นโยบายความมั่นคงปลอดภัยที่ใช้กำกับดูแลบุคคลหรือหน่วยงานภายนอก

Third Party Security Policy

รุ่นเอกสาร	1.5	เลขที่เอกสาร	ISMS-PL-10
สายงาน	บริหารความมั่นคงปลอดภัยระบบสารสนเทศ		
กลุ่ม	ดิจิทัลทรานส์ฟอร์เมชั่น		
อนุมัติโดย			
นโยบายนี้ให้มีผลใช้บังคับ ตั้งแต่วันที่ 22 สิงหาคม 2566 เป็นต้นไป ตามมติที่ประชุมคณะทำงานกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ ครั้งที่ 3 เมื่อวันที่ 22 สิงหาคม 2566 ลงนามโดย คุณเคียน ฮิน ลิม (President)			

ประวัติการแก้ไข

รุ่นเอกสาร	วันที่	รายละเอียด	ทบทวนโดย
1.0	30/06/2017	จัดทำเอกสาร	นายมานะ ขจรมาศบุษป์
1.1	16/06/2019	ปรับปรุงเอกสาร	นายมานะ ขจรมาศบุษป์ นางกรกมล สุภวัฒนกูล
1.2	30/04/2020	ปรับปรุงเอกสาร	นายเต็มภาคย์ ภัทรรัชต์ภาคย์
1.3	04/06/2021	ปรับปรุงเอกสารเพิ่ม -บริษัทฯ -บทลงโทษ	นายเต็มภาคย์ ภัทรรัชต์ภาคย์
1.4	27/07/2022	ปรับปรุงเอกสาร - เพิ่มการทบทวนเอกสาร	นายสุวัฒชัย สันตินรศักดิ์
1.5	16/05/2023	ทบทวนเอกสาร	น.ส.เมกรินทร์ วุฒิฑา

นโยบายความมั่นคงปลอดภัยที่ใช้กำกับดูแลบุคคลหรือหน่วยงานภายนอก

1. บทนำ

1.1. วัตถุประสงค์

- เพื่อรักษาความมั่นคงของข้อมูลและระบบเทคโนโลยีสารสนเทศของบริษัทฯ เมื่อต้องมีการดำเนินงานร่วมกันหรือใช้บริการจาก Third-Party
- เพื่อควบคุมให้บริการที่ได้รับจาก Third-Party เป็นไปอย่างถูกต้อง มั่นคงปลอดภัย ตรงตามสัญญาหรือข้อตกลง และเพื่อให้ Third-Party ดูแลและใช้อุปกรณ์คอมพิวเตอร์และทรัพย์สินของบริษัทฯ อย่างระมัดระวัง

1.2. ขอบเขต

นโยบายนี้ครอบคลุมการดำเนินงานต่างๆ ที่เกี่ยวข้องกับ Third-Party และลูกค้าของบริษัทฯ ทั้งในด้านการว่าจ้าง การทำสัญญา การควบคุมการเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศ การตรวจสอบการเข้าปฏิบัติงาน และการตรวจสอบบริการที่ได้รับ

1.3. ขอบเขต

Vendor หมายถึง ผู้ขายสินค้า และ ผู้ให้บริการ

Third-Party หมายถึง Vendor ลูกค้า และ คู่ค้า ที่มีความจำเป็นต้องเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศของบริษัทฯ หรือใช้อุปกรณ์คอมพิวเตอร์หรือทรัพย์สินของบริษัทฯ

2. นโยบาย

2.1. การดำเนินงานร่วมกับ Vendor

- การว่าจ้าง Vendor ต้องทำการคัดเลือก ตรวจสอบคุณสมบัติ ประเมินความสามารถของ Vendor ตามระเบียบของบริษัทฯ และพิจารณาถึงระดับความสำคัญของข้อมูลและระบบเทคโนโลยีสารสนเทศที่ Vendor ต้องเข้าถึงหรือใช้งาน
- Third-Party ทุกรายที่ดำเนินธุรกิจร่วมกับบริษัทฯ ต้องลงนามในเอกสารต่อไปนี้ ตามความเหมาะสมก่อนเริ่มปฏิบัติงาน
    1. สัญญาการปฏิบัติงาน (Contract) และ/หรือ สัญญาบริการ (Service Level Agreement)
    2. ข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement)

