IRON MOUNTAIN®

สมุดปกขาว

ความปลอดภัยของแพลตฟอร์ม Iron Mountain InSight®

บทสรุปผู้บริหาร

เกี่ยวกับความปลอดภัยของ Iron Mountain

Iron Mountain รวมวิธีการรักษาความปลอดภัยเชิงลึกที่ครอบคลุมการนำเข้าเนื้อหา การจัดเก็บ และการประมวลผลเอกสารดิจิทัล ร่วมกับการโฮสต์ในศูนย์ข้อมูลที่ปลอดภัย Iron Mountain ได้นำกรอบมาตรฐานสากลด้านความปลอดภัยทางไซเบอร์ (Cyber Security Framework - CSF) ของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (National Institute of Standards and Technology - NIST) มาประยุกต์ใช้เป็นกรอบความคิดด้านความปลอดภัยขององค์กร เราให้บริการการปรับใช้ที่ปลอดภัย การจัดเก็บข้อมูลพร้อมการปกป้องความเป็นส่วนตัวของผู้ใช้ การสื่อสารระหว่างบริการ และการสนับสนุนด้านการบริหารจัดการระบบโดยแยกหน้าที่ออกจากกัน

การฝึกอบรม

Iron Mountain ทำงานร่วมกับอุตสาหกรรมที่มีการควบคุมอย่างเข้มงวดซึ่งต้องการการฝึกอบรมด้านความปลอดภัยและความเป็นส่วนตัวของพนักงานพนักงานจะเข้าร่วมหลักสูตรและการฝึกอบรมด้านความปลอดภัยต่างๆ ที่พัฒนาตลอดปีตามเป้าประสงค์จากโปรแกรมการฝึกอบรมทั่วทั้งองค์กรของเราการฝึกอบรมจะประกอบด้วยความตระหนักด้านความปลอดภัยประจำปี การฝึกอบรมด้านความเป็นส่วนตัวของข้อมูล การฝึกอบรมเกี่ยวกับรหัสรักษาความปลอดภัย หลักจรรยาบรรณ และจริยธรรมทางธุรกิจเราทำงานร่วมกับลูกค้าเพื่อให้บุคลากรได้รับการตรวจสอบประวัติอย่างเหมาะสมการจ้างงานของเราขึ้นอยู่กับการตรวจสอบภูมิหลังตามข้อกำหนดต่างๆ ในท้องถิ่นและของลูกค้า

ผลิตภัณฑ์ Iron Mountain InSight

I. โปรแกรมการปฏิบัติตามข้อกำหนด

Iron Mountain InSight ได้สร้างโปรแกรมการปฏิบัติตามข้อกำหนดในวงกว้างและเฉพาะเจาะจงซึ่งปรับให้เหมาะสมตามอุตสาหกรรมและความต้องการของลูกค้าตามกฎระเบียบซึ่งรวมไปถึงการปฏิบัติตามข้อกำหนดด้านความปลอดภัยและความเป็นส่วนตัวของข้อมูล

การรับรองการปฏิบัติตามข้อกำหนด

- ISO-27001 - InSight ได้รับการรับรองมาอย่างต่อเนื่องนับตั้งแต่ปี 2020นี่คือมาตรฐานสากลที่ช่วยให้องค์กรจัดการด้านความปลอดภัยของสินทรัพย์ข้อมูลได้โดยจัดให้มีเฟรมเวิร์กการจัดการสำหรับการนำระบบการจัดการความปลอดภัยของข้อมูล (ISMS) มาใช้เพื่อรับประกันการรักษาความลับความครบถ้วน และความพร้อมของข้อมูลทั้งหมด

- SOC2 Type 2 - Iron Mountain ยังคงรักษาการรับรอง SOC2 Type 2 สำหรับ InSight ไว้ได้นับตั้งแต่ปี 2020รายงาน SOC2 Type 2 คือการตรวจสอบการควบคุมระบบและองค์กร (Service Organization Control - SOC) เกี่ยวกับวิธีที่ผู้ให้บริการบนระบบคลาวด์จัดการกับข้อมูลที่อ่อนไหว

