

มาตรการรักษาความปลอดภัยของ ProcessMind

วันที่มีผลบังคับใช้: 14 กันยายน 2026

เอกสารฉบับนี้อธิบายมาตรการทางเทคนิคและองค์กร ("TOMs") ที่ ProcessMind B.V. ดำเนินการเพื่อคุ้มครองการรักษาความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานของข้อมูลลูกค้า ProcessMind ใช้แนวทางการป้องกันเชิงลึก โดยมีชั้นการรักษาความปลอดภัยอิสระหลายชั้นคุ้มครองข้อมูลลูกค้าในทุกระดับ ตั้งแต่เครือข่ายและโครงสร้างพื้นฐาน ไปจนถึงข้อมูลระดับตัวตน การอนุญาต การแยกข้อมูล การเข้ารหัส การตรวจสอบ และการพัฒนาซอฟต์แวร์ มาตรการเหล่านี้เป็นส่วนเพิ่มเติมจาก[ภาคผนวกการประมวลผลข้อมูล นโยบายความเป็นส่วนตัว](#) และ[นโยบายการโฮสต์ SaaS](#) ProcessMind ทบทวนและปรับปรุงมาตรการเหล่านี้อย่างน้อยปีละครั้ง.

ข้อมูลลูกค้าจะไม่ถูกขายให้ แบ่งปันกับ หรือใช้โดยบุคคลภายนอกเพื่อวัตถุประสงค์ของบุคคลภายนอกนั้นโดยเด็ดขาด.

1. ความปลอดภัยของโครงสร้างพื้นฐาน

1.1 แพลตฟอร์มคลาวด์. ProcessMind โฮสต์บน Amazon Web Services (AWS) ในสหภาพยุโรป (แฟรงก์เฟิร์ต ประเทศเยอรมนี eu-central-1) เท่านั้น AWS ได้รับการรับรอง ISO 27001, ISO 27017, ISO 27018, SOC 1/2/3 และ PCI DSS โปรดดู[โปรแกรมการปฏิบัติตามข้อกำหนดของ AWS](#) สำหรับรายการทั้งหมด.

1.2 สถาปัตยกรรมแบบ Serverless. ตรรกะการทำงานของแอปพลิเคชัน ProcessMind ทำงานบน AWS Lambda และบริการที่ AWS จัดการให้ ProcessMind ไม่ได้ดำเนินการเซิร์ฟเวอร์แอปพลิเคชันที่ลูกค้าจัดการเองและทำงานต่อเนื่องเป็นเวลานาน ซึ่งช่วยลดงานด้านการติดตั้งแพตช์ระบบปฏิบัติการและการเสริมความปลอดภัยของเซิร์ฟเวอร์จำนวนมาก.

1.3 ขอบเขตเครือข่าย. ProcessMind ดูแล AWS VPC สำหรับการควบคุมฐานข้อมูลและเครือข่าย Aurora PostgreSQL ทำงานในซับเน็ตส่วนตัวที่ไม่มีการเชื่อมต่อขาออกสู่อินเทอร์เน็ต ไม่สามารถเข้าถึงได้จากสาธารณะ และเปิดใช้งานบันทึกการไหลของ VPC โดยปกติ ProcessMind จะไม่วางฟังก์ชัน Lambda ของแอปพลิเคชันไว้ภายใน VPC Lambda เชื่อมต่อกับ Aurora ผ่าน AWS RDS Data API โดยใช้ TLS พร้อมการยืนยันตัวตนผ่าน IAM และ Secrets Manager.

1.4 การส่งมอบเนื้อหาและการควบคุม Edge เว็บไซต์ที่ให้บริการแก่ลูกค้า, SPA ส่วนหน้า และการรับส่งข้อมูลทรัพยากรสาธารณะให้บริการผ่าน Amazon CloudFront การกระจาย CloudFront ทั้งหมดกำหนดนโยบาย TLS ขั้นต่ำเป็น TLS 1.2 (2021) การกระจาย เว็บไซต์และ SPA ส่วนหน้ายังเพิ่มส่วนหัวการตอบกลับด้านความปลอดภัย ซึ่งรวมถึง HTTP Strict Transport Security (HSTS), Content Security Policy (CSP), frame-ancestors 'none', X-Frame-Options: DENY, X-Content-Type-Options, นโยบายผู้อ้างอิง และนโยบายสิทธิ์ การกระจายทรัพยากรสาธารณะใช้ CloudFront Origin Access Control เพื่อให้เกิดกีดกันเป็นส่วนตัว การรับส่งข้อมูล API ที่ให้บริการแก่ลูกค้าจัดการแยกต่างหากผ่าน Amazon API Gateway: การรับส่งคำขอ/การตอบกลับ HTTPS ให้บริการผ่าน HTTP API บนโดเมนย่อย API เฉพาะ และการเชื่อมต่อไคลเอนต์แบบเรียลไทม์ให้บริการผ่าน API Gateway WebSocket API แยกต่างหากบนโดเมนย่อย WebSocket เฉพาะ

1.5 การแยกสภาพแวดล้อม. สภาพแวดล้อมการใช้งานจริงและการพัฒนาใช้บัญชี AWS ฐานข้อมูล และชุดโครงสร้างพื้นฐานแยกจากกัน ข้อมูลประจำตัวของนักพัฒนาไม่อนุญาตให้เข้าถึงข้อมูลลูกค้าในระบบใช้งานจริง.