โดยเอกสารสัญญาและข้อตกลงต่างๆ ต้องผ่านการทบทวนโดยฝ่ายกฎหมายอย่างเหมาะสมทุกครั้ง

- หน่วยงานผู้ว่าจ้าง Vendor และ สายงานบริหารความมั่นคงปลอดภัยระบบสารสนเทศหรือผู้ที่ได้รับมอบหมาย อาจพิจารณาให้มีการเพิ่มเติมข้อกำหนดหรือวิธีการปกป้องใดๆ ในเอกสารสัญญา เพื่อรักษาความมั่นคงของข้อมูลและระบบเทคโนโลยีสารสนเทศของบริษัทฯ ทั้งนี้ขึ้นอยู่กับลักษณะงานที่ทำการว่าจ้าง และ ผลการประเมินความเสี่ยง
- กรณีของการทำสัญญาที่เกี่ยวกับการแลกเปลี่ยนข้อมูลหรือซอฟต์แวร์ระหว่างบริษัทฯ ต้องพิจารณาเพิ่มเติมหัวข้อในสัญญา ดังนี้
    1. ระบุวิธีการที่ใช้ในการแลกเปลี่ยนข้อมูลหรือซอฟต์แวร์และหน้าที่ความรับผิดชอบของทั้ง 2 ฝ่ายอย่างชัดเจน โดยวิธีในการแลกเปลี่ยนนี้ ต้องได้รับการทบทวนและอนุมัติจาก ผู้บริหารตั้งแต่ระดับผู้ช่วยผู้อำนวยการสายงานขึ้นไป ของสายงานบริหารความมั่นคงปลอดภัยระบบสารสนเทศหรือผู้ที่ได้รับมอบหมาย
    2. ระบุวิธีการ Label และช่องทางในการจัดส่งข้อมูล (Courier) อย่างชัดเจน
    3. ระบุเทคโนโลยีที่เลือกใช้งาน เพื่อปกป้องความมั่นคงให้แก่ข้อมูลตามความเหมาะสม เช่น การเข้ารหัสข้อมูล
    4. ระบุวิธีในการรับมือเมื่อเกิดเหตุละเมิดความมั่นคงปลอดภัยในระหว่างการแลกเปลี่ยนข้อมูล
- กรณีของการทำสัญญาที่เกี่ยวกับการว่าจ้าง Vendor พัฒนาโปรแกรม ต้องพิจารณาเพิ่มเติมหัวข้อในสัญญา ดังนี้
    1. ระบุความต้องการด้านคุณภาพและฟังก์ชั่นด้านความมั่นคง ในโปรแกรมและ Source Code ที่พัฒนาขึ้น
    2. ระบุข้อตกลงด้านลิขสิทธิ์และทรัพย์สินทางปัญญาของโปรแกรมที่พัฒนาขึ้น
    3. ระบุหน้าที่ความรับผิดชอบของ Vendor เกี่ยวกับการรับรองคุณภาพและความถูกต้องของโปรแกรมที่พัฒนาขึ้น
    4. ระบุสิทธิของบริษัทฯในการเข้าถึงและตรวจสอบคุณภาพและความถูกต้องของโปรแกรมที่พัฒนาขึ้น
- Vendor ต้องสื่อสารให้เจ้าหน้าที่ของตนรับทราบถึงรายละเอียดในเอกสาร Third-Party Code of Conduct รวมถึงเอกสารสัญญาหรือข้อตกลงอื่นๆ ที่เกี่ยวข้อง เพื่อให้เจ้าหน้าที่ของ Vendor สามารถปฏิบัติงานให้แก่บริษัทฯ ได้อย่างถูกต้อง เมื่อต้องเข้าติดต่อประสานงานหรือใช้งานข้อมูลและระบบเทคโนโลยีสารสนเทศของบริษัทฯ
- Vendor ต้องแจ้งรายชื่อของเจ้าหน้าที่ที่จะเข้าปฏิบัติงานต่อบริษัทฯ ก่อนเริ่มปฏิบัติงาน และหากมีการเปลี่ยนแปลงบุคคลที่เข้าปฏิบัติงาน ต้องแจ้งให้ทางบริษัทฯ ทราบล่วงหน้าทุกครั้ง