การปฏิบัติตามข้อกำหนดของอุตสาหกรรม

- InSight มีประสิทธิภาพตาม 21 CFR Part 11
- StateRAMP - ได้รับสถานะพร้อมในเดือนมกราคม 2024
- FedRAMP (NIST 800-53/37) - การทดสอบโดยบุคคลที่สามดำเนินการกับส่วนควบคุม NIST 800-53 Revision 4 และข้อกำหนด FedRAMP เพิ่มเติมInSight ได้รับการรับรองเพื่อดำเนินงาน (Authorizations to Operate - ATO) ของ FedRAMP และสถานะพร้อมของ FedRAMP

ความเป็นส่วนตัวของข้อมูล

- กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (General Data Protection Regulation - GDPR) - InSight ได้ผ่านการประเมิน GDPR และมีสำเนารายงานให้ตามคำขอ
- กฎหมายว่าด้วยการเคลื่อนย้ายและความรับผิดชอบในการประกันสุขภาพ (Health Insurance Portability and Accountability Act - HIPAA) - InSight เป็นไปตามมาตรฐาน HIPAA และได้ใช้มาตรการความเป็นส่วนตัวและความปลอดภัยเพื่อปกป้องความเป็นส่วนตัวรวมไปถึงความปลอดภัยของข้อมูลที่ระบุตัวบุคคลได้ (Personally Identifiable Information - PII)

II. ภาพรวมความปลอดภัยในการปฏิบัติงาน

การจัดการข้อมูลระบุตัวตนและการเข้าถึง

- เราปรับใช้และบังคับใช้การควบคุมการเข้าถึงตามบทบาทเพื่อผู้ใช้ที่ได้รับสิทธิพิเศษซึ่งมีการจำกัดการใช้และการจัดสรรการยืนยันตัวตนโดยใช้หลายปัจจัย (Multi-factor authentication - MFA) เป็นสิ่งจำเป็นเพื่อให้การเข้าถึงถูกจำกัดไว้เฉพาะผู้ใช้ที่ได้รับการรับรองความถูกต้องเท่านั้นสิทธิ์ขั้นต่ำถูกนำมาใช้สำหรับผู้ใช้และกระบวนการที่ได้รับอนุญาต

การตรวจสอบ

- การสแกนเพื่อความปลอดภัย - สภาพแวดล้อมของ InSight ประกอบด้วยระบบการตรวจสอบที่สแกนภาพบรรจุภัณฑ์และระบบ รวมไปถึงตรวจจับช่องโหว่
- การทดสอบความปลอดภัยของแอปพลิเคชัน - InSight ดำเนินการทดสอบความปลอดภัยของแอปพลิเคชันแบบคงที่ (Static application security testing - SAST) การทดสอบความปลอดภัยของแอปพลิเคชันแบบไดนามิก (Dynamic Application Security Testing - DAST) และการทดสอบการเจาะระบบที่ดำเนินการด้วยตนเอง
- การตรวจสอบระบบและบันทึกการตรวจสอบ - InSight ประกอบด้วยระบบ Security Information And Event Management (SIEM) สำหรับการจัดการบันทึก การตรวจสอบเหตุการณ์ด้านความปลอดภัย ความสัมพันธ์และการแจ้งเตือนเหตุการณ์ด้านความปลอดภัย รวมไปถึงบันทึกการตรวจสอบ
- การรับมือต่อเหตุการณ์ - ทีมรับมือกับเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Incident And Response Team - CIRT) ของเรารับผิดชอบต่อการจำแนกเหตุการณ์การตรวจสอบที่น่าสนใจเป็นพิเศษสำหรับระบบข้อมูลของ Iron Mountain InSight และสำหรับการดำเนินการตรวจสอบและวิเคราะห์บันทึกการตรวจสอบ
- การจัดการเหตุการณ์ - ทีมรับมือกับเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Incident And Response Team - CIRT) ของเรารับผิดชอบต่อการระบุ ปกป้อง ตรวจจับ ตอบสนอง และกู้คืนแบบเรียลไทม์เพื่อรวมการบันทึกแบบครบวงจรและการตรวจสอบผลิตภัณฑ์และโครงสร้างพื้นฐานของเราอีกทั้งเรายังรักษาความตระหนักรู้ของพนักงานและโปรแกรมการฝึกอบรมเพื่อรวมนโยบายและขั้นตอนการรักษาความปลอดภัยของข้อมูลภายใน

