

การกู้คืนจากภัยพิบัติ ความต่อเนื่องทางธุรกิจ และการตอบสนองต่อเหตุการณ์ของ ProcessMind

วันที่มีผลบังคับใช้: 14 กันยายน 2026

เอกสารนี้สรุปภาพรวมขั้นตอนการกู้คืนจากภัยพิบัติ ("DR") ความต่อเนื่องทางธุรกิจ ("BCP") และการตอบสนองต่อเหตุการณ์ด้านความปลอดภัยของ ProcessMind B.V. สำหรับบริการคลาวด์ เอกสารนี้เป็นเอกสารเพิ่มเติมจาก [มาตรการรักษาความปลอดภัย](#) [นโยบายการให้บริการ SaaS](#) [ข้อตกลงระดับการให้บริการ](#) และ [ภาคผนวกการประมวลผลข้อมูล](#).

เอกสารนี้อธิบายแนวทางปัจจุบันของเรา และไม่ได้กำหนดวัตถุประสงค์ด้านระยะเวลาการกู้คืน วัตถุประสงค์ด้านจุดกู้คืน การรับประกันความคงทนของข้อมูล กำหนดเวลาแจ้งเตือนระดับการให้บริการ หรือมาตรฐานความรับผิดชอบต่างหาก นอกเหนือจากที่ระบุไว้อย่างชัดเจนในข้อตกลง ภาคผนวกการประมวลผลข้อมูล หรือข้อตกลงระดับการให้บริการที่เกี่ยวข้อง.

1. วัตถุประสงค์และขอบเขต

ProcessMind จัดให้มีขั้นตอนเหล่านี้เพื่อ:

- คุ้มครองการรักษาความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานของข้อมูลลูกค้าในระหว่างเหตุการณ์ที่ก่อให้เกิดการหยุดชะงัก
- กู้คืนองค์ประกอบสำคัญของบริการที่ใช้งานจริงหลังจากเกิดความขัดข้องในระบบที่ ProcessMind ควบคุม
- ดำเนินการจัดการเหตุการณ์ การสื่อสารกับลูกค้า และการตัดสินใจด้านการปฏิบัติการต่อไปในระหว่างที่บริการหยุดชะงัก
- กู้คืนจากความขัดข้องของโครงสร้างพื้นฐาน การนำระบบขึ้นใช้งาน แอปพลิเคชัน หรือชั้นข้อมูล โดยใช้ขั้นตอนที่จัดทำเป็นเอกสารและคำจำกัดความโครงสร้างพื้นฐานที่ควบคุมด้วยระบบควบคุมเวอร์ชัน
- ระบุนโยบายและประเมินเหตุการณ์ด้านความปลอดภัย ควบคุมภัยคุกคาม กำจัดสาเหตุราก กู้คืนระบบที่ได้รับผลกระทบ สื่อสารตามที่กำหนด และบันทึกบทเรียนที่ได้รับ

ขั้นตอนเหล่านี้ใช้กับบริการคลาวด์ ProcessMind สำหรับการใช้งานจริง และเหตุการณ์ด้านความปลอดภัยที่เกี่ยวข้องกับผู้ประมวลผลช่วงหรือบริการคลาวด์ เท่าที่เหตุการณ์ดัง

กล่าวส่งผลกระทบต่อบริการและอยู่ในขอบเขตที่ ProcessMind สามารถตรวจสอบและจัดการได้ตามสมควร สภาพแวดล้อมสำหรับการพัฒนาและการทดสอบแยกออกจากกัน และไม่ถือเป็นเป้าหมายการกู้คืนสำหรับข้อมูลพื้นฐานในการให้บริการจริงแก่ลูกค้า.