- เจ้าหน้าที่ของ Vendor ต้องปฏิบัติตามกฎระเบียบ, นโยบาย, ขั้นตอนการปฏิบัติงาน และวิธีการปฏิบัติงานต่างๆ ของบริษัทฯ อย่างเคร่งครัด
- ข้อมูลทุกประเภทที่ Vendor ได้รับหรือรับทราบจากบริษัทฯ ต้องถูกเก็บรักษาไว้เป็นความลับ และอนุญาตให้ใช้ข้อมูลเพื่อการปฏิบัติงานให้แก่บริษัทฯ เท่านั้น
- กรณีที่การให้บริการของ Vendor อยู่นอกพื้นที่ของบริษัทฯ บริษัทฯ สงวนสิทธิ์ในการตรวจสอบทุกพื้นที่ที่มีการนำข้อมูลของบริษัทฯ ไปใช้งาน ส่งผ่าน หรือประมวลผล
- อุปกรณ์ หรือซอฟต์แวร์ที่ Vendor นำมาใช้ในการปฏิบัติงานให้แก่บริษัทฯ ต้องได้รับการรักษาความมั่นคงปลอดภัยอย่างเหมาะสม โดยอย่างน้อยต้องได้รับการติดตั้งซอฟต์แวร์ป้องกันไวรัสที่เชื่อถือได้และมีฐานข้อมูลที่ทันสมัย ทั้งนี้ สายงานบริหารความมั่นคงปลอดภัยระบบสารสนเทศหรือผู้ที่ได้รับมอบหมายอาจพิจารณาให้ Vendor ติดตั้งซอฟต์แวร์หรือสร้างมาตรการรักษาความมั่นคงปลอดภัยเพิ่มเติมตามความเหมาะสม
- กรณีที่ต้องติดตั้งอุปกรณ์และซอฟต์แวร์ของบริษัทฯ ไว้ในสถานที่ของ Vendor อุปกรณ์และซอฟต์แวร์ทั้งหมดต้องได้รับการบันทึกไว้ การเข้าถึงอุปกรณ์และเชื่อมต่อกับระบบเครือข่ายของบริษัทฯ ต้องกระทำโดยพนักงานของบริษัทฯ อุปกรณ์และซอฟต์แวร์ต้องใช้เพื่อสนับสนุนการดำเนินธุรกิจของบริษัทฯ เท่านั้น บริษัทฯ สงวนสิทธิ์ในการพิจารณายกเลิกสัญญาในกรณีที่มีการใช้อุปกรณ์หรือซอฟต์แวร์ของบริษัทฯ ในทางที่ผิด
- การเข้าถึงเพื่อใช้งานข้อมูลและระบบเทคโนโลยีสารสนเทศของบริษัทฯ โดย Vendor ต้องได้รับการควบคุมอย่างเหมาะสม
- การให้สิทธิเข้าใช้งานระบบเทคโนโลยีสารสนเทศของบริษัทฯ แก่ Vendor ต้องมีการกำหนดระยะเวลาของสิทธิอย่างชัดเจน
- การเข้าใช้งานระบบเทคโนโลยีสารสนเทศของบริษัทฯ โดย Vendor ต้องได้รับการควบคุมให้เข้าใช้งานได้เฉพาะระบบเทคโนโลยีสารสนเทศที่ได้รับอนุญาตเท่านั้น
- การให้บริการของ Vendor ที่มีความจำเป็นต้องเชื่อมต่อระบบเครือข่ายของบริษัทฯ กับระบบของ Vendor หรือ มีความจำเป็นต้องเปิดช่องทางสื่อสารเพื่อให้ Vendor เข้าถึงระยะไกล (Remote Access) หรือเพื่อส่งข้อมูลของบริษัทฯ ออกไปยังระบบของ Vendor รวมถึงกรณีอื่นๆ ที่อาจก่อให้เกิดความเสี่ยงขึ้นในระบบสารสนเทศของบริษัทฯ ต้องได้รับการประเมินความเสี่ยงและบริหารจัดการความเสี่ยงอย่างเหมาะสม ทั้งนี้ต้องได้รับการอนุมัติจาก ผู้บริหารตั้งแต่ระดับผู้ช่วยผู้อำนวยการสายงานขึ้นไปของสายงานบริหารความมั่นคงปลอดภัยระบบสารสนเทศหรือผู้ที่ได้รับมอบหมาย ทุกครั้งก่อนดำเนินการ โดยมีหัวข้อที่ควรพิจารณาอย่างน้อยดังนี้

1. ความมั่นคงปลอดภัยของสถานที่ และ/หรือ ระบบที่จะทำการเชื่อมต่อกับระบบเครือข่ายของบริษัทฯ
2. ความมั่นคงปลอดภัยของจุดหรืออุปกรณ์ที่ต้องทำการเชื่อมต่อ
3. วิธีในการพิสูจน์ตัวตนก่อนอนุญาตให้เข้าถึงระบบ
4. ความมั่นคงปลอดภัยของช่องทางและวิธีการส่งผ่านข้อมูล
5. วิธีในการควบคุมและติดตามตรวจสอบ (Monitor) การเข้าใช้งานหรือการส่งข้อมูล
6. ข้อกำหนดอื่นๆ ที่ควรจัดให้มีเพื่อเพิ่มความมั่นคงปลอดภัย เช่น การจำกัดเวลาการเชื่อมต่อ
7. ระยะเวลาที่อนุญาตให้ดำเนินการเชื่อมต่อหรือส่งผ่านข้อมูล และรอบระยะเวลาที่เหมาะสมในการประเมินความเสี่ยงซ้ำและตรวจสอบความมั่นคงปลอดภัยซ้ำ

