh hoặc các mục tiêu phát triển của công ty.
- Một sự cố khi phát sinh đòi hỏi sự can thiệp và xử lý để giải quyết vấn đề và khôi phục lại hoạt động bình thường của tổ chức bằng cách triển khai các biện pháp khẩn cấp, kế hoạch khắc phục phòng ngừa, theo dõi và kiểm tra để hạn chế tối đa các sự cố tương tự phát sinh trong tương lai.
- Một sự cố được coi là trọng yếu khi thuộc một trong các trường hợp sau:
 - + gây thiệt hại về người (thương tật, tử vong)
 - + gây thiệt hại về tài chính với số tiền lớn hơn 20 triệu đồng
 - + gây rò rỉ thông tin bảo mật theo quy định của Công ty
 - + vi phạm các quy định của pháp luật
- Sự cố được coi là xử lý hoàn tất khi sự cố đã được báo cáo, đánh giá và được giải quyết một cách triệt để nhằm đảm bảo hoạt động vận hành của Công ty được phục hồi về trạng thái bình thường.

2. Nguồn phát hiện sự cố

- Phòng LRM
- Phòng ISO
- Phòng F&A
- Phòng ban/nhân viên
- Các phòng ban liên quan khác

3. Thiệt hại tài chính

Thiệt hại tài chính là sự mất mát hoặc tổn thất về tiền bạc, giá trị tài sản, hoặc khả năng tạo ra doanh thu và lợi nhuận của Công ty do sự cố gây ra. Thiệt hại tài chính có thể bao gồm các yếu tố sau:

- Thiệt hại trực tiếp (Direct cost): hỏng hóc, mất mát thiết bị, tài sản, thất thoát hàng tồn kho, mất tiền, các chi phí phát sinh để ngăn chặn, hạn chế, khắc phục thiệt hại và khôi phục hoạt động bình thường từ sự cố (ex: chi phí xác minh nguyên nhân sự cố, chi phí làm việc thêm với các bên liên quan, trả lương làm thêm giờ cho nhân viên, nâng cấp hệ thống hoặc cải thiện an ninh để ngăn ngừa sự cố phát sinh trong

tương lại...), các khoản chi phí để giải quyết các tranh chấp hoặc khoản nộp phạt do vi phạm pháp lý.

- Thiệt hại gián tiếp (Indirect cost): thiệt hại về danh tiếng, uy tín của công ty dẫn đến việc ảnh hưởng hình ảnh công ty, mất lòng tin của khách hàng, giảm sút doanh thu, mất lợi nhuận do gián đoạn hoạt động kinh doanh.
- Chi phí cơ hội (Opportunity cost): bỏ lỡ cơ hội kinh doanh hoặc các hợp đồng hợp tác có tiềm năng tạo lợi nhuận hoặc giá trị cho công ty.

4. Chứng cứ liên quan đến sự cố

4.1. Định nghĩa

Chứng cứ liên quan đến sự cố là những thông tin, dữ liệu hoặc tài liệu được thu thập và ghi nhận trong quá trình phát hiện, điều tra và giải quyết sự cố phát sinh.

4.2. Yêu cầu

4.2.1. Chứng cứ phải đáp ứng được các điều kiện sau

a. Hình thức

Chứng cứ có thể được lưu trữ dưới dạng: văn bản, hình ảnh, dữ liệu trích xuất từ camera, video, bản ghi âm, email trao đổi, nhật ký hệ thống, dữ liệu trích xuất từ hệ thống và/hoặc các hình thức khác có thể sử dụng để xác nhận, chứng minh hoặc tái hiện một sự cố đã xảy ra và/hoặc việc xử lý, giải quyết sự cố đã được thực hiện.

b. Nội dung

- Trong mọi trường hợp, chứng cứ cần đảm bảo tính toàn vẹn và không được phép sửa đổi, thay thế dưới bất kỳ hình thức nào.
- Chứng cứ cần đảm bảo cung cấp đủ thông tin quan trọng và chính xác về sự cố phát sinh để hỗ trợ việc phân tích, đánh giá và đưa ra kết luận
- Chứng cứ cần liên quan trực tiếp hoặc gián tiếp đến sự cố nhằm hỗ trợ việc xác minh, phân tích hoặc chứng minh một cách rõ ràng, chi tiết về việc sự cố đã được xử lý, giải quyết.
- Một sự cố có thể bao gồm nhiều chứng cứ. Nội dung các chứng cứ này cần có sự liên quan logic và bổ trợ cho nhau.

