



นโยบายความมั่นคงปลอดภัยสารสนเทศ
บริษัท บัตรกรุงไทย จำกัด (มหาชน)

นโยบายความมั่นคงปลอดภัยสารสนเทศ บริษัท บัตรกรุงไทย จำกัด (มหาชน)

บริษัท บัตรกรุงไทย จำกัด (มหาชน) และบริษัทย่อย (“บริษัทฯ” หรือ “เคทีซี”) ตระหนักว่าความมั่นคงปลอดภัยสารสนเทศเป็นรากฐานสำคัญของการดำเนินธุรกิจอย่างยั่งยืน และเป็นปัจจัยสำคัญในการสร้างและรักษาความเชื่อมั่นของผู้มีส่วนได้เสีย ความมุ่งมั่นดังกล่าวสะท้อนผ่านนโยบายความมั่นคงปลอดภัยสารสนเทศของเคทีซี ซึ่งกำหนดแนวทางในการคุ้มครองความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูล ระบบสารสนเทศ และทรัพย์สินที่เกี่ยวข้องของบริษัทฯ

วัตถุประสงค์

เพื่อกำหนดกรอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและความเป็นส่วนตัว เพื่อปกป้องข้อมูลระบบ และบริการของบริษัทฯ สนับสนุนการดำเนินธุรกิจอย่างมั่นคงปลอดภัย ส่งเสริมความตระหนักรู้แก่ผู้มีส่วนได้เสียที่เกี่ยวข้อง และเสริมสร้างความเชื่อมั่นให้แก่ผู้มีส่วนได้เสียทุกฝ่าย

ขอบเขต

นโยบายฉบับนี้มีผลบังคับใช้กับสินทรัพย์สารสนเทศ ระบบสารสนเทศ และกระบวนการดำเนินธุรกิจทั้งหมดที่อยู่ภายใต้ความเป็นเจ้าของหรือการกำกับดูแลของบริษัทฯ ครอบคลุมถึงกิจกรรมการจัดเก็บ การประมวลผล การส่งต่อการเก็บรักษา และการทำลายข้อมูลสารสนเทศทุกประเภท ทั้งนี้ บริษัทฯ จะสื่อสารนโยบายฉบับนี้ให้พนักงาน บุคลากรภายนอก (Outsource) ลูกค้า คู่ค้า พันธมิตรทางธุรกิจ ตลอดจนบุคคลภายนอกที่มีสิทธิ์เข้าถึงหรือใช้งานระบบสารสนเทศของบริษัทฯ รับทราบ

แนวปฏิบัติ

1. การเสริมสร้างระบบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง

- ทบทวนและปรับปรุงนโยบาย มาตรฐาน และขั้นตอนปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศอย่างสม่ำเสมออย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ เพื่อให้สอดคล้องกับกฎหมาย ข้อบังคับ และมาตรฐานสากลที่เกี่ยวข้อง รวมถึงมาตรฐาน ISO/IEC 27001
- ดำเนินการประเมินความเสี่ยงอย่างต่อเนื่อง และปรับปรุงมาตรการควบคุมด้านความมั่นคงปลอดภัยให้สอดคล้องกับภัยคุกคาม สภาพแวดล้อมทางธุรกิจ และเทคโนโลยีที่เปลี่ยนแปลงไป โดยอ้างอิงแนวปฏิบัติจากกรอบการดำเนินงานสากล เช่น NIST Cybersecurity Framework (CSF)
- ติดตามและประเมินผลการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศอย่างสม่ำเสมอ เพื่อขับเคลื่อนการปรับปรุงและพัฒนาอย่างต่อเนื่อง

2. การคุ้มครองความถูกต้องครบถ้วนและการรักษาความลับของข้อมูล

- มุ่งมั่นในการปกป้องข้อมูลตลอดวงจรชีวิตของข้อมูล เพื่อป้องกันการเข้าถึง การแก้ไขเปลี่ยนแปลง การเปิดเผย หรือการทำลายข้อมูลโดยไม่ได้รับอนุญาต
- จัดประเภทสินทรัพย์สารสนเทศตามระดับความอ่อนไหว ความสำคัญเชิงวิกฤต และผลกระทบต่อธุรกิจ
- จำกัดการเข้าถึงข้อมูลตามหลักความจำเป็นในการรับรู้ (Need-to-Know Basis) ผ่านการกำหนดสิทธิ์การเข้าถึง ที่ชัดเจนและเหมาะสม
- นำมาตรการป้องกันทางเทคนิคมาใช้ เช่น การเข้ารหัสข้อมูล (Encryption) และการป้องกันการรั่วไหลของข้อมูล (Data Loss Prevention: DLP) เพื่อคุ้มครองข้อมูลทั้งขณะที่จัดเก็บ ส่งผ่าน และระหว่างการประมวลผล โดยข้อมูลผู้ถือบัตรจะได้รับการคุ้มครองให้สอดคล้องกับมาตรฐาน Payment Card Industry Data Security Standard (PCI DSS)