- ห้าม Vendor และ/หรือ เจ้าหน้าที่ของ Vendor นำเอกสารหรือซอฟต์แวร์ที่มีลิขสิทธิ์ของบริษัทฯ ไปใช้งานส่วนตัวหรือใช้งานในทางที่ผิด และห้ามนำเอกสารหรือซอฟต์แวร์ที่ละเมิดลิขสิทธิ์มาใช้งานในบริษัทฯ
- บริษัทฯ สงวนสิทธิในการตรวจสอบการทำงานของ Vendor รวมถึงการเพิกถอนสิทธิต่างๆ ในการเข้าใช้ข้อมูลและระบบเทคโนโลยีสารสนเทศ เมื่อพบสิ่งผิดปกติหรือมีเหตุละเมิดความมั่นคงปลอดภัยโดยไม่ต้องแจ้งให้ทราบล่วงหน้า
- สิทธิในการเข้าถึงระบบต่างๆ ของ Vendor ต้องถูกบันทึกและตรวจสอบการใช้งานอย่างสม่ำเสมอ
- Vendor ต้องรายงานสิ่งผิดปกติหรือเหตุละเมิดความมั่นคงปลอดภัยต่อผู้ดูแลระบบและพนักงานที่เป็นผู้ติดต่อประสานงานทันทีที่พบเหตุ
- การกระทำใดๆ โดยเจ้าหน้าที่ของ Vendor ที่ก่อให้เกิดความเสียหาย หรือละเมิดข้อตกลงหรือสัญญาต่างๆ ที่ได้ทำไว้กับบริษัทฯ Vendor ที่เป็นต้นสังกัดของเจ้าหน้าที่ ต้องรับผิดชอบต่อความเสียหายทั้งหมด
- Vendor ที่มีการจ้างช่วงงานต่อให้ Subcontractor ต้องแจ้งให้ทางบริษัทฯ ทราบทุกครั้ง และต้องดำเนินการให้ Subcontractor ปฏิบัติตามนโยบาย Third Party Code of Conduct และสัญญาที่ Vendor ได้ทำไว้กับบริษัทฯ โดย Vendor มีหน้าที่กำกับดูแลและรับผิดชอบต่อผลงานและการกระทำทั้งหมดของ Subcontractor
- ผู้ดูแลระบบและพนักงานผู้ติดต่อประสานงานกับ Vendor มีหน้าที่ดูแล ควบคุม และตรวจสอบการปฏิบัติงานของ Vendor ที่เกี่ยวข้องให้เป็นไปตามเอกสารสัญญา ข้อตกลง รวมถึงกฎระเบียบ นโยบาย ขั้นตอนการปฏิบัติงานและวิธีการปฏิบัติงานต่างๆ ของบริษัทฯ อย่างเคร่งครัด

- พนักงานผู้ติดต่อประสานงานกับ Vendor หรือผู้ที่เกี่ยวข้อง ต้องทำการตรวจสอบความสมบูรณ์เรียบร้อยของงานที่ส่งมอบโดย Vendor และต้องทำการตรวจสอบ ทดสอบให้มั่นใจว่าสามารถปฏิบัติงานได้จริง ผ่านการปรับปรุงแก้ไขอย่างเหมาะสม และตรงตามเอกสารสัญญาหรือ SLA (Service Level Agreement) ทุกครั้งก่อนการตรวจรับงาน
- เมื่อสิ้นสุดสัญญาการปฏิบัติงาน มีการเปลี่ยนแปลงสัญญา ยกเลิกสัญญา หรือ มีการเปลี่ยนแปลงบุคคลที่เข้าปฏิบัติงานของ Vendor พนักงานผู้ติดต่อประสานงาน ผู้ดูแลระบบที่เกี่ยวข้อง หรือ พนักงานที่ได้รับมอบหมาย ต้องทำการควบคุมดูแลให้มีการส่งคืนทรัพย์สินต่างๆ ของบริษัทฯ และ เพิกถอนสิทธิในการเข้าระบบต่างๆ อย่างเหมาะสม
- การดำเนินการเปลี่ยนแปลงใดๆ ของ Vendor ที่อาจส่งผลกระทบต่อการให้บริการตามข้อตกลงหรือสัญญากับทางบริษัทฯ Vendor ต้องแจ้งต่อทางบริษัทฯ อย่างเป็นลายลักษณ์อักษรล่วงหน้าอย่างน้อย 30 วัน เพื่อให้บริษัทฯทำการพิจารณา วิเคราะห์ผลกระทบ ประเมินความเสี่ยงที่อาจเกิดขึ้น และหาวิธีในการแก้ไขควบคุมความเสี่ยงอย่างเหมาะสม