2. การเข้ารหัสข้อมูล

2.1 การเข้ารหัสระหว่างการส่ง. ข้อมูลทั้งหมดที่ส่งระหว่างไคลเอนต์กับบริการของ ProcessMind จะได้รับการเข้ารหัสโดยใช้ TLS 1.2 หรือสูงกว่า จุดเชื่อมต่อที่ให้บริการแก่ลูกค้าเปิดให้เข้าถึงผ่าน HTTPS บัณฑิต S3 หัวข้อ SNS และคิว SQS ที่ ProcessMind สร้างขึ้นโดยตรงกำหนดให้เข้าถึงได้ผ่าน SSL เท่านั้น การเข้าถึงฐานข้อมูลผ่าน RDS Data API และการเรียกใช้บริการ AWS อื่น ๆ ใช้ HTTPS/TLS.

2.2 การเข้ารหัสขณะจัดเก็บ. Aurora PostgreSQL เข้ารหัสขณะจัดเก็บโดยใช้คีย์ AWS KMS ที่ลูกค้าจัดการ พร้อมการหมุนเวียนคีย์โดยอัตโนมัติ บัณฑิต S3 สำหรับข้อมูลลูกค้า และการปฏิบัติงานที่ ProcessMind สร้างขึ้นโดยตรง รวมถึงบัณฑิตสำหรับการอัปโหลดทรัพยากร และบันทึกการเข้าถึง ใช้คีย์ KMS ที่ลูกค้าจัดการ กลุ่มบันทึก CloudWatch หัวข้อ SNS และคิว SQS ที่ ProcessMind สร้างขึ้นโดยตรงก็ใช้คีย์ KMS ที่ลูกค้าจัดการ เช่นกัน บัณฑิตต้นทางของเว็บไซต์และส่วนหน้าที่ SST จัดการใช้การเข้ารหัสฝั่งเซิร์ฟเวอร์ของ S3 ที่ AWS จัดการ (SSE-S3 / AES-256) แทนคีย์ KMS ที่ลูกค้าจัดการ.

2.3 การจัดการคีย์และข้อมูลลับ. คีย์เข้ารหัสฐานข้อมูลได้รับการจัดการจากส่วนกลางผ่าน AWS KMS และการเข้าถึงคีย์อยู่ภายใต้การกำกับดูแลของนโยบาย IAM ตามหลักสิทธิ์เท่า

ที่จำเป็น ข้อมูลประจำตัวฐานข้อมูลจัดเก็บไว้ใน AWS Secrets Manager ข้อมูลหลักของ Aurora และข้อมูลลับของผู้ใช้แอปพลิเคชันที่มีสิทธิ์จำกัดจะหมุนเวียนโดยอัตโนมัติทุกสามสิบ (30) วัน คีย์และข้อมูลลับของระบบใช้งานจริงจะไม่จัดเก็บไว้ในซอร์สโค้ดโดยเด็ดขาด ข้อมูลประจำตัวที่ใช้เฉพาะในการพัฒนาจะแยกออกจากระบบใช้งานจริง ทรัพยากรสนับสนุนบางรายการที่ AWS/CDK/SST จัดการยังคงใช้การเข้ารหัสที่ AWS จัดการ ในกรณีที่บริการหรือเฟรมเวิร์กไม่มีการตั้งค่าคีย์ที่ลูกค้าจัดการให้ใช้.

3. การแยกข้อมูลและถิ่นที่อยู่ของข้อมูล

3.1 การแยกผู้เช่า. ผู้เช่าแต่ละรายของลูกค้าจะได้รับอินสแตนซ์ฐานข้อมูลเฉพาะที่แยกเป็นอิสระ ข้อมูลลูกค้าจะไม่ถูกรวมปะปนกับข้อมูลของลูกค้ารายอื่นในระดับฐานข้อมูลโดยเด็ดขาด ข้อมูลเมตาที่ใช้ร่วมกัน (เช่น ระเบียบบัญญัติ การเรียกเก็บเงิน และการจับคู่ผู้เช่ากับผู้เช่า) จัดเก็บไว้ในฐานข้อมูลแบบหลายผู้เช่าแยกต่างหาก ซึ่งมีการควบคุมการเข้าถึงอย่างเข้มงวด ตารางที่ใช้ร่วมกันซึ่งกำหนดขอบเขตตามผู้เช่าและองค์กรยังได้รับการคุ้มครองเพิ่มเติมด้วยนโยบายความปลอดภัยระดับแถว (RLS) ของ PostgreSQL ซึ่งบังคับใช้ผ่านบริบทฐานข้อมูลที่กำหนดขอบเขตตามคำขอ.