4.2.2. Cách thức và thời điểm lưu trữ

- Chứng cứ về sự cố của từng phòng ban sẽ được lưu trữ trên thư mục Google Drive do LRM chỉ định, mỗi sự cố của từng phòng ban sẽ được phân loại vào từng thư mục nhỏ riêng biệt.

QUY TRÌNH: XỬ LÝ SỰ CỐ

- Người phụ trách của phòng ban phát sinh sự cố có trách nhiệm tạo thư mục nhỏ, đặt mã cho từng thư mục nhỏ theo mẫu dưới đây:
 - + Tên phòng ban: Theo quy định viết tắt tên phòng ban của Công ty
 - + Ngày tháng năm phát sinh sự cố: 8 ký tự: DD - MM - YYYY
 - + Số thứ tự của sự cố phát sinh trong ngày đó: 2 chữ sốEx: GA-10072003-01
- Chứng cứ cần được tải lên ngay tại thời điểm phòng ban thu thập được trong quá trình phát hiện và xử lý sự cố. Tại thời điểm sự cố được xử lý hoàn tất, toàn bộ chứng cứ liên quan đến việc phát hiện sự cố, đánh giá, khắc phục và xử lý sự cố trên thực tế để hoạt động quay trở lại bình thường và các chứng cứ liên quan khác phải được lưu trữ đầy đủ trên thư mục Google Drive do LRM chỉ định.
- Phân quyền truy cập cho:
 - + Phòng Pháp chế & Quản trị rủi ro thông qua email: **bao.fcov.rm.members@sun-asterisk.com**
 - + Phòng ISO: **iso@sun-asterisk.com**

4.2.3. Trách nhiệm

LM của phòng ban phát sinh sự cố hoặc người được LM của phòng ban đó phân công, chỉ định có trách nhiệm lưu trữ và đảm bảo chứng cứ đáp ứng đủ các điều kiện được quy định tại mục IV.3.2. của quy trình này.

5. Phân loại sự cố

Sự cố phát sinh được phân loại theo **Mức độ ưu tiên của sự cố (Priority)**. Trong đó, Mức độ ưu tiên của sự cố là thứ tự ưu tiên giải quyết sự cố, được chia làm **5 mức** tương ứng với thời gian xử lý sự cố, cụ thể như sau:

Mức độ ưu tiên (Priority)	Thời gian xử lý sự cố tối đa
Immediate	4 giờ
Urgent	8 giờ
High	24 giờ
Medium	48 giờ
Low	72 giờ

Mức độ ưu tiên của sự cố được xác định theo hai tiêu chí sau:

- (i) Mức độ khẩn cấp của sự cố (Urgency)
- (ii) Mức độ nghiêm trọng của sự cố (Severity)

QUY TRÌNH: XỬ LÝ SỰ CỐ

Mức độ nghiêm trọng (Severity)	Mức độ khẩn cấp (Urgency)		
	Low	Medium	High
Low	Low	Medium	High
Medium	Medium	Medium	Urgent
High	High	Urgent	Immediate

5.1. Mức độ nghiêm trọng của sự cố (Severity)

5.1.1. Định nghĩa

Mức độ nghiêm trọng (Severity) của sự cố được đánh giá dựa trên sự kết hợp của 2 yếu tố: phạm vi ảnh hưởng và mức độ ảnh hưởng đến người, tài chính, bảo mật thông tin.