2. กลยุทธ์ด้านความยืดหยุ่น

2.1 การออกแบบระดับภูมิภาค บริการสำหรับการใช้งานจริงโฮสต์อยู่บน AWS EU (แฟรงก์เฟิร์ต ประเทศเยอรมนี eu-central-1) สถาปัตยกรรมอาศัยบริการที่ AWS จัดการภายในภูมิภาคดังกล่าว ซึ่ง AWS ดำเนินการครอบคลุม Availability Zones หลายแห่ง ปัจจุบันคลัสเตอร์ Aurora ทำงานด้วยอินสแตนซ์ writer เพียงรายการเดียว ดังนั้นการกู้คืนฐานข้อมูลจึงอาศัยข้อมูลสำรองอัตโนมัติและการกู้คืน ณ จุดเวลา แทนการมีระบบสำรองภายในภูมิภาค ปัจจุบัน ProcessMind ไม่ได้ดำเนินการภูมิภาคที่สองสำหรับข้อมูลลูกค้าแบบแอ็กทีฟ.

2.2 บริการแบบมีการจัดการและแบบ Serverless ProcessMind ใช้ AWS Lambda, Amazon API Gateway, Amazon CloudFront, Amazon Aurora PostgreSQL, Amazon S3, Amazon SQS, Amazon SNS และ Amazon CloudWatch ซึ่งช่วยลดการพึ่งพาเซิร์ฟเวอร์ที่มีอายุการใช้งานยาวนานซึ่งลูกค้าต้องจัดการเอง และสนับสนุนการกู้คืนโดยสร้างแอปพลิเคชันและองค์ประกอบแบบคงที่ขึ้นใหม่จากซอร์สโค้ด

2.3 การแยกสภาพแวดล้อม สภาพแวดล้อมสำหรับการใช้งานจริงและการพัฒนาดำเนินการอยู่ในบัญชี AWS แยกจากกัน โดยมีฐานข้อมูลและชุดโครงสร้างพื้นฐานแยกกัน ซึ่งช่วยลดความเสี่ยงที่กิจกรรมการพัฒนาจะส่งผลกระทบต่อการกู้คืนระบบสำหรับการใช้งานจริง.

2.4 การติดตามตรวจสอบและการตรวจจับ การแจ้งเตือนของ CloudWatch แดชบอร์ด การแจ้งเตือนคิว dead-letter การบันทึกข้อมูลแบบรวมศูนย์ และการติดตามตรวจสอบบริการแบบสังเคราะห์ สนับสนุนการตรวจจับ การประเมินเบื้องต้น และการยกระดับเหตุการณ์ นอกจากนี้ อาจระบุเหตุการณ์ที่อาจเกิดขึ้นได้จากการรับเรื่องสนับสนุน รายงานจากพนักงาน การแจ้งเตือนจากผู้ให้บริการ หรือสิ่งกระตุ้นอื่น ๆ ให้ตรวจสอบ.

3. ลำดับความสำคัญในการกู้คืน

โดยทั่วไป ลำดับความสำคัญในการกู้คืนของ ProcessMind ระหว่างเหตุการณ์ร้ายแรงมีดังนี้:

1. คุ้มครองความถูกต้องสมบูรณ์ของข้อมูลลูกค้าและป้องกันความเสียหายเพิ่มเติม
2. ควบคุมเหตุการณ์และทำให้ระบบที่ได้รับผลกระทบมีเสถียรภาพ
3. กู้คืนช่องทางการเข้าถึงหลักสำหรับการใช้งานจริงและเวิร์กโฟลว์ที่สำคัญ
4. ตรวจสอบความถูกต้องของการทำงานของบริการ ความถูกต้องสมบูรณ์ของข้อมูล และการติดตามตรวจสอบ ก่อนประกาศว่าการกู้คืนเสร็จสมบูรณ์
5. แจ้งข้อมูลอัปเดตเกี่ยวกับสถานะ ผลกระทบต่อลูกค้า และการดำเนินการติดตามผล.

ลำดับที่แน่นอนอาจแตกต่างกันไปตามลักษณะของเหตุการณ์ รวมถึงว่าเหตุการณ์นั้นส่งผลกระทบต่อความถูกต้องสมบูรณ์ของข้อมูล การเข้าถึงของลูกค้า การประมวลผลแบบอะซิงโครนัส หรือโครงสร้างพื้นฐานสนับสนุนหรือไม่.