3.2 ถิ่นที่อยู่ของข้อมูล. ข้อมูลลูกค้าทั้งหมด รวมถึงฐานข้อมูล การอัปโหลดไฟล์ ข้อมูลสำรอง และผลลัพธ์การสืบค้น จัดเก็บไว้เฉพาะในสหภาพยุโรป (แฟรงก์เฟิร์ต ประเทศเยอรมนี) ในกรณีที่มีการว่าจ้างผู้ประมวลผลช่วงซึ่งตั้งอยู่นอกเขตเศรษฐกิจยุโรป (EEA) สำหรับกิจกรรมการประมวลผลเฉพาะ (เช่น การประมวลผลโมเดล AI หรือการประมวลผลการชำระเงิน) การโอนข้อมูลจะอยู่ภายใต้กลไกการโอนข้อมูลที่เหมาะสมตามที่อธิบายไว้ในภาคผนวกการประมวลผลข้อมูล และผู้ประมวลผลช่วงกับสถานที่ประมวลผลของผู้ประมวลผลช่วงดังกล่าวจะระบุไว้ในรายชื่อผู้ประมวลผลช่วง.

3.3 การเก็บรักษาและการลบข้อมูล. กำหนดระยะเวลาการเก็บรักษาและการลบไว้ในข้อ 6 ของ [ภาคผนวกการประมวลผลข้อมูล](#) ลูกค้าสามารถลบข้อมูลของตนได้ทุกเมื่อผ่านแอปพลิเคชันหรือติดต่อ ProcessMind สำเนาข้อมูลสำรองจะถูกลบเมื่อพ้นระยะเวลาเก็บรักษาข้อมูลสำรองที่เกี่ยวข้อง (ข้อ 7.1).

4. การจัดการข้อมูลระบุตัวตนและการเข้าถึง

4.1 การยืนยันตัวตน. ProcessMind รองรับการลงชื่อเข้าใช้ครั้งเดียว (SSO) ผ่าน Microsoft Entra ID (Azure AD), Google OAuth 2.0/OIDC และ LinkedIn OAuth

2.0/OIDC ProcessMind ทำหน้าที่เป็นผู้พึ่งพาการยืนยันตัวตนและไม่จัดเก็บรหัสผ่านของผู้ใช้ การยืนยันตัวตนแบบหลายปัจจัยบังคับใช้โดยผู้ให้บริการข้อมูลระบุตัวตน ตัวอย่างเช่น เมื่อองค์กรเชื่อมต่อ Microsoft Entra ID (Azure AD) นโยบาย MFA และนโยบายการเข้าถึงขององค์กรนั้นเองจะมีผลบังคับใช้.

4.2 การจัดการเซสชัน. เซสชันของเบราว์เซอร์ใช้ JSON Web Tokens (JWT) ที่ลงนามแล้วและส่งผ่านคุกกี้ที่ปลอดภัยและมีคุณสมบัติ HttpOnly พร้อมแฟล็ก SameSite และ Secure ระบบจะตรวจสอบลายเซ็นของโทเค็นในทุกคำขอที่ผ่านการยืนยันตัวตน.

4.3 รูปแบบการอนุญาต ProcessMind ไม่พึ่งพา authorizer แบบเนทีฟของ API Gateway สำหรับ API หลักของแอปพลิเคชัน การอนุญาตบังคับใช้ผ่าน wrapper ของตัวจัดการ Lambda ที่ใช้ร่วมกัน ซึ่งตรวจสอบสถานะเซสชันและขอบเขตผู้เข้าก่อนเรียกใช้ตรรกะทางธุรกิจ มีการกำหนดเส้นทางสาธารณะที่อนุญาตไว้อย่างชัดเจนสำหรับขั้นตอนที่ไม่ต้องยืนยันตัวตน, webhook, การรับข้อมูลเหตุการณ์ และ CORS preflight ไปยังปลายทาง API ภายนอกใช้ตัวจัดการการยืนยันตัวตนเฉพาะ การเข้าถึงข้อมูลลูกค้าจำกัดอยู่ภายในบริบทผู้เช่าหรือองค์กรที่ผ่านการยืนยันตัวตนแล้ว

4.4 สิทธิ์เท่าที่จำเป็น. ระบบภายในปฏิบัติตามหลักสิทธิ์เท่าที่จำเป็น บทบาท IAM จำกัดขอบเขตไว้เฉพาะทรัพยากรขั้นต่ำที่จำเป็น ในกรณีที่เฟรมเวิร์กอนุญาตให้กำหนดขอบเขตได้อย่างแม่นยำ บทบาทบางรายการที่ SST/CDK สร้างขึ้นใช้ Managed Policy หรือนโยบายแบบ Inline ที่มีขอบเขตกว้างกว่าเพื่อรองรับการผูกทรัพยากรและการทำงานขณะรันไทม์ กรณีเหล่านี้ได้รับการทบทวน จำกัดขอบเขตตามทรัพยากรเมื่อทำได้ และติดตามในฐานะข้อบกพร่องที่ระบุไว้อย่างชัดเจน.

