IRON MOUNTAIN®

กระดาษสีขาว

ภาพรวมการรักษาความปลอดภัย Iron Mountain InSight

ภาพรวมการรักษาความปลอดภัย Iron Mountain InSight

บทสรุปผู้บริหาร

การรักษาความปลอดภัยเป็นสิ่งที่ลูกค้าของเราให้ความสำคัญเป็นอันดับแรก ลูกค้าของเราต้องการโซลูชันที่พิสูจน์แล้วว่าจะปกป้องพวกเขาและลูกค้าของพวกเขาจากแฮกเกอร์ มัลแวร์ และการดำเนินการที่ไม่ปลอดภัย นอกจากนี้ยังต้องการโซลูชันที่จะขยายแนวทางปฏิบัติด้านความปลอดภัยในปัจจุบันเพื่อให้ตรงตามข้อปฏิบัติและข้อกำหนดการรับรองที่สำคัญ และให้การควบคุมการเข้าถึงของผู้ใช้อย่างละเอียด รวมถึงเข้าถึงความสามารถในการตรวจสอบและติดตามที่ใช้งานง่าย

Iron Mountain InSight® มีกลยุทธ์การรักษาความปลอดภัยแบบครบวงจรที่ครอบคลุมการนำเข้าเนื้อหาลงในที่จัดเก็บเอกสารดิจิตอลและเมตาดาต้า Iron Mountain ได้นำกรอบมาตรฐานสากลด้านความปลอดภัยทางไซเบอร์ (Cyber Security Framework, CSF) ของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (National Institute of Standards and Technology, NIST) มาประยุกต์ใช้เป็นกรอบความคิดด้านความปลอดภัยขององค์กร

เราให้บริการการปรับใช้ที่ปลอดภัย การจัดเก็บข้อมูลพร้อมการปกป้องความเป็นส่วนตัวของผู้ใช้ การสื่อสารระหว่างบริการและการสนับสนุนด้านการบริหารจัดการระบบโดยแยกหน้าที่ออกจากกัน

โครงสร้างพื้นฐานได้ออกแบบมาในระดับที่มีความก้าวหน้า โดยเริ่มจากการรักษาความปลอดภัยทางกายภาพของศูนย์ข้อมูลโฮสต์ ต่อด้วยการรักษาความปลอดภัยของฮาร์ดแวร์และซอฟต์แวร์ที่สนับสนุนโครงสร้างพื้นฐาน และสุดท้าย ข้อจำกัดทางเทคนิคและกระบวนการที่สนับสนุนความปลอดภัยในการปฏิบัติงานตามข้อกำหนด (ISO 27001 และ SOC 2 Type II)

ภาพรวมของการรักษาความปลอดภัยของ Iron Mountain

แนวทางปฏิบัติด้านความปลอดภัยของเราถูกกำหนดโดยมาตรฐานระดับสูงขององค์กรและขับเคลื่อนโดยทีมธุรกิจซึ่งทุ่มเทให้กับการป้องกันข้อมูลและสินทรัพย์ทั้งในปัจจุบันและในอีกหลายปีข้างหน้า

เพื่อปกป้องข้อมูลของลูกค้า Iron Mountain InSight® จะรักษาระดับการควบคุมขั้นสูงไว้โดย:

- การมีส่วนร่วมในสังคมการทำงานที่ตระหนักถึงการรักษาความปลอดภัยและมีการตรวจสอบอย่างเข้มงวด
- การพัฒนาและการปฏิบัติตามมาตรฐานที่เข้มงวด
- การนำแนวทางปฏิบัติที่ดีที่สุดที่สอดคล้องกับอุตสาหกรรมที่มีการพัฒนาอย่างต่อเนื่องและข้อกำหนดด้านกฎระเบียบมาปรับใช้

แนวทางปฏิบัติข้างต้นเกิดขึ้นจากการออกแบบทางกายภาพและโครงสร้างอาคาร การควบคุมสภาพแวดล้อม และระบบคอมพิวเตอร์ของเรา และด้วยคู่ค้าระบบคลาวด์ของเราเช่น Google และ Amazon Web Services เราขอรับรองว่าการรักษาความลับ ความสมบูรณ์ และความพร้อมของข้อมูลที่จัดเก็บไว้ในคลาวด์จะมีความปลอดภัยเทียบเท่ากับข้อมูลที่จัดเก็บอยู่ในอาคารและระบบคอมพิวเตอร์ของเรา

กรอบการทำงานของ Iron Mountain InSight® ในการปฏิบัติตามข้อกำหนดด้านความปลอดภัยเป็นไปตามมาตรฐาน NIST นั่นคือการระบุ การป้องกัน การตรวจจับ การรับมือ และการฟื้นฟูระบบ

การระบุ

ฟังก์ชันนี้ช่วยในการพัฒนาความเข้าใจขององค์กรในการจัดการความเสี่ยงด้านความปลอดภัยทางไซเบอร์ให้กับระบบ บุคคล สินทรัพย์ ข้อมูล และความสามารถ ซึ่งรวมถึง:

- การประเมินความเสี่ยงตาม NIST 800-53/53A
- ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System-ISMS) เพื่อปกป้องข้อมูลส่วนบุคคล (personal identifiable information-PII)
- การจัดการสินทรัพย์ ความเสี่ยง และห่วงโซ่อุปาน

การป้องกัน

ฟังก์ชันนี้จะสรุปการป้องกันเพื่อให้มั่นใจว่ามีการส่งมอบบริการโครงสร้างพื้นฐานที่สำคัญและสนับสนุนความสามารถในการจำกัดหรือควบคุมผลกระทบของเหตุการณ์ที่เป็นภัยทางไซเบอร์ที่อาจเกิดขึ้น ซึ่งรวมถึง:

