สรุปมาตรการรักษาความปลอดภัยของ HP

เพื่อเป็นการปกป้องข้อมูลลูกค้า HP จะปฏิบัติตามชุดมาตรการควบคุมการรักษาความปลอดภัยข้อมูลอย่างเข้มงวด รวมถึงนโยบาย หลักปฏิบัติ ระเบียบ และโครงสร้างองค์กร เพื่อรักษาความลับ บูรณภาพ และความพร้อมของข้อมูลของบริษัทและของลูกค้า (รวมถึงข้อมูลส่วนบุคคลของลูกค้าดังที่ระบุไว้ในภาคผนวกว่าด้วยลูกค้าของ HP และการประมวลข้อมูล) โดยต่อไปนี้เป็นข้อมูลเบื้องต้นของมาตรการรักษาความปลอดภัยทางเทคนิค/องค์กรของ HP ทั่วทั้งบริษัท

1. นโยบายการรักษาความปลอดภัย

   HP ปฏิบัติตามนโยบาย มาตรฐาน และระเบียบต่างๆ ที่เกี่ยวข้องทั่วโลก เพื่อปกป้องข้อมูลของ HP และลูกค้า โดยรายละเอียดของนโยบายการรักษาความปลอดภัยของ HP ถือเป็นความลับ เพื่อรักษาบูรณภาพของข้อมูลและระบบของ HP อย่างไรก็ตามนโยบายที่สำคัญของเรามีสรุปไว้ด้านล่างดังนี้

2. คณะทำงานระบบบริหารการรักษาความปลอดภัยสารสนเทศ

   แผนงานการรักษาความปลอดภัยสารสนเทศของ HP ออกแบบมาเพื่อกำกับและดูแลกลยุทธ์และมาตรการควบคุมการรักษาความปลอดภัยสารสนเทศขององค์กร ระบบดังกล่าวช่วยให้มั่นใจถึงการปฏิบัติตามนโยบายและมาตรการควบคุมการรักษาความปลอดภัยของ HP โดยทั่วทั้งองค์กร ตลอดจนการปฏิบัติตามข้อกำหนดการรักษาความปลอดภัยของลูกค้า กรอบการทำงานที่จัดทำขึ้นตามกรอบกฎหมาย และข้อบังคับด้านความมั่นคงปลอดภัยทางไซเบอร์ที่เป็นมาตรฐานอุตสาหกรรมได้รับการทบทวนทุกปีเพื่อปรับเปลี่ยนให้เข้ากับลักษณะภัยคุกคามที่ไม่หยุดนิ่งที่ HP ต้องเผชิญ

3. การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์

   แผนงานการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ของ HP ออกแบบมาเพื่อรักษาความลับ บูรณภาพ และความพร้อมในสินทรัพย์สารสนเทศ โดยให้แนวทางที่สอดคล้องกันเพื่อระบุ ประเมิน กำหนดลำดับความสำคัญ จัดการ แก้ไข ติดตาม และรายงานถึงความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ ทั้งนี้ HP ได้กำหนดความระดับเสี่ยงที่ยอมรับได้และระดับความเสี่ยงเบี่ยงเบนที่ยอมรับได้เอาไว้ โดยจะมีการประเมินความเสี่ยงด้วยระเบียบวิธีตามที่กำหนด ทำให้ HP สามารถบรรเทาความเสี่ยงด้านการรักษาความปลอดภัยสารสนเทศให้อยู่ในระดับที่ยอมรับได้ และแผนงานนี้ยังสอดคล้องตามกระบวนการบริหารความเสี่ยงองค์กรของ HP ด้วย