4.5 การควบคุมการเข้าถึงของพนักงาน. การเข้าถึงระบบภายในของพนักงานจัดการผ่าน Active Directory โดยใช้ SSO และบังคับใช้ MFA การควบคุมการเข้าถึงตามบทบาท (RBAC) ทำให้มั่นใจว่าการเข้าถึงข้อมูลลูกค้าจำกัดเฉพาะบุคลากรที่ได้รับอนุญาตและจำเป็นต้องทราบเท่านั้น มีการทบทวนสิทธิ์การเข้าถึงเป็นระยะ.

5. การบันทึก การตรวจสอบ และการตรวจประเมิน

5.1 การบันทึกข้อมูลจากส่วนกลาง. เปิดใช้งานการบันทึกการเข้าถึง HTTP API และ WebSocket โดยมีฟิลด์ JSON แบบมีโครงสร้าง และเขียนข้อมูลลงใน Amazon CloudWatch Logs โดยเก็บรักษาไว้หนึ่ง (1) ปี กลุ่มบันทึกการเข้าถึงดังกล่าวเข้ารหัสด้วยคีย์ AWS KMS ที่ลูกค้าจัดการ บันทึกของแอปพลิเคชันรวมไว้ในกลุ่มบันทึก Amazon

CloudWatch ที่เข้ารหัสด้วยคีย์ AWS KMS ที่ถูกค่าจัดการ และเก็บรักษาไว้สิบ (10) ปี กลุ่มบันทึกการตรวจประเมินและข้อมูลเทเลเมทรีแยกต่างหากก็เข้ารหัสด้วยคีย์ AWS KMS ที่ถูกค่าจัดการ และเก็บรักษาไว้สิบ (10) ปี กลุ่มบันทึกการส่งออกบันทึกของกลไก Aurora PostgreSQL เก็บรักษาไว้หนึ่ง (1) สัปดาห์.

5.2 ข้อมูลที่บันทึกและข้อมูลที่ไม่ได้บันทึก. ProcessMind บันทึกเหตุการณ์การเข้าถึง HTTP API และ WebSocket ได้แก่ เวลาที่ส่งคำขอ ตัวระบุคำขอ เส้นทางหรือพารามิเตอร์ สถานะการตอบกลับ และเวลาแฝง บันทึกการเข้าถึงจะไม่รวมที่อยู่ IP ต้นทางหรือ user agent ของผู้เรียก ProcessMind ยังบันทึกเหตุการณ์การยืนยันตัวตน เส้นทางความล้มเหลวแบบอะซิงโครนัส และกิจกรรมของแอปพลิเคชัน Lambda ที่เกี่ยวข้องลงในกลุ่มบันทึก CloudWatch จากส่วนกลางด้วย มีการเปิดใช้งานบันทึกการไหลของ VPC ปัจจุบัน ProcessMind ไม่ได้เปิดใช้งานการบันทึกการเข้าถึงมาตรฐานของ CloudFront บนการกระจายเว็บไซต์ SPA ส่วนหน้า หรือทรัพยากรสาธารณะ.

5.3 การตรวจสอบและการแจ้งเตือน. สัญญาณเตือนและแดชบอร์ดของ CloudWatch ใช้ตรวจสอบสถานะระบบ คิวจดหมายตีกลับ และความล้มเหลวที่เกี่ยวข้องกับความปลอดภัย ความล้มเหลวในการประมวลผลแบบอะซิงโครนัสจะถูกส่งไปยังคิวจดหมายตีกลับที่เข้ารหัส (เก็บรักษาไว้สิบสี่ (14) วัน และสอง (2) วันสำหรับคิวภาพขนาดย่อและดัชนีการค้นหา) และสัญญาณเตือน DLQ จะเรียกใช้การแจ้งเตือน SNS เพื่อให้ตรวจสอบ นอกจากนี้ ProcessMind ใช้ Sentry เพื่อติดตามข้อผิดพลาดส่วนหน้าแบบเรียลไทม์ ตรวจสอบประสิทธิภาพ และเล่นซ้ำเซสชัน ระบบจะบันทึกการเล่นซ้ำเซสชันเฉพาะเซสชันที่เกิดข้อผิดพลาด และจะปกปิดหรือบล็อกข้อความ ข้อมูลที่ป้อนในแบบฟอร์ม และสื่อในการเล่นซ้ำข้อมูล Sentry จะรับเข้ามาในสหภาพยุโรป (แฟรงก์เฟิร์ต) และจำกัดเฉพาะข้อมูลการใช้งาน ProcessMind (ข้อผิดพลาดของเบราว์เซอร์ ร่องรอยประสิทธิภาพ ข้อมูลเมตาของอุปกรณ์ และบันทึกการเล่นซ้ำที่ปกปิดข้อมูลแล้ว) Sentry ระบุไว้ใน[รายชื่อผู้ประมวลผลช่วง](#).

