

Khôi phục sau thảm họa, Duy trì hoạt động kinh doanh và Ứng phó sự cố của ProcessMind

Ngày có hiệu lực: 14 tháng 9, 2026

Tài liệu này cung cấp bản tóm tắt khái quát về các quy trình khôi phục sau thảm họa (“DR”), duy trì hoạt động kinh doanh (“BCP”) và ứng phó sự cố bảo mật của ProcessMind B.V. đối với dịch vụ đám mây. Tài liệu này bổ sung cho [Các Biện pháp Bảo mật](#), [Chính sách Lưu trữ SaaS](#), [Thỏa thuận Mức dịch vụ](#) và [Phụ lục Xử lý Dữ liệu](#).

Tài liệu giải thích phương thức hiện tại của chúng tôi và không tạo ra các mục tiêu thời gian khôi phục, mục tiêu điểm khôi phục, bảo đảm về độ bền dữ liệu, thời hạn thông báo, mức dịch vụ hoặc tiêu chuẩn trách nhiệm pháp lý riêng biệt nào ngoài những nội dung được nêu rõ trong thỏa thuận, DPA hoặc SLA hiện hành.

1. Mục tiêu và Phạm vi

ProcessMind duy trì các quy trình này nhằm:

- bảo vệ tính bảo mật, tính toàn vẹn và tính sẵn có của Dữ liệu Khách hàng trong sự kiện gây gián đoạn
- khôi phục các thành phần dịch vụ sản xuất trọng yếu sau sự cố trong các hệ thống do ProcessMind kiểm soát
- tiếp tục quản lý sự cố, trao đổi thông tin với khách hàng và ra quyết định vận hành trong thời gian dịch vụ bị gián đoạn
- khôi phục sau sự cố ở tầng cơ sở hạ tầng, triển khai, ứng dụng hoặc dữ liệu bằng các quy trình đã được lập thành văn bản và định nghĩa cơ sở hạ tầng được quản lý bằng hệ thống kiểm soát phiên bản
- xác định và đánh giá Sự cố Bảo mật, ngăn chặn mối đe dọa, loại bỏ nguyên nhân gốc rễ, khôi phục các hệ thống bị ảnh hưởng, thực hiện thông báo theo yêu cầu và ghi nhận các bài học kinh nghiệm

Các quy trình này áp dụng cho dịch vụ đám mây ProcessMind trong môi trường sản xuất và các sự kiện bảo mật liên quan đến bên xử lý phụ hoặc dịch vụ đám mây trong phạm vi chúng ảnh hưởng đến Dịch vụ và ProcessMind có khả năng hợp lý để điều tra và quản lý. Các môi trường phát triển và thử nghiệm được tách biệt và không được xem là mục tiêu khôi phục cho các cam kết sản xuất hướng đến khách hàng.

2. Chiến lược khả năng phục hồi

2.1 Thiết kế khu vực. Các dịch vụ sản xuất được lưu trữ trên AWS EU (Frankfurt, Đức, eu-central-1). Kiến trúc dựa vào các dịch vụ được AWS quản lý trong khu vực đó, do AWS vận hành trên nhiều Vùng sẵn sàng. Cụm Aurora hiện chạy một phiên bản ghi duy nhất, vì vậy việc khôi phục cơ sở dữ liệu dựa vào các bản sao lưu tự động và khôi phục tại một thời điểm cụ thể thay vì một phiên bản dự phòng trong cùng khu vực. Hiện ProcessMind không vận hành khu vực dữ liệu khách hàng thứ hai đang hoạt động.

2.2 Dịch vụ được quản lý và không máy chủ. ProcessMind sử dụng AWS Lambda, Amazon API Gateway, Amazon CloudFront, Amazon Aurora PostgreSQL, Amazon S3, Amazon SQS, Amazon SNS và Amazon CloudWatch. Điều này làm giảm sự phụ thuộc vào các máy chủ hoạt động lâu dài do khách hàng quản lý và hỗ trợ khôi phục ứng dụng cũng như các thành phần tĩnh bằng cách xây dựng lại từ mã nguồn.

2.3 Tách biệt môi trường. Môi trường sản xuất và phát triển hoạt động trong các tài khoản AWS riêng biệt, với cơ sở dữ liệu và ngăn xếp hạ tầng riêng. Điều này làm giảm nguy cơ hoạt động phát triển ảnh hưởng đến các hoạt động khôi phục môi trường sản xuất.