4. การรักษาความปลอดภัยด้านทรัพยากรบุคคล

   นโยบายการรักษาความปลอดภัยด้านทรัพยากรบุคคลของ HP ช่วยรับประกันการรักษาความปลอดภัยสารสนเทศตลอดวงจรชีวิตของพนักงาน โดยการกำหนดกระบวนการในการเข้าถึงสถานที่ ระบบสารสนเทศ และสินทรัพย์อื่นๆ ซึ่งรวมถึงการได้รับความยินยอมเป็นลายลักษณ์อักษรตามสัญญาการรักษาความลับและการไม่เปิดเผยข้อมูล ตลอดจนการดำเนินขั้นตอนการคัดกรองภูมิหลัง โดยผู้สมัครทุกคนที่ HP ว่าจ้างจะต้องผ่านการตรวจสอบยืนยันประวัติตามกฎหมาย ข้อบังคับ และหลักจริยธรรมที่เกี่ยวข้อง

ปรับปรุงครั้งล่าสุด: เดือนกันยายน 2024

5. การบริหารสินทรัพย์

HP มีขั้นตอนในการระบุสินทรัพย์สารสนเทศทางเทคนิค การจัดประเภทสินทรัพย์ที่สำคัญ และดูแลขั้นตอนการจัดการที่เป็นลายลักษณ์อักษรสำหรับแต่ละประเภทการจำแนกสารสนเทศ ซึ่งรวมถึงที่ประกอบด้วยข้อมูลส่วนบุคคล ขั้นตอนเหล่านี้จะครอบคลุมการจัดเก็บ การส่ง การสื่อสาร การเข้าถึง การบันทึก การเก็บรักษา การทำลาย การกำจัด การจัดการอุบัติการณ์ และการแจ้งเตือนการละเมิด นโยบายและมาตรฐานการรักษาความปลอดภัยของ HP ยังกำหนดเรื่องการกำจัดสื่อวัสดุอย่างปลอดภัยเอาไว้ด้วย

6. การรักษาความปลอดภัยของข้อมูล

แผนงานการรักษาความปลอดภัยของข้อมูลของ HP จะสรุปแนวทางปฏิบัติด้านการรักษาความปลอดภัยและมาตรการควบคุมทางเทคนิคที่ต้องดำเนินการเพื่อปกป้องความลับ ความถูกต้อง และบูรณภาพของข้อมูล ข้อกำหนดทางกฎหมาย ค่านิยม ความวิกฤต และความอ่อนไหวต่อการเปิดเผยหรือการแก้ไขโดยไม่ได้รับอนุญาตถือเป็นปัจจัยบางส่วนที่ใช้กำหนดว่าจะจำแนกสารสนเทศตามนโยบายการรักษาความปลอดภัยของข้อมูลของ HP อย่างไร นอกเหนือจากขั้นตอนการจัดการข้อมูลแล้ว นโยบายฉบับนี้ยังระบุถึงการเข้ารหัสข้อมูล การลบ การเก็บรวบรวมและการประมวลผล การเก็บรักษา การสำรองข้อมูล และการป้องกันการสูญหายของข้อมูล

7. การควบคุมการเข้าถึง

HP ใช้หลักการให้สิทธิเฉพาะเท่าที่จำเป็นเพื่อควบคุมการเข้าถึงทางตรรกะ โดยผู้ใช้สามารถเข้าถึงด้วยรหัสผู้ใช้ที่ไม่ซ้ำกันและรหัสผ่าน นโยบายรหัสผ่านจะกำหนดระดับความซับซ้อน ความเข้มงวด ความถูกต้อง และการควบคุมประวัติการตั้งรหัสผ่าน นอกจากนี้ยังมีการทบทวนสิทธิ์การเข้าถึงเป็นระยะ ทั้งยังมีการเพิกถอนสิทธิ์เมื่อบุคลากรพ้นจากหน้าที่แล้วด้วย ส่วนการสร้างและการลบบัญชีผู้ใช้นั้นก็ดำเนินการตามระเบียบที่กำหนดไว้ในการให้และเพิกถอนสิทธิ์การเข้าถึงระบบไคลเอ็นต์ในระหว่างที่มีการว่าจ้าง