5.4 การคุ้มครองบันทึก. บันทึกจัดเก็บไว้ในกลุ่มบันทึก CloudWatch เฉพาะที่มีการควบคุมการเข้าถึง และเข้ารหัสขณะจัดเก็บ บันทึกของระบบใช้งานจริงและระบบพัฒนาแยกจากกันตามขอบเขตสภาพแวดล้อมและบัญชี.

6. การตรวจสอบความถูกต้องของการควบคุมโดยอัตโนมัติและการจัดการช่องโหว่

6.1 สิ่งที่ ProcessMind ดำเนินการ ProcessMind เรียกใช้ cdk-nag เป็นส่วนหนึ่งของเวิร์กโฟลว์การสังเคราะห์และการปรับใช้โครงสร้างพื้นฐาน โดยใช้ชุดกฎมาตรฐาน

อุตสาหกรรมหลายชุด (รวมถึง AWS Solutions, NIST 800-53 และ PCI DSS) มีการจัดทำรายงานแยกตามสแต็กและทบทวนเป็นส่วนหนึ่งของการจัดการการเปลี่ยนแปลงโครงสร้างพื้นฐาน โดยจัดประเภทข้อค้นพบเป็นแก้ไขแล้ว ยอมรับความเสี่ยง หรือวางแผนปรับปรุง.

6.2 วิธีจัดการข้อบกพร่อง มีการบันทึกการระงับการแจ้งเตือนไว้ในทะเบียนส่วนกลางในกรณีที่เฟรมเวิร์กกรองรับ โดยจำกัดขอบเขตเฉพาะสแต็กที่ได้รับผลกระทบและต้องมีเหตุผลเป็นลายลักษณ์อักษร หากสแต็กมีการระงับแบบ Inline จะมีการบันทึกไว้ควบคู่กับสแต็กนั้นเมื่อแก้ไขข้อค้นพบแล้ว จะปรับปรุงหรือนำการระงับที่เกี่ยวข้องออก ProcessMind ไม่ถือว่าการระงับเป็นการยกเว้นการทบทวนทั้งหมด.

6.3 สิ่งที่ ProcessMind ยังไม่ได้ดำเนินการในปัจจุบัน ProcessMind ติดตามและทบทวนข้อบกพร่องที่มีสาระสำคัญเกี่ยวกับการควบคุมโครงสร้างพื้นฐาน ข้อหลักมีดังนี้:

- โดยค่าเริ่มต้น Lambda ของแอปพลิเคชันจะไม่อยู่ใน VPC แต่จะเชื่อมต่อกับ Aurora ผ่าน RDS Data API โดยใช้ TLS พร้อมการยืนยันตัวตนด้วย IAM และ Secrets Manager
- ไม่มีส่วนใดของบริการที่ได้รับการปกป้องโดย AWS WAF: AWS WAF ไม่รองรับ API Gateway HTTP APIs และจุดเชื่อมต่อที่เหลือก็ไม่ได้รับการปกป้องด้วย WAF เช่นกัน (การเชื่อมต่อ WebSocket ใช้โทเค็น HMAC ที่มีอายุสั้น ส่วนข้อจำกัดทางภูมิศาสตร์ที่เกี่ยวข้องกับการชำระเงินบังคับใช้ในระบบการชำระเงิน); การกระจายเนื้อหาแบบคงที่ยังไม่มีการบันทึกการเข้าถึงมาตรฐานของ CloudFront
- การกู้คืนฐานข้อมูลอาศัยการสำรองข้อมูลอัตโนมัติของ Aurora และการกู้คืน ณ เวลาใดเวลาหนึ่ง แทนแผน AWS Backup แยกต่างหากหรือ Aurora Enhanced Monitoring
- ไม่มีการจำลองข้อมูล S3 ข้ามภูมิภาคหรือ S3 Object Lock สำหรับบังคับที่แก้ไขได้
- ทรัพยากรสนับสนุนบางรายการที่จัดการโดย AWS/CDK/SST ใช้การเข้ารหัสที่ AWS จัดการหรือนโยบาย IAM ที่สร้างขึ้นซึ่งมีขอบเขตกว้างกว่า ในกรณีที่บริการไม่มีทางเลือกอื่นที่ลูกค้าควบคุมได้

ทะเบียนการระงับการแจ้งเตือนฉบับสมบูรณ์ได้รับการดูแลควบคู่กับโค้ดโครงสร้างพื้นฐาน และสามารถขอรับได้ การใช้ชุดกฎ cdk-nag เป็นการตรวจสอบความถูกต้องของการควบคุมทางวิศวกรรม ไม่ใช้การรับรองจากภายนอก ความเห็นจากการตรวจประเมิน หรือการรับรองทางกฎหมายเกี่ยวกับการปฏิบัติตาม HIPAA, NIST หรือ PCI DSS.