3. การเฝ้าระวังและตอบสนองต่อภัยคุกคามทางไซเบอร์

- เฝ้าติดตามข่าวกรองภัยคุกคามทางไซเบอร์จากแหล่งข้อมูลที่หลากหลายอย่างต่อเนื่อง เพื่อให้สามารถตรวจจับ และคาดการณ์ความเสี่ยงที่เกิดขึ้นใหม่ได้ โดยสอดคล้องกับแนวทางด้าน Identify และ Detect ของ NIST Cybersecurity Framework (CSF)
- จัดให้มีขีดความสามารถด้านการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศโดยเฉพาะ เพื่อควบคุมเหตุการณ์ ตรวจสอบสาเหตุ และดำเนินการแก้ไขฟื้นฟูได้อย่างทัน่วงที
- ทบทวนเหตุการณ์ที่เกิดขึ้นเพื่อวิเคราะห์สาเหตุที่แท้จริงของปัญหา (Root Cause Analysis) และถอดบทเรียนที่ได้รับ เพื่อนำไปเสริมสร้างความแข็งแกร่งด้านความมั่นคงปลอดภัยของเครือข่าย และป้องกันไม่ให้เกิดเหตุการณ์ซ้ำ

4. การส่งเสริมวัฒนธรรมด้านความตระหนักรู้และความรับผิดชอบด้านความมั่นคงปลอดภัย

- กำหนดให้พนักงาน ผู้รับจ้าง และผู้ฝึกงานทุกคนปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ และรายงานเหตุการณ์หรือช่องโหว่ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยโดยทันที
- จัดให้มีการฝึกอบรมและกิจกรรมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศอย่างสม่ำเสมอทั่วทั้งองค์กร
- ติดตามการปฏิบัติตามข้อกำหนด และดำเนินการกับกรณีการฝ่าฝืนผ่านกระบวนการทางวินัยและการกำกับดูแล ที่กำหนดไว้อย่างเหมาะสม

5. ข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศสำหรับบุคคลภายนอก

- บริษัทฯ ขยายขอบเขตมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศไปยังความสัมพันธ์กับบุคคลภายนอก เพื่อบริหารจัดการความเสี่ยงที่เกิดจากผู้ส่งมอบ ผู้ขาย และผู้ให้บริการที่สามารถเข้าถึงระบบ โครงสร้างพื้นฐาน หรือข้อมูลของบริษัทฯ
- ประเมินแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศของผู้ส่งมอบ ผู้ขาย และผู้ให้บริการที่มีความสำคัญ พร้อมทั้งจัดทำและดูแลข้อมูลความเสี่ยง (Risk Profile) เพื่อสนับสนุนการกำกับดูแลและติดตามความเสี่ยงอย่างต่อเนื่อง
- บูรณาการข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศไว้ในสัญญาและข้อตกลงการให้บริการ โดยกำหนดให้บุคคลที่สามต้องนำมาตรการควบคุมที่สอดคล้องกับมาตรฐานของบริษัทฯ ไปปฏิบัติ รวมถึงข้อกำหนดตามมาตรฐานความปลอดภัยข้อมูลอุตสาหกรรมบัตรเครดิตชำระเงิน (PCI DSS) สำหรับบุคคลที่สามที่สามารถเข้าถึงข้อมูลผู้ถือบัตร (Cardholder Data)
- ติดตามและควบคุมการเข้าถึงข้อมูลและระบบของบริษัทฯ โดยบุคคลที่สาม รวมถึงการดำเนินการทบทวนผลการดำเนินงานด้านความมั่นคงปลอดภัยของบุคคลที่สามเป็นระยะ เพื่อให้ระบบ โครงสร้างพื้นฐาน และข้อมูลที่มีการใช้งานร่วมกัน ได้รับการปกป้องอย่างเหมาะสมและปลอดภัย

แนวปฏิบัติเหล่านี้สะท้อนถึงความมุ่งมั่นอย่างต่อเนื่องของบริษัทฯ ในการสร้างและรักษาความเชื่อมั่นของลูกค้าและผู้มีส่วนได้เสีย ตลอดจนการดำเนินธุรกิจอย่างมั่นคงปลอดภัยและยั่งยืนในสภาพแวดล้อมที่มีการเปลี่ยนแปลงผ่านสู่ดิจิทัล และการเชื่อมโยงถึงกันมากยิ่งขึ้น

การทบทวนนโยบาย

นโยบายฉบับนี้ต้องได้รับการทบทวนอย่างน้อยปีละ 1 ครั้ง หรือเมื่อเกิดเหตุการณ์สำคัญที่อาจส่งผลกระทบต่อ การบังคับใช้นโยบาย เพื่อให้สามารถรองรับการเปลี่ยนแปลงที่สำคัญในด้านข้อกำหนดทางกฎหมายและกฎระเบียบ การดำเนินธุรกิจ เทคโนโลยี รวมถึงความเสี่ยงที่เกิดขึ้นใหม่

นโยบายฉบับนี้ได้รับการอนุมัติจากคณะกรรมการบริษัท และมีผลบังคับใช้นับตั้งแต่วันที่ได้รับอนุมัติเป็นต้นไป