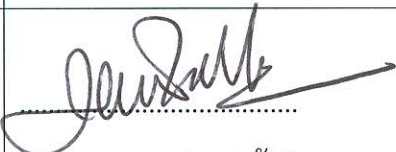




นโยบายเทคโนโลยีสารสนเทศ

บริษัท บริการเชื้อเพลิงการบินกรุงเทพ จำกัด (มหาชน)

จัดทำครั้งที่	1.0
วันที่มีผลบังคับใช้	วันที่ 8 พฤศจิกายน 2560
อนุมัติโดย	มติคณะกรรมการบริษัท ในการประชุมครั้งที่ 4/2560 วันที่ 8 พฤศจิกายน 2560
	 (นายพลากร สุวรรณรัฐ) ประธานกรรมการบริษัท

สารบัญ

	หน้า
1. หลักการและเหตุผล	1
2. วัตถุประสงค์	1
3. ขอบเขตการบังคับใช้	1
4. คำจำกัดความ	1
5. บทบาทหน้าที่และความรับผิดชอบ	3
6. นโยบายการจัดสรรและบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศ	3
7. นโยบายการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ	4
8. นโยบายความมั่นคงปลอดภัยสารสนเทศของบริษัท	5
9. การควบคุมภายในสำหรับการปฏิบัติงานให้เป็นไปตามนโยบายฯ	6

1. หลักการและเหตุผล

บริษัท บริการเชื่อเพลิงการบินกรุงเทพ จำกัด (มหาชน) ตระหนักถึงความสำคัญของการนำเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการธุรกิจ จึงกำหนดนโยบายฉบับนี้เพื่อให้บริษัทมีกรอบการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี โดยอ้างอิงหลักการจากหลักเกณฑ์และแนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศ แนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ของสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ตลอดจนกฎหมายอื่นที่เกี่ยวข้อง มาปรับใช้ให้เหมาะสมกับบริบทการดำเนินธุรกิจของบริษัท ซึ่งกำหนดนโยบายการดำเนินการด้านเทคโนโลยีสารสนเทศของบริษัท ดังนี้

- 1) นโยบายการจัดสรรและบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศ
- 2) นโยบายการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- 3) นโยบายรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

2. วัตถุประสงค์

เพื่อให้บริษัทมีกรอบการกำกับดูแลและการบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กร ที่สอดคล้องกับความต้องการของกิจการ รวมทั้งดูแลให้มีการนำเทคโนโลยีสารสนเทศมาใช้ในการสนับสนุนและพัฒนากิจการดำเนินธุรกิจ การบริหารความเสี่ยง รวมถึงเพื่อให้กิจการสามารถบรรลุวัตถุประสงค์และเป้าหมายหลักของกิจการ โดยมีการใช้ทรัพยากรและการบริหารจัดการความเสี่ยงอย่างเหมาะสม สอดคล้องกับการกำกับดูแลกิจการที่ดี

3. ขอบเขตการบังคับใช้

นโยบายฉบับนี้มีผลบังคับใช้กับบริษัท บริการเชื่อเพลิงการบินกรุงเทพ จำกัด (มหาชน) โดยนโยบายหลักเกณฑ์ ระเบียบปฏิบัติและคำสั่งที่ใช้อีกก่อนนโยบายฉบับนี้ ให้ยังมีผลใช้บังคับต่อไปเท่าที่ไม่ขัดหรือแย้งกับนโยบายฉบับนี้

4. คำจำกัดความ

คำศัพท์	คำนิยาม
บริษัท	บริษัท บริการเชื่อเพลิงการบินกรุงเทพ จำกัด (มหาชน)
บริษัทย่อย	บริษัทหรือนิติบุคคลที่ บริษัท บริการเชื่อเพลิงการบินกรุงเทพ จำกัด (มหาชน) ถือหุ้นมากกว่าร้อยละ 50
คณะกรรมการบริษัท	คณะกรรมการของบริษัท บริการเชื่อเพลิงการบินกรุงเทพ จำกัด (มหาชน)
ฝ่ายบริหาร	กรรมการผู้จัดการและผู้อำนวยการฝ่ายต่าง ๆ ของบริษัท
นโยบาย ฯ	นโยบายเทคโนโลยีสารสนเทศ