6.4 การจัดการการพึ่งพาซอฟต์แวร์. มีการตรวจสอบการพึ่งพาซอฟต์แวร์อย่างต่อเนื่องเพื่อค้นหาช่องโหว่ที่ทราบแล้ว ช่องโหว่ระดับวิกฤตและระดับสูงจะได้รับการแก้ไขโดยมีเป้าหมายภายในเจ็ด (7) วัน และมีการปรับปรุงการพึ่งพาซอฟต์แวร์ตามรอบอย่างสม่ำเสมอ.

6.5 วงจรการพัฒนาซอฟต์แวร์ที่ปลอดภัย (SDLC). ProcessMind ใช้แนวทางการป้องกันเชิงลึกในการพัฒนาซอฟต์แวร์ การเปลี่ยนแปลงทุกครั้งที่จะนำไปใช้ในระบบใช้งานจริงต้องผ่านขั้นตอนการตรวจสอบความถูกต้องอัตโนมัติที่เป็นอิสระหลายชั้นก่อนการปรับใช้:

- **การวิเคราะห์แบบสถิตและความปลอดภัยของชนิดข้อมูล:** โหมดเข้มงวดของ TypeScript และ ESLint บังคับใช้ความถูกต้องของชนิดข้อมูล ความปลอดภัยจากค่า null และรูปแบบการเขียนโค้ดที่เกี่ยวข้องกับความปลอดภัยในเวลาคอมไพล์
- **การตรวจทานโค้ดโดยใช้ AI ช่วย:** การวิเคราะห์โดยใช้ AI ช่วยให้มุมมองเพิ่มเติมในการตรวจทาน pull request เพื่อระบุความเสี่ยงด้านความปลอดภัย ข้อผิดพลาดทางตรรกะ และการเบี่ยงเบนจากแนวปฏิบัติ โดยเป็นส่วนเสริมของการทดสอบอัตโนมัติ
- **การทดสอบหน่วยและการทดสอบการผสานรวม:** ชุดทดสอบ Vitest ที่ครอบคลุมตรวจสอบตรรกะทางธุรกิจ รูปแบบการเข้าถึงข้อมูล ลักษณะการทำงานของ API และการจัดการข้อผิดพลาดกับทรัพยากร AWS จริงในสภาพแวดล้อมการพัฒนา
- **การทดสอบตั้งแต่ต้นจนจบ:** การทดสอบเบราว์เซอร์ที่ใช้ Playwright ตรวจสอบเวิร์กโฟลว์สำคัญของผู้ใช้ รวมถึงการยืนยันตัวตน การอัปโหลดข้อมูล การสร้างแบบจำลองกระบวนการ การจำลอง และการแยกผู้เช่าหลายราย
- **การสแกนการปฏิบัติตามข้อกำหนดของโครงสร้างพื้นฐาน:** cdk-nag ตรวจสอบโครงสร้างพื้นฐานในรูปแบบโค้ดตามกรอบการปฏิบัติตามข้อกำหนดหลายกรอบ ทุกครั้งที่มีการเปลี่ยนแปลง
- **การสแกนช่องโหว่ของการพึ่งพาซอฟต์แวร์:** การตรวจสอบการพึ่งพาซอฟต์แวร์โดยอัตโนมัติจะบล็อกไม่ให้ช่องโหว่ระดับวิกฤตและระดับสูงที่ทราบแล้วเข้าสู่ระบบใช้งานจริง.

การตรวจทานโดยมนุษย์มุ่งเน้นที่สถาปัตยกรรม ขอบเขตด้านความปลอดภัย และการตัดสินใจในระดับการออกแบบ มากกว่าการตรวจสอบโค้ดที่ละบรรทัด ในกรณีที่เกี่ยวข้องกับการเปลี่ยนแปลงเชิงโครงสร้าง การเปลี่ยนแปลงที่มีความอ่อนไหวด้านความปลอดภัย หรือการเปลี่ยนแปลงโครงสร้างพื้นฐาน ต้องได้รับการอนุมัติโดยชัดเจนจากมนุษย์เพิ่มเติมจากการตรวจสอบความถูกต้องโดยอัตโนมัติ.

มีการบังคับใช้ขั้นตอนการตรวจสอบความถูกต้องทั้งหมดผ่าน CI ในฐานะเงื่อนไขบังคับก่อนการผสานการเปลี่ยนแปลงแอปพลิเคชันและโครงสร้างพื้นฐานเข้าสู่สาขาหลัก เนื้อหาเว็บไซต์และการเผยแพร่ทรัพยากรแบบคงที่เป็นไปตามกระบวนการเผยแพร่แยกต่างหากที่มีการจัดทำเป็นเอกสาร พร้อมการตรวจสอบขณะปรับใช้ ซึ่งรวมถึงการตรวจสอบโดยอัตโนมัติว่าเอกสารทางกฎหมายเป็นฉบับปัจจุบัน แทนการใช้เงื่อนไข CI ของแอปพลิเคชัน การแก้ไขฉุกเฉินในระบบใช้งานจริงอาจข้ามเงื่อนไข CI ได้ แต่ต้องดำเนินการเรียกใช้ไปป์ไลน์ทั้งหมดและทบทวนหลังเกิดเหตุภายในสี่สิบสี่ (24) ชั่วโมง.