8. การเข้ารหัสลับ

HP ได้กำหนดชุดกระบวนการเพื่อการเข้ารหัสลับที่แข็งแกร่ง เพื่อให้มั่นใจได้ในการรักษาความลับ บูรณภาพ และความพร้อมของสินทรัพย์สารสนเทศ สินทรัพย์บางอย่างต้องได้รับการเข้ารหัสลับตามระเบียบการที่ได้รับอนุมัติ ซึ่งรวมถึงที่มีข้อมูลส่วนบุคคลด้วย แผนงานการเข้ารหัสลับของเราเกี่ยวข้องกับการใช้เทคนิคทางคณิตศาสตร์เพื่อปกป้องสารสนเทศและการสื่อสาร เพื่อให้แน่ใจว่าผู้ที่เข้าถึงข้อมูลได้จะต้องเป็นบุคคลที่ได้รับอนุญาตเท่านั้น โดยสาระสำคัญของแผนงานการรักษาความปลอดภัยสารสนเทศของ HP ก็คือการปกป้องข้อมูลจากการเข้าถึงและการดัดแปลงโดยไม่ได้รับอนุญาต

9. การรักษาความปลอดภัยทางกายภาพและสิ่งแวดล้อม

สถานที่ของ HP ได้รับการรักษาความปลอดภัยโดยใช้การควบคุมการเข้าถึงทางกายภาพและทางอิเล็กทรอนิกส์หลากหลายแบบ รวมถึงเจ้าหน้าที่รักษาความปลอดภัย การควบคุมการเข้าถึงทางอิเล็กทรอนิกส์ และกล้องวงจรปิด (CCTV) นอกจากนี้สถานที่ต่างๆ ยังติดตั้งอุปกรณ์สนับสนุนทางโครงสร้างพื้นฐานที่จำเป็น ซึ่งรวมถึงการควบคุมอุณหภูมิและการสำรองไฟฟ้า โดยใช้ UPS และ/หรือเครื่องกำเนิดไฟฟ้าดีเซลเพื่อรองรับบริการที่สำคัญ บุคลากรของ HP ทุกคนต้องลงทะเบียนและต้องพกบัตรประจำตัวตามความเหมาะสม

10. การจัดการการดำเนินงาน

HP ได้กำหนดข้อบังคับขั้นต่ำอันเข้มงวดสำหรับโครงสร้างพื้นฐานทางเทคโนโลยี ซึ่งรวมถึงเวิร์กสเตชัน เซิร์ฟเวอร์ และอุปกรณ์เครือข่าย อุปกรณ์เหล่านี้จะใช้อิมเมจระบบปฏิบัติการที่มีการติดตั้งมาตรการความปลอดภัยเอาไว้แล้ว โดยเป็นไปตามข้อบังคับที่แตกต่างกันไปตามระบบปฏิบัติการและมาตรการควบคุมที่ใช้บังคับ นอกจากนี้ HP ยังติดตั้งและใช้ระบบตรวจสอบ/ป้องกันการบุกรุกเครือข่าย (NIDS/NIPS) ที่มีการติดตามและจัดการตลอด 24 ชั่วโมงด้วย

ปรับปรุงครั้งล่าสุด: เดือนกันยายน 2024

11. การรักษาความปลอดภัยด้านการสื่อสาร

    การรักษาความปลอดภัยด้านการสื่อสารเป็นไปเพื่อการปกป้องสารสนเทศภายในเครือข่ายองค์กร ซึ่งรวมถึงการติดตั้งและการจัดการองค์ประกอบการรักษาความปลอดภัยเครือข่าย (เช่น ไฟร์วอลล์) การแบ่งแยกเครือข่าย และมาตรการควบคุมการคัดกรองเว็บและการจัดการอีเมล นอกจากนี้ยังเกี่ยวข้องกับการติดตามและจัดการช่องทางการสื่อสารเพื่อตรวจจับและป้องกันการเข้าถึงหรือการละเมิดข้อมูลโดยไม่ได้รับอนุญาตด้วย