- โซลูชัน Web Application Firewall (WAF) และ Data Loss Prevention (DLP)
- การจัดการข้อมูลระบุตัวตนและการเข้าถึง (IAM)
- การทดสอบการเจาะข้อมูลอย่างสม่ำเสมอ
- การเข้ารหัสข้อมูลขณะจัดเก็บและระหว่างการส่งข้อมูลด้วย AES256, TLS 1.2/3
- การฝึกอบรมเกี่ยวกับการปกป้องข้อมูล ความเป็นส่วนตัว และการรักษาความปลอดภัยสำหรับพนักงานทุกคน

การตรวจจับ

ฟังก์ชันนี้จะระบุกิจกรรมที่เหมาะสมเพื่อระบุเหตุการณ์ที่เป็นภัยทางไซเบอร์ที่เกิดขึ้น ซึ่งรวมถึง:

- โซลูชันระบบการจัดการข้อมูลความปลอดภัยและเหตุการณ์ (SIEM) สำหรับการตรวจสอบระบบ
- การตรวจสอบสภาพแวดล้อม คอนเทนเนอร์ และโค้ดทั้งหมด
- บันทึกการตรวจสอบ ระบบ และเครือข่ายทั้งหมดสำหรับกิจกรรมของผู้ใช้และผู้ดูแลระบบ

การรับมือ

ฟังก์ชันนี้ประกอบด้วยกิจกรรมที่เหมาะสมในการรับมือในกรณีที่ตรวจพบเหตุการณ์ที่เป็นภัยทางไซเบอร์ ซึ่งรวมถึง:

- ศูนย์เฝ้าระวังภัยคุกคามทางด้านไซเบอร์ (Virtual Security Operations Center-vSOC) ที่มีทรัพยากรที่ผ่านการจัดการโดยรัฐบาลกลางเพื่อการตรวจสอบความปลอดภัย
- กำหนดและอนุมัติขั้นตอนการรับมือต่อเหตุการณ์

การฟื้นฟูระบบ

ฟังก์ชันนี้จะระบุกิจกรรมที่เหมาะสมในคงแผนความยืดหยุ่นและกู้คืนความสามารถหรือบริการใดๆ ที่เกิดความบกพร่องจากเหตุการณ์ที่เป็นภัยทางไซเบอร์ ซึ่งรวมถึง:

- กำหนดและอนุมัติความต่อเนื่องทางธุรกิจ แผนสำรองฉุกเฉิน และแผนการกู้คืนความเสียหาย (RTO ภายใน 24 ชั่วโมง RPO ภายใน 1 ชั่วโมง)
- ทดสอบและประเมินแผนเหล่านี้เป็นประจำ

นอกเหนือจากรากฐานความปลอดภัยที่แน่นหนานี้ Iron Mountain InSight® ยังมีคุณสมบัติด้านความปลอดภัยเพิ่มเติมที่สามารถใช้ในการอนุญาตหรือจำกัดการเข้าถึงเนื้อหาภายในแพลตฟอร์มได้ การควบคุมผู้ใช้ข้างต้นจะถูกปรับใช้ในระดับบทบาทและสามารถเพิ่มประสิทธิภาพได้โดยการเพิ่มเกณฑ์ตามเมตาดาต้าของเนื้อหาเพื่อจำกัดการเข้าถึงข้อมูลที่สำคัญเพิ่มเติม ฟังก์ชันทางธุรกิจทั้งหมดจะได้รับการบันทึกไว้ เพื่อให้แน่ใจว่ามีการตรวจสอบที่ครอบคลุม

โปรดติดต่อเราเพื่อขอข้อมูลเพิ่มเติม

IRON MOUNTAIN®

+662 407 3333 | ironmountain.com/th

เกี่ยวกับ Iron Mountain

Iron Mountain Incorporated (NYSE: IRM) ก่อตั้งขึ้นในปี 1951 เป็นผู้นำระดับโลกของบริการจัดเก็บข้อมูลและการจัดการข้อมูล ได้รับความไว้วางใจ จากองค์กรกว่า 220,000 แห่งทั่วโลก และเครือข่ายอสังหาริมทรัพย์ที่ครอบคลุมพื้นที่กว่า 85 ล้านตารางฟุตของสถานที่ทำงานกว่า 1,400 แห่งในกว่า 50 ประเทศ Iron Mountain จึงจัดเก็บและปกป้องสินทรัพย์อันมีคุณค่าได้หลายพันล้านรายการ ไม่ว่าจะเป็นข้อมูลธุรกิจที่สำคัญเป็นอย่างยิ่ง ข้อมูลที่มีความอ่อนไหวสูง และสิ่งประดิษฐ์ทางวัฒนธรรมและประวัติศาสตร์ จัดหาโซลูชันที่มีทั้งการจัดเก็บข้อมูลที่ปลอดภัย การจัดการข้อมูลการเปลี่ยนแปลงทางดิจิทัล การทำลายข้อมูลอย่างปลอดภัย ตลอดจนศูนย์ข้อมูล ที่จัดเก็บศิลปะและโลจิสติกส์ รวมถึงบริการคลาวด์ Iron Mountain ช่วยลูกค้าลดค่าใช้จ่าย และความเสี่ยง ปฏิบัติตามกฎระเบียบ ฟื้นฟูจากภัยพิบัติ และสนับสนุนให้มีวิธีการทำงานในระบบดิจิทัลมากขึ้น