5.1.2. Tiêu chí

Tiêu chí	Low	Medium	High
Phạm vi ảnh hưởng (Phạm vi trong và ngoài công ty mà thiệt hại sự cố có thể ảnh hưởng đến)	<ul style="list-style-type: none"> Sự cố ảnh hưởng hoặc làm gián đoạn hoạt động trong phạm vi nội bộ một phòng ban trong công ty Phòng ban có lý do/ căn cứ để tin tưởng rằng phạm vi ảnh hưởng của sự cố đó sẽ được kiểm soát trong nội bộ của phòng ban và không phát triển, ảnh hưởng đến phòng ban khác (ví dụ: tiền lệ trước đó, lý do về hệ thống, lý do về việc kiểm soát thông tin giữa người với người...) 	<ul style="list-style-type: none"> Sự cố ảnh hưởng hoặc làm gián đoạn hoạt động của 2 phòng ban trở lên, nhưng ko ảnh hưởng đến toàn bộ công ty. Phòng ban có lý do/ căn cứ để đánh giá (ví dụ: tiền lệ trước đó, lý do về hệ thống, lý do về việc kiểm soát thông tin giữa người với người,...) 	<ul style="list-style-type: none"> Sự cố ảnh hưởng hoặc làm gián đoạn hoạt động của toàn bộ công ty hoặc các đối tác, khách hàng Phòng ban có lý do/ căn cứ để đánh giá (ví dụ: tiền lệ trước đó, lý do về hệ thống, lý do về việc kiểm soát thông tin giữa người với người,...)
Mức độ ảnh hưởng (Mức độ ảnh hưởng sẽ bao gồm những yếu tố liên quan như: thiệt hại về tài chính, thiệt hại về người, mức độ ảnh hưởng đến hoạt động, làm lộ thông tin công ty)	<p>Sự cố phát sinh bao gồm tất cả các điều kiện sau:</p> <ul style="list-style-type: none"> Không gây thiệt hại về người Không gây thiệt hại về tài chính Không làm lộ bất kỳ thông tin nào quy định tại Thỏa thuận về bảo mật thông tin: https://sal.vn/VDe8Yj 	<p>Sự cố phát sinh bao gồm tất cả các điều kiện sau:</p> <ul style="list-style-type: none"> Không gây thiệt hại về người Gây tổn hại về tài chính với số tiền dưới 20 triệu đồng Không làm lộ bất kỳ thông tin nào quy định tại Thỏa thuận về bảo mật thông tin: https://sal.vn/VDe8Yj 	<p>Sự cố phát sinh dẫn đến một những thiệt hại sau:</p> <ul style="list-style-type: none"> Có phát sinh thiệt hại về người (bị thương tật, tử vong) Gây tổn hại về tài chính với số tiền từ 20 triệu đồng trở lên hoặc gây tổn hại về hình ảnh, uy tín, danh tiếng của công ty. Làm lộ bất kỳ thông tin nào quy định tại Thỏa thuận về bảo mật thông tin: https://sal.vn/VDe8Yj

5.1.3. Phân loại

Ma trận xác định mức độ nghiêm trọng (Severity) của sự cố

Mức độ ảnh hưởng	Phạm vi ảnh hưởng		
	Low	Medium	High
Low	Low	Medium	High
Medium	Medium	Medium	High
High	High	High	High

5.2. Mức độ khẩn cấp của sự cố (Urgency)

5.2.1. Định nghĩa

Mức độ khẩn cấp của sự cố (Urgency) là khoảng thời gian cần thiết phải xử lý triệt để sự cố trước khi sự cố gây ra hậu quả nghiêm trọng hơn nhằm giảm thiểu tối đa thiệt hại và đảm bảo hoạt động của công ty được phục hồi nhanh chóng.

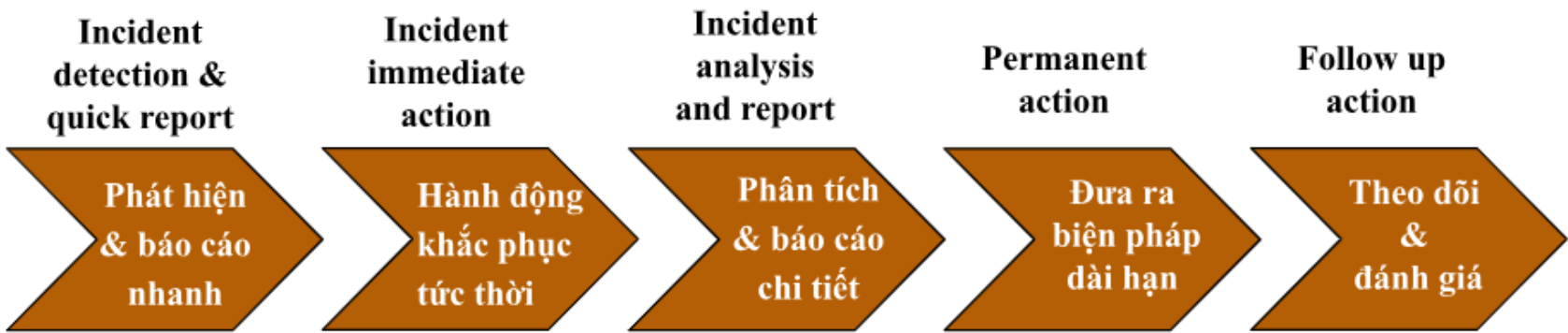
5.2.2. Phân loại

Urgency	Thời gian Công ty chấp nhận sự cố tồn tại
Low	Tối đa 120 giờ (tương đương 5 ngày)
Medium	Tối đa 72 giờ (tương đương 3 ngày)
High	Tối đa 24 giờ (tương đương 1 ngày)

Note: Trong đó, thời gian Công ty chấp nhận sự cố tồn tại là khoảng thời gian tối đa phải hoàn thành việc xử lý sự cố mà các phòng ban thống nhất sau khi họp đánh giá sự cố.