4. ขั้นตอนการกู้คืนจากภัยพิบัติ

4.1 การประกาศเหตุการณ์และการประสานงาน การหยุดชะงักของบริการที่มีนัยสำคัญ และเหตุการณ์ด้านความปลอดภัยจะได้รับการประเมินเบื้องต้นตามขั้นตอนการตอบสนองต่อเหตุการณ์ ProcessMind แต่งตั้งหัวหน้ารับผิดชอบเหตุการณ์ จำกัดการมีส่วนร่วมในการตอบสนองไว้เฉพาะบุคลากรที่ได้รับอนุญาต ประเมินความรุนแรงและขอบเขต ประสานงานผู้ตอบสนองด้านเทคนิค และติดตามการดำเนินการกู้คืนจนกว่าเหตุการณ์จะได้รับการแก้ไขหรือลดระดับ.

4.2 การควบคุมเหตุการณ์ ProcessMind ใช้ความพยายามตามสมควรในเชิงพาณิชย์เพื่อหยุดหรือลดผลกระทบที่กำลังเกิดขึ้นก่อนเริ่มการกู้คืนในวงกว้าง การดำเนินการควบคุมอาจรวมถึงการย้อนกลับการเปลี่ยนแปลงล่าสุด การปิดใช้งานช่องทางที่ได้รับผลกระทบ การแยกองค์ประกอบที่ทำงานผิดปกติ การหยุดการประมวลผลเบื้องหลังชั่วคราวระหว่างตรวจสอบความถูกต้องสมบูรณ์ การเพิกถอนหรือเปลี่ยนข้อมูลรับรอง หรือการปิดกั้นกิจกรรมที่เป็นการละเมิด ทั้งนี้ขึ้นอยู่กับรูปแบบความขัดข้อง.

4.3 การกำจัดสาเหตุ หลังจากควบคุมผลกระทบเฉพาะหน้าให้มีเสถียรภาพแล้ว ProcessMind จะดำเนินการกำจัดสาเหตุหลักหรือเงื่อนไขที่มีส่วนทำให้เกิดเหตุ ซึ่งอาจรวมถึงการใช้การแก้ไขโค้ดหรือการกำหนดค่า การนำสิ่งที่เป็อันตรายนอก การเปลี่ยนข้อมูลลับ การคืนค่าการกำหนดค่าที่เชื่อถือได้ หรือการปิดช่องทางการเข้าถึงที่เปิดเผย.

4.4 การกู้คืนฐานข้อมูล Aurora PostgreSQL สำรองข้อมูลอัตโนมัติอย่างต่อเนื่อง โดยเก็บรักษาข้อมูลไว้เจ็ด (7) วัน และรองรับการกู้คืน ณ จุดเวลา หากความขัดข้องระดับฐาน

ข้อมูล เหตุการณ์ข้อมูลเสียหาย หรือการเปลี่ยนแปลงที่ทำลายข้อมูลโดยไม่ตั้งใจจำเป็นต้องได้รับการกู้คืน ProcessMind อาจกู้คืนจากข้อมูลสำรองล่าสุดที่เหมาะสมหรือ ณ จุดเวลาที่เลือก ตรวจสอบสภาพแวดล้อมที่กู้คืนแล้ว และเปลี่ยนเส้นทางการรับส่งข้อมูลของแอปพลิเคชันกลับไปยังฐานข้อมูลที่ถูกคืนแล้ว.

4.5 การกู้คืนออบเจกต์และสิ่งที่สร้างขึ้น ไฟล์ที่ถูกค่าอัปโหลดและสิ่งที่สร้างขึ้นจากการปฏิบัติการจัดเก็บไว้ใน Amazon S3 โดยเปิดใช้การกำหนดเวอร์ชันในบักเก็ตสำหรับการอัปโหลดและบักเก็ตทรัพยากร เพื่อรองรับการกู้คืนในกรณีลบหรือเขียนทับโดยไม่ตั้งใจ บักเก็ตสำหรับติดตั้งใช้งานเว็บไซต์และส่วนหน้าเว็บถือเป็นสิ่งที่สร้างซ้ำได้ และอาจสร้างใหม่จากซอร์สโค้ดแทนการกู้คืนจากข้อมูลสำรอง.