12. การรักษาความปลอดภัยระบบ

    นโยบายของ HP ได้กำหนดระเบียบวิธีการพัฒนาระบบและซอฟต์แวร์อย่างปลอดภัยตลอดวงจรด้วย โดยวงจรการพัฒนาซอฟต์แวร์ครอบคลุมตั้งแต่การเริ่มต้น การพัฒนา/การจัดหา การใช้งาน การปฏิบัติงาน และการกำจัดทิ้ง องค์ประกอบระบบทั้งหมดจะได้รับการประเมินผลกระทบต่อการรักษาความปลอดภัยโดยรวม โดย HP ได้กำหนดมาตรการควบคุมสำหรับธุรกรรมของบริการแอปพลิเคชันอันประกอบด้วยการตรวจสอบความถูกต้องของข้อมูลรับรองผู้ใช้ ลายเซ็นดิจิทัล การเข้ารหัส โปรโตคอลการสื่อสารอย่างปลอดภัย และจัดเก็บรายละเอียดธุรกรรมภายในโซนการรักษาความปลอดภัยเครือข่ายที่เหมาะสม นอกจากนี้ยังมีการสแกนช่องโหว่ภายในเป็นประจำด้วย

13. บุคคลที่สามและผู้รับจ้างช่วง

    HP มีกระบวนการคัดเลือกผู้รับจ้างช่วงที่ปฏิบัติตามข้อกำหนดด้านการรักษาความปลอดภัยตามสัญญาอย่างครบถ้วน สำหรับซัพพลายเออร์ที่เกี่ยวข้องกับการจัดการข้อมูลของ HP หรือลูกค้า หรือมีการเข้าถึงเครือข่ายของ HP ทางฝ่ายความมั่นคงปลอดภัยทางไซเบอร์ของ HP จะดำเนินการประเมินความเสี่ยงเพื่อตรวจสอบแผนงานการรักษาความปลอดภัยสารสนเทศตามมาตรการความปลอดภัยทางกายภาพ ทางเทคนิค และด้านการบริหารจัดการ โดยจะต้องมีการประเมินก่อนที่ซัพพลายเออร์จะเข้าถึงข้อมูลของ HP

14. การจัดการอุบัติการณ์ด้านการรักษาความปลอดภัยสารสนเทศ

    HP มีกระบวนการจัดการอุบัติการณ์ทางไซเบอร์ที่ครอบคลุมซึ่งระบุวัตถุประสงค์ ขอบเขต บทบาท ความรับผิดชอบ คำมั่นของฝ่ายบริหาร การประสานงานขององค์กร ขั้นตอนการดำเนินการ และการตรวจสอบการปฏิบัติตามข้อกำหนด โดยกระบวนการนี้จะได้รับการตรวจสอบและปรับปรุงทุกปี ทีมรับมืออุบัติการณ์ทางไซเบอร์ ซึ่งรวมถึงบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์ของ HP ที่ได้รับการฝึกอบรมในการรับมืออุบัติการณ์และการจัดการภาวะฉุกเฉิน ยังมีการทบทวนขั้นตอน อุบัติการณ์ หรือเหตุการณ์ภายใต้สถานการณ์จำลองเป็นประจำ

15. การบริหารความต่อเนื่องทางธุรกิจ

    แผนงานความต่อเนื่องในการดำเนินงานทั่วโลกของ HP ช่วยรับประกันความต่อเนื่องในทุกกระบวนการผ่านกระบวนการที่การทำงานร่วมกัน เป็นไปตามมาตรฐาน และได้รับการวางแผนเป็นลายลักษณ์อักษร โดยบริษัทจะดำเนินการตามแผนความต่อเนื่องทางธุรกิจเป็นระยะๆ เพื่อให้มั่นใจว่าแผนดังกล่าวมีประสิทธิภาพ โดยมีการทดสอบและปรับปรุงแผนงานทั้งหมดอย่างน้อยปีละหนึ่งครั้ง นอกจากนี้บุคลากรทุกคนที่เกี่ยวข้องกับแผนความต่อเนื่องทางธุรกิจยังได้รับการฝึกอบรมที่เหมาะสมด้วย