คำศัพท์	คำนิยาม
หน่วยงานเทคโนโลยีสารสนเทศ	หน่วยงานตามโครงสร้างของบริษัทที่มีหน้าที่รับผิดชอบงานด้านเทคโนโลยีสารสนเทศ และวิศวกรรมระบบเทคโนโลยีสารสนเทศ
ผู้ใช้งาน	พนักงานประจำ พนักงานตามสัญญาจ้าง ผู้ให้บริการภายนอก คู่ค้าหรือลูกค้า
ผู้ให้บริการภายนอก	บุคคลจากภายนอกองค์กร ซึ่งผู้ประกอบการธุรกิจ ว่าจ้างเพื่อให้บริการที่เกี่ยวข้องกับระบบสารสนเทศ
ระบบเทคโนโลยีสารสนเทศ	ระบบคอมพิวเตอร์ที่หน่วยงานเทคโนโลยีสารสนเทศให้บริการ
บุคลากร	เจ้าหน้าที่หรือพนักงานภายใต้หน่วยงานเทคโนโลยีสารสนเทศ และผู้ให้บริการภายนอก
เครื่องมือ	วิธีดำเนินการจัดการด้านเทคโนโลยีสารสนเทศ
ทรัพยากรด้านเทคโนโลยีสารสนเทศ	1) ระบบเทคโนโลยีสารสนเทศ 2) บุคลากร 3) อุปกรณ์คอมพิวเตอร์
ทรัพย์สินสารสนเทศ	1) ทรัพย์สินสารสนเทศประเภทระบบ ได้แก่ ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ 2) ทรัพย์สินสารสนเทศประเภทอุปกรณ์ ได้แก่ ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด 3) ทรัพย์สินสารสนเทศประเภทข้อมูล ได้แก่ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์ 4) ทรัพย์สินสารสนเทศประเภทลิขสิทธิ์ คือ ทรัพย์สินที่เกิดการพัฒนา หรือ สิทธิในการใช้จากเจ้าของผลิตภัณฑ์
สิ่งอำนวยความสะดวกในการประมวลผลข้อมูล	อุปกรณ์ ระบบงาน หรือสภาพแวดล้อม ที่จำเป็นหรือมีส่วนช่วยให้การประมวลผลข้อมูลเป็นไปอย่างครบถ้วน ถูกต้อง และมีประสิทธิภาพ เช่น อุปกรณ์หรือโปรแกรมประมวลผลข้อมูล ระบบเครือข่ายคอมพิวเตอร์ ขึ้นตอน หรือสถานที่ประมวลผลข้อมูล

5. บทบาทหน้าที่และความรับผิดชอบ

5.1 คณะกรรมการบริษัท

- 5.3.1 กำหนดนโยบายเทคโนโลยีสารสนเทศของบริษัท
- 5.3.2 กำกับดูแลให้ฝ่ายบริหารปฏิบัติตามนโยบายฯ ให้สอดคล้องกับความต้องการของบริษัท รวมทั้งสนับสนุนและพัฒนาการดำเนินธุรกิจ การบริหารความเสี่ยง เพื่อให้สามารถบรรลุวัตถุประสงค์และเป้าหมายหลักของบริษัท
- 5.3.3 ทบทวนหรือปรับปรุงนโยบายฯ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีเหตุการณ์ใด ๆ ซึ่งอาจส่งผลกระทบต่อการทำงานของฝ่ายบริหารจัดการเทคโนโลยีสารสนเทศอย่างมีนัยสำคัญ

5.2 ฝ่ายบริหาร

- 5.2.1 กำหนดแนวปฏิบัติ หลักเกณฑ์ และระเบียบปฏิบัติที่เกี่ยวข้องกับนโยบาย ฯ
- 5.2.2 ติดตามควบคุมและกำกับดูแลให้หน่วยงานที่เกี่ยวข้องดำเนินการตามนโยบายฯที่กำหนด

5.3 หน่วยงานเทคโนโลยีสารสนเทศ

- 5.3.1 ติดตามดูแลให้ผู้ใช้งานปฏิบัติตาม นโยบายฯ หลักเกณฑ์ระเบียบปฏิบัติของบริษัทที่เกี่ยวข้อง อย่างถูกต้องเหมาะสม และหากมีการปฏิบัติที่ไม่ถูกต้องให้รายงานต่อฝ่ายบริหารทราบ
- 5.3.2 สื่อสารนโยบายฯ ให้แก่ผู้ใช้งาน ผู้ประกอบธุรกิจที่เกี่ยวข้องอย่างทั่วถึงในลักษณะที่สามารถเข้าถึงได้ง่าย เพื่อให้บุคลากรดังกล่าวเข้าใจและสามารถปฏิบัติตาม นโยบายดังกล่าวได้อย่างถูกต้อง

6. นโยบายการจัดสรรและบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศ

บริษัทกำหนดให้การจัดสรรและบริหาร ทรัพยากรด้านเทคโนโลยีสารสนเทศต้องมีความสอดคล้องกับแผนกลยุทธ์องค์กร เพื่อให้บรรลุเป้าหมายตามภารกิจ กลยุทธ์และแผนการดำเนินงานที่กำหนดไว้ โดยมีการปฏิบัติ ดังนี้