VI. QUY TRÌNH

Tổng quan các bước trong quy trình:



Bước 1: Phát hiện và báo cáo nhanh về sự cố - Incident detection and quick report

Bước	Lưu đồ	Mô tả	PIC	Kết quả đầu ra	Thời gian
1.1	<div>Sự cố phát sinh</div> <div>↓</div> <div>Người phát hiện thông báo cho LM hoặc phòng LRM ngay sau khi phát hiện sự cố</div> <div>↓</div>	<ul style="list-style-type: none">Bất kỳ ai khi phát hiện sự cố, cần ngay lập tức thông báo cho LM của phòng ban phát sinh sự cố hoặc phòng LRM các thông tin ban đầu về sự cố và tiến hành thu thập chứng cứ liên quan. Việc báo cáo có thể được thực hiện qua Slack hoặc email của công ty. Để liên lạc với LRM, phòng ban có thể thực hiện thông báo qua chatbox được tạo riêng trên Slack để trao đổi tất cả các vấn đề liên quan đến hoạt động quản trị rủi ro giữa RM và mỗi phòng ban hoặc trao đổi trực tiếp đến các thành viên RM qua Slack hoặc email: Lê Thế Vinh: le.the.vinh@sun-asterisk.com Đinh Hà My: ding.ha.my@sun-asterisk.com Nguyễn Thị Linh Trang: nguyen.thi.linh.trang@sun-asterisk.comTrường hợp người phát hiện sự cố báo cho phòng LRM về sự cố phát sinh, LRM sẽ ngay lập tức tiến hành thông báo cho LM của phòng ban phát sinh sự cố.Người phát hiện sự cố phải tuân thủ các quy định và quy trình của công ty liên quan đến báo cáo sự cố, đảm bảo rằng thông tin được truyền đạt một cách chính xác, rõ ràng, đảm bảo tính toàn vẹn của thông tin.	<ul style="list-style-type: none">Các nhân sự và phòng/ban liên quan trong công tyLRM	LM của phòng ban phát sinh sự cố và LRM nhận được thông tin ban đầu về sự cố.	Ngay sau khi phát hiện ra sự cố
1.2	<div>LM xác nhận thông tin và trao đổi với các phòng ban liên quan, chỉ định nhân sự gửi Báo Cáo Nhanh Sự Cố</div> <div>↓</div>	LM của phòng ban phát sinh sự cố xác nhận thông tin, xem xét chứng cứ và tiến hành trao đổi với các bên liên quan (bao gồm các phòng ban bị ảnh hưởng bởi sự cố, phòng ban có liên quan đến việc xử lý sự cố) để xác minh các thông tin về sự cố phát sinh và chỉ định nhân sự điền biểu mẫu Báo Cáo Nhanh Sự Cố.	LM của phòng ban phát sinh sự cố	Thông tin về sự cố được kiểm tra và xác nhận. Chứng cứ liên quan đến sự cố được thu thập.	
1.3	<div>Nhân sự được chỉ định gửi Báo Cáo Nhanh Sự Cố cho LRM theo thời gian quy định</div> <div>↓</div> <div>Biểu mẫu: BM_01</div>	Nhân sự được chỉ định thực hiện điền biểu mẫu Báo Cáo Nhanh Sự Cố cho phòng LRM.	Nhân sự được chỉ định của phòng ban phát sinh sự cố	Phòng LRM nhận được Báo Cáo Nhanh Sự Cố từ phòng ban	