ปรับปรุงครั้งล่าสุด: เดือนกันยายน 2024

16. การปฏิบัติตามกฎระเบียบ

การปฏิบัติตามกฎระเบียบเป็นสิ่งที่กำหนดแนวทางของ HP ให้เป็นไปตามความคาดหวังทางกฎหมาย ทางสัญญา และเป็นการภายใน เพื่อแผนงานการรักษาความปลอดภัยสารสนเทศที่มีประสิทธิภาพ การตรวจสอบการรักษาความปลอดภัยสารสนเทศเป็นประจำทำให้มั่นใจได้ว่า ระเบียบการต่างๆ ได้รับการผสานไว้ในการดำเนินงานของแต่ละกลุ่มธุรกิจ กระบวนการตรวจสอบยังรวมถึงการดูแลเอกสารให้ได้รับการปรับปรุงล่าสุดเพื่อให้สอดคล้องตามภาระผูกพันทางกฎหมายในปัจจุบันตามข้อบังคับที่เปลี่ยนไป

17. อุตสาหกรรมบัตรชำระเงิน

กรอบการทำงานของ Payment Card Industry (PCI) เป็นสิ่งกำหนดแนวทางของ HP ในการบรรลุ PCI Compliance ซึ่งว่าด้วยความรับผิดชอบทางธุรกิจและมาตรการควบคุมการรักษาความปลอดภัยที่สอดคล้องตาม PCI DSS ซึ่งการติดตั้งและดูแลระบบควบคุมการรักษาความปลอดภัยเครือข่ายอย่างเช่นไฟร์วอลล์นั้น HP รับประกันว่าจะเป็นไปตามข้อกำหนดของ PCI Compliance

18. การรักษาความปลอดภัยผลิตภัณฑ์ HP

การรักษาความปลอดภัยผลิตภัณฑ์ HP ครอบคลุมหลักปฏิบัติที่สำคัญในการรักษาความปลอดภัยผลิตภัณฑ์ HP เช่น การลงชื่อในรหัสโปรแกรม การจัดการช่องโหว่ด้านความปลอดภัยของผลิตภัณฑ์ การออกรายงานด้านความปลอดภัย และการแจ้งรายงานปัญหาการรักษาความปลอดภัยผลิตภัณฑ์ โดยมาตรการเหล่านี้ช่วยให้มั่นใจได้ว่าผลิตภัณฑ์ HP จะยังคงปลอดภัยและเชื่อถือได้สำหรับผู้ใช้ การรักษาความปลอดภัยผลิตภัณฑ์ HP เป็นสิ่งสำคัญที่สุดที่ HP เนื่องจากช่วยรักษาความเชื่อถือของลูกค้าและป้องกันภัยคุกคามที่อาจเกิดขึ้น

19. การรักษาความปลอดภัยบริการ HP

การรักษาความปลอดภัยบริการ HP มีหลักปฏิบัติที่สำคัญในการรักษาความปลอดภัยให้แก่บริการต่างๆ ที่มอบให้ลูกค้าของ HP โดยนโยบายนี้ระบุถึงส่วนต่างๆ ในการรักษาความปลอดภัยบริการ อันรวมถึงสภาพแวดล้อมระบบที่จัดเก็บบนโครงสร้างพื้นฐานของ HP, ของบุคคลที่สาม, ของพันธมิตร และของลูกค้า โดยมาตรการเหล่านี้ช่วยให้มั่นใจได้ว่าบริการ HP จะยังคงปลอดภัยและเชื่อถือได้สำหรับผู้ใช้ ทั้งนี้การปฏิบัติตามมาตรการรักษาความปลอดภัยที่เข้มงวดทำให้ HP มั่นใจได้ในความปลอดภัยและบูรณภาพของผลิตภัณฑ์และบริการ เพื่อส่งเสริมสภาพแวดล้อมที่ปลอดภัยและเชื่อถือได้สำหรับผู้ใช้ทุกคน

ปรับปรุงครั้งล่าสุด: เดือนกันยายน 2024