2.2. การดำเนินงานร่วมกับลูกค้าและคู่ค้า

- การเข้าใช้งานข้อมูลและระบบเทคโนโลยีสารสนเทศโดยลูกค้าและคู่ค้า ต้องได้รับการควบคุมและกำหนดข้อพึงปฏิบัติด้านความมั่นคงอย่างเหมาะสม และต้องชี้แจงข้อพึงปฏิบัติและเงื่อนไขการเข้าใช้งานให้ลูกค้าและคู่ค้ารับทราบก่อนอนุญาตให้เข้าใช้งาน โดยข้อพึงปฏิบัติและเงื่อนไขควรครอบคลุม
  1. ระบุข้อมูล, ระบบเทคโนโลยีสารสนเทศ หรือพื้นที่ที่อนุญาตให้ลูกค้าและคู่ค้าเข้าใช้งานอย่างชัดเจน
  2. ระบุกฎระเบียบ, นโยบาย, ขั้นตอนการปฏิบัติงาน และวิธีการปฏิบัติงานต่างๆ ของบริษัทฯ ที่เกี่ยวข้องอย่างเหมาะสม
  3. ระบุวิธีในการควบคุมการเข้าถึงและใช้งาน เช่นการใช้งาน User Account และรหัสผ่าน รวมถึงสิทธิในการเข้าถึงและใช้งานของลูกค้าและคู่ค้า
  4. ระบุวิธีในการรายงานเมื่อพบสิ่งผิดปกติ
  5. ระบุถึงสิทธิของบริษัทฯในการตรวจสอบ และเพิกถอนสิทธิของลูกค้าและคู่ค้า
- ข้อพึงปฏิบัติและเงื่อนไขการเข้าใช้งานข้อมูลและระบบเทคโนโลยีสารสนเทศโดยลูกค้าและคู่ค้าต้องได้รับการทบทวนโดยสายงานบริหารความมั่นคงปลอดภัยระบบสารสนเทศหรือผู้ที่ได้รับมอบหมายอย่างเหมาะสม

- การเข้าใช้งานข้อมูลและระบบเทคโนโลยีสารสนเทศโดยลูกค้าและคู่ค้า ต้องได้รับการตรวจสอบอย่างเหมาะสม เพื่อป้องกันการลักลอบแก้ไข เปลี่ยนแปลง หรือกระทำใดๆ ที่อาจก่อให้เกิดความเสียหายต่อข้อมูลและระบบเทคโนโลยีสารสนเทศของบริษัทฯ

3. การทบทวนและปรับปรุงนโยบาย

นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศทั้งหมด รวมถึงระเบียบและคำสั่งต่างๆ ที่เกี่ยวข้อง ต้องได้รับการทบทวนและประเมินผลเพื่อปรับปรุงเนื้อหา หรือยืนยันเนื้อหาเดิมโดยผู้บริหารอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าเนื้อหาของนโยบายยังคงไว้ซึ่งความครบถ้วนสมบูรณ์ มีประสิทธิภาพ และสามารถนำไปใช้งานได้อย่างเหมาะสม

4. บทลงโทษ

การละเมิด ฝ่าฝืน ละเลย หรือไม่ปฏิบัติตามนโยบาย ตลอดจนวิธีการปฏิบัติงาน และเอกสารสนับสนุนต่างๆ ที่เกี่ยวข้อง ไม่ว่าโดยเจตนาหรือไม่ก็ตาม ถือเป็นความผิดทางวินัย ซึ่งจะต้องพิจารณาลงโทษทางวินัยตามกฎระเบียบของบริษัทฯ และหากการละเมิดหรือฝ่าฝืนนโยบายนั้นเข้าข่ายการกระทำที่ผิดกฎหมาย ผู้ละเมิดต้องได้รับการดำเนินคดีตามที่กฎหมายระบุไว้

5. เอกสารอ้างอิง

1. Third Party Code of Conduct

End of Document