ความต่อเนื่องทางธุรกิจ

- ระยะเวลาเป้าหมายเวลาในการกู้คืน (Recovery Time Objective - RTO) ของ InSight สำหรับแอปพลิเคชันทางธุรกิจระดับเทียร์ 1 อยู่ระหว่าง 10 - 24 ชั่วโมง และจุดเป้าหมายเวลาที่ข้อมูลจะได้รับการกู้คืน (Recovery Point Objective - RPO) ได้รับการประเมินไว้ที่ 1 ชั่วโมงในการทดสอบแผนดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan - BCP) ล่าสุดของเราที่ดำเนินการในไตรมาสที่ 4 ของปี 2023RTO/RPO สามารถปรับเปลี่ยนได้ตามความต้องการของลูกค้า

การกู้คืนจากความเสียหาย

- การทดสอบการกู้คืนจากความเสียหายของ InSight ได้รับการออกแบบมาเพื่อให้เราทำการกู้คืนได้อย่างมีประสิทธิภาพไม่ว่าจะเป็นวัตถุ ฐานข้อมูล และดัชนีจากการลบหรืออัปเดตโดยไม่ตั้งใจ เนื่องจากสิ่งเหล่านี้เป็นแหล่งที่มาของข้อมูลถาวรสำหรับแอปพลิเคชัน InSight ภายใน RTO/RPO ที่กำหนดตามเอกสารในแผนการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan - BCP) ของเรา

การวางแผนกำลังการผลิต

- การวางแผนกำลังการผลิตของเรามุ่งเน้นไปที่การตรวจสอบประสิทธิภาพของภาระงานและช่วยให้กำลังผลิตตรงตามความต้องการในปัจจุบันและอนาคตซึ่งจะรวมไปถึงประสิทธิภาพในการตรวจวัดและการตรวจสอบเพื่อที่เราจะไม่ทำเกินขีดจำกัดของกำลังการผลิต

การบริหารจัดการความเสี่ยงและแก้ไขช่องโหว่

- การบริหารจัดการความเสี่ยงและแก้ไขช่องโหว่ ป้องกันมัลแวร์ การเข้ารหัสดิสก์ปลายทาง และการป้องกันการบุกรุกจะได้รับการจัดการด้วยสินทรัพย์เทคโนโลยีสารสนเทศและแนวทางการจัดการปลายทาง

การเข้ารหัส

- ข้อมูลทั้งหมดจะได้รับการเข้ารหัสแบบระหว่างการส่งผ่านและที่อยู่นิ่งตามมาตรฐานการประมวลผลข้อมูลของรัฐบาลกลาง (Federal Information Processing Standards - FIPS 140-2) โดยใช้มาตรฐานอุตสาหกรรม เช่น มาตรฐานการเข้ารหัสขั้นสูง (Advanced Encryption Standard - AES) 256 และคีย์จัดการบริการ

III. ความเป็นส่วนตัวของข้อมูล

ที่อยู่ของข้อมูล

- ที่อยู่ของข้อมูลเพื่อช่วยปฏิบัติตามข้อกำหนดด้านที่อยู่ของข้อมูล InSight มีความสามารถในการควบคุมที่จัดเก็บข้อมูล รวมไปถึงสามารถปรับแต่งและจำกัดการจัดเก็บข้อมูลในบางภูมิภาค

การคุ้มครองข้อมูล

- InSight มีการใช้เทคนิคที่เหมาะสม มาตรการเชิงองค์กรและการบริหารจัดการ รวมไปถึงการเข้ารหัสและการยืนยันตัวตนโดยใช้หลายปัจจัย (MFA) เพื่อให้ข้อมูลของลูกค้ามีความปลอดภัยอยู่เสมอInSight สามารถปรับใช้ไฟร์วอลล์แอปพลิเคชันเว็บ (Web Application Firewall - WAF) ตามคำขอของลูกค้าได้

การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data protection impact assessments - DPIAs)