4.6 การกู้คืนภาระงานแบบอะซิงโครนัส เส้นทางการประมวลผลแบบอะซิงโครนัสใช้คิว dead-letter เพื่อเก็บเหตุการณ์ที่ล้มเหลวไว้สำหรับการตรวจสอบ การกู้คืนอาจรวมถึงการลองส่งข้อความที่ล้มเหลวอีกครั้ง การเรียกใช้ตรรกะการประมวลผลซ้ำ หรือการเล่นงานซ้ำในกรณีที่เวิร์กโฟลว์พื้นฐานรองรับการประมวลผลซ้ำอย่างปลอดภัย.

4.7 การสร้างแอปพลิเคชันและโครงสร้างพื้นฐานใหม่ โครงสร้างพื้นฐานได้รับการจัดการผ่านคำจำกัดความโครงสร้างพื้นฐานในรูปแบบโค้ดที่ควบคุมเวอร์ชันด้วยซอร์สโค้ด หากจำเป็นต้องสร้างโครงสร้างพื้นฐานของแอปพลิเคชันหรือทรัพยากรแบบคงที่ขึ้นใหม่ ProcessMind สามารถสร้างและติดตั้งใช้งานองค์ประกอบที่ได้รับผลกระทบอีกครั้งจากคำจำกัดความและสิ่งที่สร้างขึ้นซึ่งควบคุมเวอร์ชันไว้.

4.8 การตรวจสอบก่อนกลับมาให้บริการ ก่อนปิดเหตุการณ์ ProcessMind จะตรวจสอบสถานะความพร้อมใช้งานของบริการโดยใช้การติดตามตรวจสอบ บันทึกข้อมูล การตรวจสอบแบบสังเคราะห์ และการตรวจสอบการทำงานเฉพาะจุดที่มีอยู่ และกู้คืนฟังก์ชันการทำงานที่ได้รับผลกระทบโดยใช้ขั้นตอนการติดตั้งใช้งาน การกู้คืน และโครงสร้างพื้นฐานที่ผ่านการตรวจสอบแล้ว อาจมีการทบทวนเพิ่มเติมเมื่อเหตุการณ์เกี่ยวข้องกับการกู้คืนข้อมูลหรือความเสี่ยงต่อความถูกต้องสมบูรณ์ของข้อมูล.

5. มาตรการด้านความต่อเนื่องทางธุรกิจ

5.1 ความต่อเนื่องในการปฏิบัติการ ProcessMind จัดทำและเก็บรักษาขั้นตอนการปฏิบัติการเป็นลายลักษณ์อักษร เพื่อให้การจัดการเหตุการณ์ การรับเรื่องสนับสนุนลูกค้า การตอบสนองด้านวิศวกรรม และการตัดสินใจสามารถดำเนินต่อไปได้ในระหว่างเหตุการณ์ที่ก่อให้เกิดการหยุดชะงัก.

5.2 การสื่อสาร สำหรับเหตุการณ์ที่มีนัยสำคัญในการให้บริการจริง ProcessMind ใช้ความพยายามตามสมควรในเชิงพาณิชย์เพื่อแจ้งข้อมูลอัปเดตผ่านช่องทางสนับสนุนลูกค้าและหากเหมาะสม ผ่านหน้าสถานะสาธารณะที่ processmind.com/status.

5.3 การจัดการการเปลี่ยนแปลงแบบควบคุม มีการใช้วงจรการพัฒนาซอฟต์แวร์แบบการป้องกันหลายชั้น ซึ่งประกอบด้วยชั้นการตรวจสอบอัตโนมัติที่เป็นอิสระต่อกันหลายชั้น การติดตั้งใช้งานแบบควบคุม การติดตามตรวจสอบแบบรวมศูนย์ และการทบทวนหลังเกิดเหตุการณ์ เพื่อลดการหยุดชะงักที่หลีกเลี่ยงได้และปรับปรุงความต่อเนื่องเมื่อเวลาผ่านไป.