* Biểu mẫu: BM_01

Link báo cáo nhanh - Quick report: <https://sal.vn/puaUXG>

Bước 2: Hành động khắc phục tức thời - Incident immediate action

Bước	Lưu đồ	Mô tả	PIC	Kết quả đầu ra	Thời gian
2.1	<pre>graph TD; A[LM họp với các phòng ban liên quan để đánh giá và phê duyệt mức độ khẩn cấp, mức độ nghiêm trọng và mức độ ưu tiên xử lý sự cố.] -- Low --> B[Phòng ban Hoàn thiện BM_02]; A -- "Mức Low và sự cố xảy ra từ 3 lần trở lên/tháng" --> C[Xây dựng hành động khắc phục tức thời và chỉ định PIC xử lý sự cố]; A -- "Mức Medium trở lên" --> C; C --> D[Xử lý sự cố theo phương án hành động khắc phục tức thời đã được phê duyệt]; D -- Không đạt --> C; D -- Đạt --> E[Xử lý sự cố hoàn tất];</pre>	<p>Sau khi xác định được sự cố phát sinh, LM cần tiến hành họp với các phòng ban liên quan (Theo quy trình Xử lý Liên Phòng Ban) để phân tích, đánh giá tình trạng của sự cố theo các tiêu chí: Mức độ khẩn cấp của sự cố (Urgency), Mức độ nghiêm trọng của sự cố (Severity), Mức độ ưu tiên xử lý sự cố (Priority).</p> <ul style="list-style-type: none">- Đối với sự cố có mức độ ưu tiên ở mức Medium trở lên: phòng ban tiến hành tiếp bước 2.2.- Đối với sự cố có mức độ ưu tiên ở mức Low: phòng ban hoàn thiện biểu mẫu BM_02 và chủ động theo dõi, nhưng trường hợp sự cố đó xảy ra 3 lần trở lên/tháng, phòng ban phải thực hiện tiếp bước 2.2.	<ul style="list-style-type: none">- LM của phòng ban phát sinh sự cố;- Phòng/ban có liên quan	<ul style="list-style-type: none">- Phòng ban phát sinh sự cố có trách nhiệm đưa ra kết quả đánh giá của sự cố bao gồm:<ul style="list-style-type: none">+ Mức độ khẩn cấp (Urgency);+ Mức độ nghiêm trọng (Severity);+ Mức độ ưu tiên (Priority).- Kết quả đánh giá sự cố cần phải được bộ phận phụ trách đánh giá một cách chính xác, được LM phê duyệt và ghi nhận tại BM_02 & BM_03 (phòng ban phát sinh sự cố cần trao đổi với các phòng ban liên quan để hỗ trợ đánh giá).	Tương ứng với từng mức độ ưu tiên, thời gian xử lý tối đa được quy định tại mục IV.4.3 của quy trình
2.2		<ul style="list-style-type: none">- Tiến hành xây dựng Hành động khắc phục tức thời (Immediate action) và chỉ định PIC xử lý sự cố sau khi xác định được tình trạng của sự cố tại Bước 2.1.- Hành động khắc phục tức thời cần được xác nhận và phê duyệt của LM (xác nhận bằng văn bản hoặc qua Slack).	<ul style="list-style-type: none">- LM của phòng ban phát sinh sự cố- Phòng/ban có liên quan	<p>Đưa ra được Hành động khắc phục tức thời bao gồm nhưng không giới hạn những nội dung chính sau:</p> <ul style="list-style-type: none">- Nội dung kế hoạch thực hiện;- Người chịu trách nhiệm chính thực hiện;- Thời gian xử lý dự kiến;- Deadline xử lý	
2.3		<p>PIC tiến hành xử lý sự cố theo đúng phương án hành động khắc phục tức thời đã được UM phê duyệt:</p> <ul style="list-style-type: none">- Nếu sự cố chưa được xử lý triệt để, quay lại bước 2.2.- Nếu sự cố đã được xử lý hoàn tất, tiến hành tiếp bước 2.4.	<ul style="list-style-type: none">- PIC- LM, UM của phòng ban phát sinh sự cố- Phòng/ban có liên quan	<ul style="list-style-type: none">- Sự cố được xử lý triệt để- Kết quả đánh giá sự cố và hành động khắc phục sự cố được LRM kiểm tra, xác nhận	
2.4		<p>Sau khi sự cố được xử lý hoàn tất, LM cần tiến hành báo cáo tình trạng xử lý sự cố cho phòng LRM</p>	<ul style="list-style-type: none">- LM của phòng ban phát sinh sự cố	<p>Phòng LRM nhận được thông tin sự cố xử lý hoàn tất qua Slack</p>	<p>Sớm nhất có thể, tối đa trong vòng 24h kể từ thời điểm sự cố được xử lý hoàn tất.</p>