7. การสำรองข้อมูลและการกู้คืนจากภัยพิบัติ

7.1 การสำรองข้อมูลอัตโนมัติ. Amazon Aurora ดำเนินการสำรองข้อมูลอย่างต่อเนื่องและโดยอัตโนมัติ โดยมีระยะเวลาเก็บรักษาเจ็ด (7) วัน ข้อมูลสำรองเข้ารหัสโดยใช้คีย์ KMS ที่ลูกค้าจัดการชุดเดียวกับฐานข้อมูลต้นทาง.

7.2 การกู้คืน ณ เวลาใดเวลาหนึ่ง. Aurora รองรับการกู้คืน ณ เวลาใดเวลาหนึ่งภายในช่วงเวลาเก็บรักษาข้อมูลสำรองได้ทุกวัน ทำให้สามารถกู้คืนได้อย่างรวดเร็วในกรณีข้อมูลเสียหายหรือถูกลบโดยไม่ตั้งใจ.

7.3 ความคงทนและการกำหนดเวอร์ชันของ S3. การอัปโหลดไฟล์และสิ่งประดิษฐ์ที่ใช้ในการปฏิบัติงานจัดเก็บไว้ใน Amazon S3 ซึ่งมีความคงทน 99.99999999% (11 nines) เปิดใช้งานการกำหนดเวอร์ชันในบัคเก็ตสำหรับการอัปโหลดและบัคเก็ตทรัพยากรเพื่อรองรับการกู้คืนและการย้อนกลับ บัคเก็ตสำหรับการปรับใช้เว็บไซต์และส่วนหน้าเป็นสิ่งประดิษฐ์จากการสร้างที่ทำซ้ำได้ และไม่ได้ถือเป็นระบบสำรองข้อมูล ปัจจุบัน ProcessMind ไม่ได้เปิดใช้งานการทำสำเนาข้อมูล S3 ข้าม Region.

7.4 ความต่อเนื่องทางธุรกิจ. มีการจัดทำเอกสารและทดสอบขั้นตอนการกู้คืนจากภัยพิบัติเป็นระยะ ดูเอกสารสรุปได้ในเอกสาร[การกู้คืนจากภัยพิบัติ ความต่อเนื่องทางธุรกิจ และ การตอบสนองต่อเหตุขัดข้อง](#) สถาปัตยกรรมอาศัยบริการที่ AWS จัดการภายใน Region eu-central-1 ซึ่ง AWS ดำเนินงานครอบคลุม Availability Zone หลายแห่ง ปัจจุบันคลัสเตอร์ Aurora ทำงานด้วยอินสแตนซ์ผู้เขียนเพียงหนึ่งอินสแตนซ์ ดังนั้นการกู้คืนฐานข้อมูลจึงอาศัยการสำรองข้อมูลอัตโนมัติและการกู้คืน ณ เวลาใดเวลาหนึ่ง แทนการมีอินสแตนซ์สำรองภายใน Region ข้อมูลสำรองของ Aurora ความคงทนของ S3 คิวจดหมายตีกลับ และทรัพยากรแบบคงที่ที่สร้างใหม่จากซอร์ส เป็นส่วนหนึ่งของกลยุทธ์การกู้คืน.

8. การตอบสนองต่อเหตุขัดข้อง

8.1 การแจ้งเหตุขัดข้อง. ในกรณีที่เกิดเหตุการณ์ด้านความปลอดภัย (ตามที่นิยามไว้ใน DPA) ProcessMind จะแจ้งลูกค้าที่ได้รับผลกระทบโดยไม่ชักช้าเกินควร และหากสามารถทำได้ จะแจ้งภายในเจ็ดสิบสอง (72) ชั่วโมงนับจากเวลาที่ทราบถึงเหตุการณ์.

8.2 การจัดการเหตุขัดข้อง. ProcessMind มีขั้นตอนการตอบสนองต่อเหตุขัดข้องที่จัดทำเป็นเอกสาร ครอบคลุมการระบุเหตุ การควบคุม การกำจัด การกู้คืน และการทบทวนหลังเหตุขัดข้อง ดูเอกสารสรุปได้ในเอกสาร [การกู้คืนจากภัยพิบัติ ความต่อเนื่องทางธุรกิจ และการตอบสนองต่อเหตุขัดข้อง](#) มีการนำบทเรียนที่ได้รับจากเหตุขัดข้องมาปรับใช้กับการควบคุมและกระบวนการด้านความปลอดภัย.