5.4 ความปลอดภัยระหว่างการกู้คืน การดำเนินการกู้คืนอยู่ภายใต้หลักการรักษาความปลอดภัยทั่วไปเช่นเดียวกับที่ใช้ระหว่างการปฏิบัติการตามปกติ รวมถึงการให้สิทธิ์เข้าถึงเท่าที่จำเป็น การบันทึกกิจกรรมการปฏิบัติการเมื่อมีระบบรองรับ และการควบคุมการเข้าถึงระบบและข้อมูลสำหรับการใช้งานจริง.

6. สรุปการสำรองข้อมูลและการคุ้มครองข้อมูล

6.1 การสำรองฐานข้อมูล ข้อมูลสำรองอัตโนมัติของ Aurora ได้รับการเข้ารหัสและเก็บรักษาไว้เป็นเวลาเจ็ด (7) วัน โดยสามารถกู้คืน ณ จุดเวลาได้ภายในระยะเวลาเก็บรักษาดังกล่าว.

6.2 มาตรการคุ้มครอง S3 Amazon S3 ให้ความทนทานสูงสำหรับออบเจกต์ที่จัดเก็บไว้ บังเกิดข้อมูลลูกค้าที่เปลี่ยนแปลงได้อาศัยความทนทานและการกำหนดเวอร์ชันภายในภูมิภาคหลัก ปัจจุบัน ProcessMind ไม่ได้เปิดใช้การจำลองข้อมูล S3 ข้ามภูมิภาคสำหรับบังเกิดเหล่านั้น.

6.3 บันทึกและการวินิจฉัย บันทึกข้อมูล การแจ้งเตือน และข้อมูลเทเลเมทรีแบบรวมศูนย์สนับสนุนการตรวจสอบความขัดข้องและการตรวจสอบการกู้คืน กลไกเหล่านี้สนับสนุนการปฏิบัติการเพื่อความต่อเนื่อง แต่ไม่ได้ถือเป็นผลิตภัณฑ์สำรองข้อมูลแยกต่างหาก.

7. การระบุและประเมินเหตุการณ์เบื้องต้น

7.1 การประเมินเบื้องต้น เหตุการณ์ที่มีการรายงานจะได้รับการประเมินเบื้องต้นเพื่อพิจารณาว่าเข้าเกณฑ์นิยามของเหตุการณ์ด้านความปลอดภัยหรือไม่ ระบบหรือข้อมูลใดอาจได้รับผลกระทบ ขอบเขตและความรุนแรงที่คาดว่าจะเกิดขึ้น และจำเป็นต้องควบคุม

เหตุการณ์โดยทันทีหรือไม่ การเก็บรักษาพยานหลักฐานจะดำเนินการในลักษณะที่เหมาะสมกับลักษณะของเหตุการณ์และระบบที่เกี่ยวข้อง.

7.2 การปฏิบัติหน้าที่เวรและการยกระดับ ProcessMind จัดให้มีเจ้าหน้าที่เวรสำหรับเหตุการณ์ที่เกิดกับระบบใช้งานจริง รวมถึงการให้บริการตลอด 24 ชั่วโมงทุกวันสำหรับเหตุการณ์ระดับวิกฤต (ตามนิยามในข้อตกลงระดับการให้บริการ) เพื่อให้สามารถรับทราบและประเมินเบื้องต้นเกี่ยวกับเหตุการณ์ได้ตลอดเวลา.

7.3 การจัดทำเอกสาร ProcessMind จัดทำเอกสารบันทึกผลการตรวจสอบที่มีนัยสำคัญ การดำเนินการตอบสนอง และการตัดสินใจเกี่ยวกับการกู้คืน เพื่อให้สามารถทบทวนลำดับเหตุการณ์และการดำเนินการแก้ไขที่เกิดขึ้นภายหลังเหตุการณ์ได้.