2.4 Giám sát và phát hiện. Cảnh báo CloudWatch, bảng điều khiển, cảnh báo hàng đợi thư chết, ghi nhật ký tập trung và giám sát dịch vụ tổng hợp hỗ trợ phát hiện, phân loại và chuyển cấp sự cố. Các sự cố tiềm ẩn cũng có thể được xác định thông qua tiếp nhận yêu cầu hỗ trợ, báo cáo của nhân viên, thông báo của nhà cung cấp hoặc các yếu tố khác kích hoạt việc điều tra.

3. Ưu tiên khôi phục

Trong một sự cố nghiêm trọng, các ưu tiên khôi phục của ProcessMind nhìn chung là:

1. Bảo vệ tính toàn vẹn dữ liệu khách hàng và ngăn ngừa thiệt hại thêm.
2. Khoanh vùng sự cố và ổn định các hệ thống bị ảnh hưởng.
3. Khôi phục các đường truy cập sản xuất cốt lõi và quy trình làm việc trọng yếu.
4. Xác thực hoạt động của dịch vụ, tính toàn vẹn dữ liệu và việc giám sát trước khi tuyên bố hoàn tất khôi phục.
5. Thông báo cập nhật tình trạng, ảnh hưởng đến khách hàng và các hành động tiếp theo.

Trình tự cụ thể có thể thay đổi tùy thuộc vào tính chất của sự cố, bao gồm việc sự cố có ảnh hưởng đến tính toàn vẹn dữ liệu, quyền truy cập của khách hàng, xử lý bất đồng bộ hay hạ tầng hỗ trợ hay không.

4. Quy trình khôi phục sau thảm họa

4.1 Tuyên bố sự cố và điều phối. Các gián đoạn dịch vụ đáng kể và sự cố bảo mật được phân loại theo quy trình ứng phó sự cố. ProcessMind chỉ định người phụ trách sự cố, giới hạn việc tham gia ứng phó ở nhân sự được ủy quyền, đánh giá mức độ nghiêm trọng và phạm vi, điều phối nhân sự ứng phó kỹ thuật và theo dõi các hành động khôi phục cho đến khi sự cố được giải quyết hoặc hạ mức độ.

4.2 Khoanh vùng. ProcessMind nỗ lực hợp lý về mặt thương mại để ngăn chặn hoặc giảm thiểu ảnh hưởng đang tiếp diễn trước khi bắt đầu khôi phục trên diện rộng. Tùy thuộc vào dạng lỗi, các hành động khoanh vùng có thể bao gồm hoàn tác các thay đổi gần đây, vô hiệu hóa các đường dẫn bị ảnh hưởng, cô lập các thành phần hoạt động sai, tạm dừng xử lý nền trong khi

tiến hành kiểm tra tính toàn vẹn, thu hồi hoặc luân chuyển thông tin xác thực, hoặc chặn hoạt động lạm dụng.

4.3 Loại bỏ nguyên nhân. Sau khi tình trạng ảnh hưởng tức thời được ổn định, ProcessMind nỗ lực loại bỏ nguyên nhân gốc rễ hoặc điều kiện góp phần gây ra sự cố. Việc này có thể bao gồm áp dụng các bản sửa lỗi mã hoặc cấu hình, loại bỏ các thành phần độc hại, luân chuyển bí mật, khôi phục cấu hình đáng tin cậy hoặc đóng các đường truy cập bị lộ.

4.4 Khôi phục cơ sở dữ liệu. Aurora PostgreSQL thực hiện sao lưu tự động liên tục với thời hạn lưu giữ bảy (7) ngày và hỗ trợ khôi phục tại một thời điểm cụ thể. Nếu lỗi ở cấp cơ sở dữ liệu, sự kiện hỏng dữ liệu hoặc thay đổi phá hủy ngoài ý muốn đòi hỏi phải khôi phục, ProcessMind có thể khôi phục từ bản sao lưu phù hợp mới nhất hoặc tại một thời điểm được chọn, xác thực môi trường đã khôi phục và chuyển lưu lượng ứng dụng trở lại đường dẫn cơ sở dữ liệu đã khôi phục.