*Biểu mẫu: BM_02 & BM_03

Bước 3: Phân tích và báo cáo sự cố - Incident analysis and report

Bước	Lưu đồ	Mô tả	PIC	Kết quả đầu ra	Thời gian
3.1	<div>Hành động khắc phục sự cố tức thời được hoàn tất</div> <div>↓</div> <div>LRM gửi thông báo hoàn thiện Báo Cáo Chi Tiết Sự Cố tới LM</div>	Sau khi sự cố được xử lý, LRM gửi yêu cầu qua Slack đến LM của phòng ban phát sinh sự cố về việc hoàn thiện Báo Cáo Chi Tiết Sự Cố (Final Report form).	LRM	Yêu cầu hoàn thiện Báo Cáo Chi Tiết sự cố qua Slack	Ngay sau khi có thông tin sự cố xử lý hoàn tất hoặc sau khoảng thời gian tối đa tương đương với thời giải quyết sự cố có mức độ Priority ở mức Low (72h).
3.2	<div>↓</div> <div>LM hoàn thiện Báo Cáo Chi Tiết Sự Cố và thông báo cho LRM</div> <div>↓</div>	LM của phòng ban hoặc người được LM chỉ định tiến hành hoàn thiện Báo Cáo Chi Tiết Sự Cố và gửi thông báo cho LRM: - Nếu phòng ban chưa hoàn thiện, LRM sẽ tiến hành nhắc nhở phòng ban tối đa 2 lần. Trường hợp phòng ban gửi báo cáo muộn thì sẽ phải có trách nhiệm giải trình lý do. - Nếu phòng ban đã hoàn thiện, chuyển tiếp xuống bước 3.3.	LM của phòng ban phát sinh sự cố	LRM nhận được Báo Cáo Chi Tiết Sự Cố đầy đủ thông tin theo biểu mẫu BM_03	Trong vòng 7 ngày kể từ ngày sự cố được xử lý hoàn tất
3.3	<div>↓</div> <div>LRM kiểm tra tính đầy đủ của báo cáo</div>	LRM tiến hành xem xét tính đầy đủ của Báo Cáo Chi Tiết Sự Cố, bao gồm: - Mức độ kịp thời trong việc xử lý sự cố - Tính chính xác và hợp lý của việc đánh giá hệ số (Urgency, Severity và Priority) - Báo cáo cần chỉ ra được nguyên nhân gốc rễ của vấn đề (root cause)	LRM	Thời gian xử lý sự cố và các hệ số đánh giá trong Báo Cáo Chi Tiết Sự Cố là phù hợp với quy định. Đồng thời, tìm ra được nguyên nhân gốc rễ của vấn đề và cách khắc phục	Trong vòng 7 ngày kể từ ngày LRM nhận được Báo Cáo Chi Tiết Sự Cố

*Biểu mẫu: BM_02 & BM_03

Bước 4: Đưa ra biện pháp dài hạn - Permanent action

Bước	Lưu đồ	Mô tả	PIC	Kết quả đầu ra	Thời gian
4.1	<div>Phòng ban hợp tổng kết bài học kinh nghiệm & đề xuất biện pháp KPPN lâu dài</div> <div>↓</div>	Phòng ban trao đổi nội bộ và rút kinh nghiệm (lesson learnt), từ đó đề xuất Biện pháp khắc phục phòng ngừa lâu dài (Permanent action) và lên kế hoạch triển khai thực hiện	LM của phòng ban phát sinh sự cố	- Rút ra được bài học kinh nghiệm - Đưa ra Biện pháp khắc phục phòng ngừa lâu dài bao gồm nhưng không giới hạn những tiêu chí sau: + Cụ thể công việc cần triển khai + Nhân sự phụ trách + Lịch biểu thực hiện	Trong vòng 10 ngày kể từ ngày sự cố được xử lý hoàn tất
4.2	<div>↓</div> <div>Phòng ban gửi biện pháp KPPN được phê duyệt cho LRM</div> <div>↓</div>	Phòng ban hoàn thiện và thông báo cho LRM về Biện pháp khắc phục phòng ngừa lâu dài đã được UM phê duyệt.	- PIC - UM của phòng ban phát sinh sự cố	Biện pháp khắc phục phòng ngừa lâu dài được thông qua bởi UM	Tối đa 48h kể từ thời điểm UM thông qua Biện pháp khắc phục phòng ngừa lâu dài
4.3	<div>↓</div> <div>Phòng ban thực hiện biện pháp KPPN lâu dài theo đúng kế hoạch được phê duyệt</div> <div>↓</div>	Thực hiện Biện pháp khắc phục phòng ngừa lâu dài theo đúng kế hoạch đã đề ra	PIC	Cập nhật tình trạng trên Báo Cáo Chi Tiết Sự Cố về việc hoàn tất triển khai Biện pháp khắc phục phòng ngừa lâu dài theo kế hoạch và lịch biểu đề ra	Theo lịch biểu được phòng ban đề ra
4.4	<div>↓</div> <div>LRM kiểm tra việc thực hiện kế hoạch của phòng ban theo lịch biểu</div>	LRM sẽ tiến hành kiểm tra kế hoạch thực hiện Biện pháp khắc phục phòng ngừa lâu dài của phòng ban	LRM	LRM xác nhận được tình trạng thực hiện Biện pháp khắc phục phòng ngừa lâu dài của phòng ban	