8. การสื่อสารและการแจ้งเตือน

8.1 การสื่อสารภายใน ProcessMind ประสานงานผู้ตอบสนอง ผู้มีอำนาจตัดสินใจ และช่องทางสนับสนุน เพื่อให้การตอบสนองทางเทคนิคและการสื่อสารกับลูกค้าสอดคล้องกันตลอดวงจรชีวิตของเหตุการณ์.

8.2 การแจ้งลูกค้า ในกรณีที่เกิดเหตุการณ์ด้านความปลอดภัยซึ่งต้องแจ้งตาม DPA หรือกฎหมายที่ใช้บังคับ ProcessMind จะแจ้งลูกค้าที่ได้รับผลกระทบโดยไม่ชักช้าเกินควร และหากสามารถทำได้ ภายในเจ็ดสิบสอง (72) ชั่วโมงนับแต่ทราบเหตุการณ์ โดยทั่วไปการแจ้งจะระบุลักษณะและขอบเขตของเหตุการณ์ ประเภทข้อมูลที่ได้รับผลกระทบหากทราบ มาตรการที่ดำเนินการเพื่อควบคุมและแก้ไขเหตุการณ์ และการดำเนินการที่แนะนำให้ลูกค้าทำในกรณีที่เกี่ยวข้อง.

8.3 การแจ้งข้อมูลอัปเดตอย่างต่อเนื่อง หากเหตุการณ์ยังดำเนินอยู่หรือข้อเท็จจริงที่มีนัยสำคัญเปลี่ยนแปลง ProcessMind จะให้ข้อมูลอัปเดตติดตามผลเมื่อมีข้อมูลเพิ่มเติมที่ผ่านการตรวจสอบแล้ว สำหรับการหยุดชะงักของบริการจริงในวงกว้าง ProcessMind อาจใช้ช่องทางสนับสนุนลูกค้า และหากเหมาะสม ใช้หน้าสถานะสาธารณะที่ processmind.com/status.

9. การทดสอบ การทบทวน และการบำรุงรักษา

ProcessMind ทบทวนขั้นตอนเหล่านี้อย่างน้อยปีละครั้งและหลังเกิดเหตุการณ์ที่มีนัยสำคัญหรือการเปลี่ยนแปลงสถาปัตยกรรมครั้งสำคัญ ทดสอบองค์ประกอบที่เกี่ยวข้องของ

แนวทางการตอบสนองและการกู้คืนเป็นระยะ (เช่น การกู้คืนจากข้อมูลสำรอง การสร้างการติดตั้งใช้งานใหม่ การติดตามตรวจสอบ การแจ้งเตือน และการสื่อสารเกี่ยวกับเหตุการณ์) และนำบทเรียนที่ได้รับมาปรับใช้ในขั้นตอนด้านความปลอดภัย ความน่าเชื่อถือ และความต่อเนื่อง.

10. ข้อจำกัดและขอบเขตตามสัญญา

เอกสารฉบับนี้เป็นบทสรุประดับสูง และไม่ได้อธิบายคู่มือปฏิบัติการภายในทุกฉบับ เส้นทางการยกระดับ วิธีการตรวจสอบ หรือขั้นตอนการจัดการพยานหลักฐานโดยละเอียดในเชิงปฏิบัติการ เอกสารฉบับนี้ไม่ได้ผูกพัน ProcessMind ให้จัดการการออกแบบการสลับระบบข้ามภูมิภาคแยกต่างหาก การเก็บรักษาข้อมูลแบบแก้ไขไม่ได้สำหรับบันทึกที่เปลี่ยนแปลงได้ทั้งหมด หรือการรับประกัน RTO/RPO ที่เป็นอิสระ นอกเหนือจากที่ระบุไว้อย่างชัดเจนในข้อตกลงหรือคำสั่งซื้อที่ใช้บังคับ.

หากเอกสารฉบับนี้ขัดแย้งกับข้อตกลงลูกค้า ภาคผนวกการประมวลผลข้อมูล ข้อตกลงระดับการให้บริการ หรือกฎหมายที่มีผลบังคับเป็นการทั่วไป ให้ยึดถือเอกสารหรือกฎหมายดังกล่าวเป็นหลัก.