4.5 Khôi phục đối tượng và cấu phần. Tập khách hàng tải lên và cấu phần vận hành được lưu trữ trong Amazon S3. Tính năng tạo phiên bản được bật trên vùng lưu trữ tải lên và các vùng lưu trữ tài nguyên để hỗ trợ khôi phục trong trường hợp vô tình xóa hoặc ghi đè. Các vùng lưu trữ triển khai trang web và giao diện người dùng được xem là cấu phần có thể tái tạo và có thể được dựng lại từ mã nguồn thay vì khôi phục dưới dạng bản sao lưu.

4.6 Khôi phục khối lượng công việc bất đồng bộ. Các đường xử lý bất đồng bộ sử dụng hàng đợi thư chết để lưu giữ các sự kiện thất bại nhằm phục vụ điều tra. Việc khôi phục có thể bao gồm thử lại các thông điệp thất bại, chạy lại logic xử lý hoặc phát lại công việc nếu quy trình làm việc cơ sở hỗ trợ xử lý lại an toàn.

4.7 Dựng lại ứng dụng và hạ tầng. Hạ tầng được quản lý thông qua các định nghĩa hạ tầng dưới dạng mã được kiểm soát phiên bản. Nếu cần tạo lại hạ tầng ứng dụng hoặc tài sản tĩnh, ProcessMind có thể dựng lại và triển khai lại các thành phần bị ảnh hưởng từ các định nghĩa được kiểm soát phiên bản và cấu phần bản dựng.

4.8 Xác thực trước khi đưa dịch vụ trở lại hoạt động. Trước khi đóng sự cố, ProcessMind xác thực tình trạng dịch vụ bằng cách sử dụng hoạt động giám sát, nhật ký, kiểm tra tổng hợp và xác minh chức năng có mục tiêu hiện có, đồng thời khôi phục chức năng bị ảnh hưởng bằng các quy trình triển khai, khôi phục và hạ tầng đã được xác thực. Có thể tiến hành rà soát bổ sung khi sự cố liên quan đến việc khôi phục dữ liệu hoặc rủi ro về tính toàn vẹn dữ liệu.

5. Biện pháp duy trì hoạt động kinh doanh

5.1 Duy trì hoạt động. ProcessMind duy trì các quy trình vận hành được lập thành văn bản để việc xử lý sự cố, tiếp nhận yêu cầu hỗ trợ khách hàng, ứng phó kỹ thuật và ra quyết định có thể tiếp tục trong các sự kiện gây gián đoạn.

5.2 Truyền thông. Đối với các sự cố sản xuất đáng kể, ProcessMind nỗ lực hợp lý về mặt thương mại để cung cấp thông tin cập nhật qua các kênh hỗ trợ khách hàng và, khi phù hợp, trên trang trạng thái công khai tại processmind.com/status.

5.3 Quản lý thay đổi có kiểm soát. Vòng đời phát triển phần mềm theo nguyên tắc phòng thủ nhiều lớp, với nhiều lớp xác thực tự động độc lập, triển khai có kiểm soát, giám sát tập trung và rà soát sau sự cố, được sử dụng để giảm thiểu các sự cố ngừng hoạt động có thể tránh được và cải thiện khả năng duy trì hoạt động theo thời gian.

5.4 Bảo mật trong quá trình khôi phục. Các hành động khôi phục được thực hiện theo cùng các nguyên tắc bảo mật chung áp dụng trong hoạt động bình thường, bao gồm quyền truy cập tối thiểu cần thiết, ghi nhật ký hoạt động vận hành khi có thể và kiểm soát quyền truy cập vào hệ thống và dữ liệu sản xuất.

6. Tóm tắt về sao lưu và bảo vệ dữ liệu

6.1 Sao lưu cơ sở dữ liệu. Các bản sao lưu tự động của Aurora được mã hóa và lưu giữ trong bảy (7) ngày; có thể khôi phục tại một thời điểm cụ thể trong khoảng thời gian lưu giữ đó.

6.2 Biện pháp bảo vệ S3. Amazon S3 cung cấp độ bền cao cho các đối tượng được lưu trữ. Các vùng lưu trữ dữ liệu khách hàng có thể thay đổi dựa vào độ bền và tính năng tạo phiên bản trong khu vực chính. Hiện ProcessMind không bật tính năng sao chép S3 liên khu vực cho các vùng lưu trữ đó.

6.3 Nhật ký và chẩn đoán. Nhật ký, cảnh báo và dữ liệu đo từ xa tập trung hỗ trợ điều tra lỗi và xác thực việc khôi phục. Các cơ chế này hỗ trợ hoạt động duy trì liên tục nhưng bản thân chúng không được giới thiệu như một sản phẩm sao lưu riêng biệt.