- Iron Mountain จัดการข้อมูลส่วนบุคคลและข้อมูลที่สามารถระบุตัวบุคคลได้ในนามของผู้อื่นในฐานะผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล Iron Mountain สามารถจัดการหรือประมวลผลข้อมูลของลูกค้าได้โดยไม่ได้รับแจ้งถึงเนื้อหาหรือที่มาของข้อมูลที่แท้จริง
- เมื่อเราทำหน้าที่เป็นผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลจากเขตเศรษฐกิจยุโรป (European Economic Area - EEA) และสวิตเซอร์แลนด์ (หรือเข้าถึงข้อมูลจากสหรัฐอเมริกาใน EEA หรือสวิตเซอร์แลนด์) ข้อมูลจะได้รับการประมวลผลตามหลักการคุ้มครองความเป็นส่วนตัวที่เกี่ยวข้อง
- เราดำเนินการประเมินผลด้านการคุ้มครองข้อมูลส่วนบุคคล (Data protection impact assessments - DPIAs) เป็นระยะตามที่ได้รับคำสั่งที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล

หมายเหตุ: โปรดดูคำแถลงนโยบายความเป็นส่วนตัวของ Iron Mountain สำหรับข้อมูลเกี่ยวกับประเภทของข้อมูลส่วนบุคคลและวัตถุประสงค์ในการถ่ายโอนและประมวลผลข้อมูลดังกล่าว รวมถึงบุคคลที่สามที่อาจแบ่งปันข้อมูลดังกล่าวด้วย

Elevate the power of your work

เป็นเวลากว่า 70 ปีมาแล้วที่ Iron Mountain เป็นพาร์ทเนอร์เชิงกลยุทธ์ของคุณในการให้ความดูแลข้อมูลและสินทรัพย์เป็นผู้นำระดับโลกด้านบริการจัดเก็บและจัดการข้อมูลและได้รับความไว้วางใจจากองค์กรมากกว่า 225,000 แห่งทั่วโลก ซึ่งรวมถึงกว่า 90% ของบริษัทต่างๆ ใน Fortune 1000 เราจะปกป้อง ปลดล็อก และขยายคุณค่าของงานของคุณ ไม่ว่าจะเป็นอะไร ไม่ว่าจะอยู่ที่ไหน หรือเก็บไว้อย่างไร

IRON MOUNTAIN®

+662 407 3333 | ironmountain.com/th-th

เกี่ยวกับ Iron Mountain

Iron Mountain Incorporated (NYSE: IRM) ก่อตั้งขึ้นในปี 1951 เป็นผู้นำระดับโลกด้านบริการพื้นที่จัดเก็บข้อมูลและการจัดการข้อมูล ได้รับความไว้วางใจจากองค์กรกว่า 225,000 แห่งทั่วโลก และด้วยเครือข่ายอสังหาริมทรัพย์ที่มีพื้นที่มากกว่า 9.1 ล้านตารางเมตรในอาคารกว่า 1,400 แห่งในกว่า 60 ประเทศ Iron Mountain จัดเก็บและปกป้องสินทรัพย์ข้อมูลนับพันล้านรายการ รวมถึงข้อมูลทางธุรกิจที่สำคัญ ข้อมูลที่มีความละเอียดอ่อนสูง และสิ่งประดิษฐ์ทางวัฒนธรรมและประวัติศาสตร์ Iron Mountain ช่วยให้องค์กรสามารถลดค่าใช้จ่ายและความเสี่ยง ปฏิบัติตามกฎระเบียบ กู้คืนจากความเสียหาย และเปิดใช้งานวิธีการทำงานแบบดิจิตอลมากขึ้นด้วยโซลูชันที่ประกอบด้วยพื้นที่จัดเก็บข้อมูลที่ปลอดภัย การจัดการข้อมูล การเปลี่ยนผ่านสู่ระบบดิจิตอล การทำลายที่ปลอดภัย รวมถึงศูนย์ข้อมูล การจัดเก็บงานศิลปะและโลจิสติกส์ รวมทั้งบริการคลาวด์ ไปที่ www.ironmountain.com/th-th เพื่อดูข้อมูลเพิ่มเติม