8.3 การสื่อสาร. การแจ้งเหตุขัดข้องประกอบด้วยลักษณะและขอบเขตของเหตุการณ์ ประเภทข้อมูลที่ได้รับผลกระทบ มาตรการที่ดำเนินการเพื่อควบคุมเหตุการณ์ และการดำเนินการที่แนะนำสำหรับลูกค้า.

9. มาตรการด้านองค์กร

9.1 การจัดการความมั่นคงปลอดภัยสารสนเทศ. ProcessMind ดูแลระบบการจัดการความมั่นคงปลอดภัยสารสนเทศที่สอดคล้องกับหลักการ ISO 27001 ProcessMind ได้เลือกแนวทางการรับรองสำหรับการรับรอง ISO 27001 และการรับรอง SOC 2 Type II แล้ว แต่ยังไม่ได้เริ่มกระบวนการรับรองอย่างเป็นทางการ.

9.2 การสร้างความตระหนักรู้ด้านความปลอดภัย. บุคลากรทุกคนที่เข้าถึงข้อมูลลูกค้าจะได้รับการฝึกอบรมเพื่อสร้างความตระหนักรู้ด้านความปลอดภัย แนวปฏิบัติที่ดีที่สุดด้านความปลอดภัยถูกผนวกไว้ในการปฐมนิเทศ เวิร์กโฟลว์การพัฒนา และขั้นตอนการปฏิบัติงาน.

9.3 การจัดการผู้ขายและผู้ประมวลผลช่วง. ผู้ประมวลผลช่วงมีข้อผูกพันตามสัญญาให้ปฏิบัติตามมาตรฐานการคุ้มครองข้อมูลที่เทียบเท่ากับมาตรฐานที่อธิบายไว้ในเอกสารฉบับนี้ ProcessMind ดู [รายชื่อผู้ประมวลผลช่วง](#) ที่เปิดเผยต่อสาธารณะ และแจ้งล่วงหน้าอย่างน้อยสามสิบ (30) วันก่อนว่าจ้างผู้ประมวลผลช่วงรายใหม่ มีการทบทวนการปฏิบัติตามข้อกำหนดของผู้ประมวลผลช่วงเป็นประจำทุกปี.

9.4 การรักษาความลับ. บุคลากรทุกคนที่ได้รับอนุญาตให้ประมวลผลข้อมูลลูกค้ามีข้อผูกพันในการรักษาความลับเป็นลายลักษณ์อักษร.

10. การปฏิบัติตามข้อกำหนดและการรับรอง

กรอบ/มาตรฐาน	สถานะ
GDPR (กฎระเบียบคุ้มครองข้อมูลทั่วไปของสหภาพยุโรป)	ปฏิบัติตามแล้ว
ถิ่นที่อยู่ของข้อมูลในสหภาพยุโรป (แฟรงก์เฟิร์ต ประเทศเยอรมนี)	บังคับใช้แล้ว
การรับรองโครงสร้างพื้นฐาน AWS (ISO 27001, SOC 2, PCI DSS)	ได้รับประโยชน์จาก AWS
ISO 27001 (ProcessMind)	วางแผนไว้ — เลือกแนวทางการรับรองแล้ว แต่ยังไม่ได้เริ่มกระบวนการอย่างเป็นทางการ
SOC 2 Type II (ProcessMind)	วางแผนไว้ — เลือกแนวทางการรับรองแล้ว แต่ยังไม่ได้เริ่มกระบวนการอย่างเป็นทางการ
การตรวจสอบความถูกต้องของการควบคุมโครงสร้างพื้นฐานโดยอัตโนมัติ (cdk-nag ครอบคลุม AWS Solutions, HIPAA Security, NIST 800-53 R4/R5, PCI DSS 3.2.1, Serverless)	นำมาใช้เป็นการตรวจสอบความถูกต้องของการควบคุมทางวิศวกรรม ไม่ใช้การรับรอง
ข้อสัญญามาตรฐาน (SCCs) สำหรับการโอนข้อมูลระหว่างประเทศ	นำมาใช้แล้ว (ดู DPA)
ภาคผนวกการประมวลผลข้อมูล (DPA)	เปิดเผยต่อสาธารณะ

การใช้ชุดกฎ cdk-nag ไม่ได้หมายความว่า ProcessMind ได้รับการรับรองอย่างเป็นทางการหรือผ่านการตรวจประเมินโดยอิสระตาม HIPAA, NIST หรือ PCI DSS ชุดกฎดังกล่าวใช้เป็นแนวทางควบคุมทางวิศวกรรมเพื่อตรวจสอบการออกแบบโครงสร้างพื้นฐานและติดตามช่องว่างอย่างชัดเจน.

หากมีคำถามเกี่ยวกับความปลอดภัย การปฏิบัติตามข้อกำหนด หรือต้องการขอเอกสาร
เช่น รายงานการตรวจประเมินหรือแบบสอบถามด้านความปลอดภัยที่กรอกแล้ว โปรด
ติดต่อ support@processmind.com.