*Biểu mẫu: BM_03

Bước 5: Theo dõi và đánh giá - Follow up action

Nội dung		Người chịu trách nhiệm	Kết quả đầu ra	Thời gian
Định kỳ hoặc thời điểm cần thiết theo yêu cầu, phòng LRM có trách nhiệm đánh giá:				
1	Hiệu quả quá trình xử lý sự cố của phòng ban	LRM	Bảng đánh giá quá trình xử lý sự cố	Tại kỳ audit hàng năm
2	Hiệu quả triển khai biện pháp khắc phục phòng ngừa lâu dài của phòng ban		Đánh giá hiệu quả việc thực hiện Biện pháp khắc phục phòng ngừa lâu dài theo lịch biểu mà phòng ban đề ra	
Tiêu chí đánh giá quá trình xử lý sự cố				
Tiêu chí	Đạt		Không đạt	
Mức độ kịp thời xử lý sự cố (kể từ thời điểm sự cố được phát hiện)	Sự cố được giải quyết đúng kế hoạch và thời gian quy định		Sự cố được giải quyết không đúng/muộn so với thời gian quy định	
Thời gian nộp báo cáo	Toàn bộ các báo cáo được nộp đúng thời hạn quy định		Toàn bộ các báo cáo được nộp muộn so với thời gian quy định	
Chất lượng báo cáo	<ul style="list-style-type: none">- Toàn bộ các trường thông tin trong báo cáo được điền đầy đủ.- Nội dung được ghi nhận trong báo cáo đều chính xác và phù hợp với yêu cầu được đưa ra.- Không xuất hiện nội dung, thông tin xung đột trong báo cáo.		<ul style="list-style-type: none">- Toàn bộ các trường thông tin trong báo cáo không được điền đầy đủ- Các nội dung trong báo cáo không rõ ràng và không phù hợp với các trường thông tin được yêu cầu trong báo cáo.- Xuất hiện nội dung, thông tin xung đột trong báo cáo.	
Phòng ban triển khai biện pháp khắc phục phòng ngừa lâu dài đúng kế hoạch	Phòng ban triển khai biện pháp phòng ngừa lâu dài đúng kế hoạch đề xuất		Phòng ban triển khai biện pháp muộn kế hoạch đề xuất.	
Hiệu quả sau khi áp dụng biện pháp khắc phục phòng ngừa lâu dài của phòng ban	LRM thực hiện đánh giá hiệu quả của Biện pháp khắc phục phòng ngừa lâu dài tại mỗi kỳ audit			

PHỤ LỤC: DANH SÁCH BIỂU MẪU ÁP DỤNG

STT	Biểu mẫu	Mã số	Hình thức lưu	Phòng/Ban lưu trữ	Link biểu mẫu	Ghi chú
1	Báo cáo nhanh sự cố/ Quick Report	BM_01	Bản mềm	Phòng LRM	https://sal.vn/phEbYP	
2	Báo cáo chi tiết sự cố/ Final Report	BM_02	Bản mềm	Phòng LRM	https://sal.vn/IMHrUc	<i>Áp dụng đối với những sự cố có mức độ ưu tiên Thấp</i>
3	Báo cáo chi tiết sự cố/ Final Report	BM_03	Bản mềm	Phòng LRM	https://sal.vn/NkxNfz	<i>Áp dụng đối với những sự cố có mức độ ưu tiên từ Trung Bình trở lên</i>