7. Xác định và phân loại sự cố

7.1 Đánh giá ban đầu. Các sự kiện được báo cáo sẽ được phân loại để xác định liệu chúng có đáp ứng định nghĩa về Sự cố bảo mật hay không, hệ thống hoặc dữ liệu nào có thể bị ảnh hưởng, phạm vi và mức độ nghiêm trọng có khả năng xảy ra, cũng như liệu có cần khoanh vùng ngay lập tức hay không. Việc bảo toàn chứng cứ được thực hiện theo cách phù hợp với tính chất của sự cố và các hệ thống liên quan.

7.2 Trực xử lý và chuyển cấp. ProcessMind duy trì nhân sự trực xử lý các sự cố sản xuất, bao gồm trực 24x7 đối với các sự cố Nghiêm trọng (theo định nghĩa trong Thỏa thuận mức dịch vụ), để sự cố có thể được xác nhận tiếp nhận và phân loại bất cứ lúc nào.

7.3 Lập hồ sơ. ProcessMind lập hồ sơ về các phát hiện điều tra đáng kể, hành động ứng phó và quyết định khôi phục để có thể rà soát dòng thời gian sự cố và các hành động khắc phục phát sinh sau sự kiện.

8. Truyền thông và thông báo

8.1 Truyền thông nội bộ. ProcessMind điều phối nhân sự ứng phó, người ra quyết định và các kênh hỗ trợ để bảo đảm hoạt động ứng phó kỹ thuật và truyền thông với khách hàng được thống nhất trong suốt vòng đời sự cố.

8.2 Thông báo cho khách hàng. Trong trường hợp xảy ra Sự cố bảo mật cần thông báo theo DPA hoặc luật hiện hành, ProcessMind thông báo cho khách hàng bị ảnh hưởng mà không chậm trễ quá mức và, nếu khả thi, trong vòng bảy mươi hai (72) giờ kể từ khi biết về sự cố. Thông báo thường bao gồm tính chất và phạm vi của sự cố, các loại dữ liệu bị ảnh hưởng nếu đã biết, biện pháp đã thực hiện để khoanh vùng và khắc phục sự cố, cũng như các hành động được khuyến nghị cho khách hàng nếu có liên quan.

8.3 Cập nhật liên tục. Khi sự cố vẫn đang diễn ra hoặc các sự kiện trọng yếu thay đổi, ProcessMind cung cấp thông tin cập nhật tiếp theo khi có thêm thông tin đã được xác minh. Đối với các gián đoạn dịch vụ sản xuất trên diện rộng, ProcessMind cũng có thể sử dụng các kênh hỗ trợ khách hàng và, khi phù hợp, trạng thái công khai tại processmind.com/status.

9. Kiểm thử, rà soát và bảo trì

ProcessMind rà soát các quy trình này ít nhất hằng năm và sau các sự cố đáng kể hoặc thay đổi kiến trúc quan trọng, định kỳ diễn tập các yếu tố liên quan trong phương thức ứng phó và khôi phục (chẳng hạn như khôi phục bản sao lưu, dựng lại triển khai, giám sát, cảnh báo và truyền thông về sự cố), đồng thời đưa các bài học kinh nghiệm vào quy trình bảo mật, độ tin cậy và duy trì hoạt động.

10. Giới hạn và ranh giới hợp đồng

Tài liệu này là bản tóm tắt ở cấp độ tổng quan và không mô tả chi tiết mọi số tay vận hành nội bộ, đường chuyển cấp, phương pháp điều tra hoặc bước xử lý chứng cứ. Tài liệu này không cam kết ProcessMind sẽ có thiết kế chuyển đổi dự phòng liên khu vực riêng biệt, lưu giữ bất biến đối với mọi

vùng lưu trữ có thể thay đổi hoặc bảo đảm RTO/RPO độc lập ngoài những nội dung được nêu rõ trong thỏa thuận hoặc đơn đặt hàng áp dụng.

Nếu có bất kỳ mâu thuẫn nào giữa tài liệu này với Thỏa thuận khách hàng, Phụ lục xử lý dữ liệu, Thỏa thuận mức dịch vụ áp dụng hoặc quy định pháp luật bắt buộc, thì các nguồn đó sẽ được ưu tiên áp dụng.