- 1) กำหนดหลักเกณฑ์และปัจจัยในการจัดลำดับความสำคัญของแผนงานด้านเทคโนโลยีสารสนเทศ เช่น ความเหมาะสมสอดคล้องกับแผนกลยุทธ์ของบริษัท ผลกระทบต่อการดำเนินธุรกิจ ความเร่งด่วนในการใช้งาน เป็นต้น
- 2) จัดทำและอนุมัติงบประมาณด้านเทคโนโลยีสารสนเทศที่สอดคล้องกับแผนงบประมาณและแผนกลยุทธ์องค์กร
- 3) จัดให้มีทรัพยากรบุคคลอย่างเพียงพอต่องานด้านเทคโนโลยีสารสนเทศ จัดให้มีหรือการพัฒนาทักษะของบุคลากร และจัดจ้างบุคลากรด้านเทคโนโลยีสารสนเทศจากภายนอก
- 4) จัดการความเสี่ยงในกรณีที่ไม่สามารถจัดสรรทรัพยากรได้เพียงพอต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ ไม่ว่าจะเป็นบุคลากร งบประมาณหรือความต้องการใช้งานเกินกว่าที่กำหนดไว้

- 5) กำหนดหน้าที่และความรับผิดชอบของบุคลากรของหน่วยงานเทคโนโลยีสารสนเทศ ในการจัดสรร และบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศของบริษัท

7. นโยบายการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

บริษัทกำหนดให้การบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศต้องมีความสอดคล้องกับนโยบายและการบริหารความเสี่ยงองค์กร โดยมีการปฏิบัติ ดังนี้

- 1) หน่วยงานเทคโนโลยีสารสนเทศ ระบุความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT-related risk)
- 2) ประเมินความเสี่ยงซึ่งครอบคลุมถึง โอกาสหรือความถี่ที่จะเกิดความเสี่ยง และความมีนัยสำคัญหรือผลกระทบที่จะเกิดขึ้น
- 3) กำหนดตัวชี้วัดระดับความเสี่ยงสำหรับความเสี่ยงสำคัญที่สอดคล้องกับความเสี่ยงที่ระบุตามข้อ 1) รวมถึงจัดให้มีการติดตามและรายงานผลตัวชี้วัดดังกล่าว เพื่อให้สามารถบริหารและจัดการความเสี่ยงได้อย่างเหมาะสมและทันต่อเหตุการณ์
- 4) กำหนดหน้าที่และความรับผิดชอบของผู้รับผิดชอบ และผู้ทำหน้าที่ ในการบริหารและจัดการ ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

7.1 การบริหารความต่อเนื่องทางธุรกิจของบริษัท

บริษัทกำหนดให้การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศเป็นส่วนหนึ่งของการบริหารความต่อเนื่องทางธุรกิจของบริษัท เพื่อให้ระบบสารสนเทศ อยู่ในสภาพที่พร้อมใช้งานอยู่เสมอ

7.2 การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศของบริษัท

บริษัทกำหนดขั้นตอนและกระบวนการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ รวมทั้งกำหนดผู้มีหน้าที่รับผิดชอบซึ่งมีความรู้ความสามารถ และประสบการณ์ รวมถึงจัดให้มีการรายงานสถานการณ์ที่เกิดขึ้นอย่างรวดเร็วและทันต่อเหตุการณ์ ผ่านบุคคลหรือหน่วยงานที่ทำหน้าที่รับแจ้งเหตุการณ์ เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศได้รับการดำเนินการอย่างถูกต้อง มีประสิทธิภาพ ในช่วงระยะเวลาที่เหมาะสม

7.3 การบริหารจัดการทรัพย์สินของบริษัท

บริษัทจัดให้มีการระบุและกำหนดหน้าที่ความรับผิดชอบในการรักษาความมั่นคงปลอดภัยของทรัพย์สินสารสนเทศ เพื่อให้ทรัพย์สินสารสนเทศที่มีความสำคัญได้รับการป้องกันอย่างเหมาะสม ดังนี้

- 7.3.1 กำหนดบุคคลหรือหน่วยงานที่มีหน้าที่ดูแลรับผิดชอบทรัพย์สินสารสนเทศแต่ละประเภทตลอดอายุการใช้งานของทรัพย์สินดังกล่าว

- 7.3.2 กำหนดข้อปฏิบัติการใช้งานทรัพย์สินสารสนเทศที่เหมาะสม
- 7.3.3 ทบทวนหน้าที่ความรับผิดชอบที่มีต่อทรัพย์สินสารสนเทศให้สอดคล้องกับหน้าที่ของผู้ปฏิบัติงานเมื่อมีการเปลี่ยนแปลงหน้าที่และความรับผิดชอบ
- 7.3.4 ทรัพย์สินสารสนเทศประเภทระบบหรืออุปกรณ์ ต้องมีการจัดทำและจัดเก็บทะเบียนทรัพย์สินดังกล่าว ตลอดจนทบทวนทะเบียนดังกล่าวอย่างน้อยปีละ 1 ครั้งหรือเมื่อมีการเปลี่ยนแปลงทรัพย์สินสารสนเทศอย่างมีนัยสำคัญด้วย

8. นโยบายความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

บริษัทกำหนดนโยบายความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ โดยคำนึงถึงลักษณะ ขนาด และความซับซ้อนของการประกอบธุรกิจ รวมทั้งกฎเกณฑ์ต่าง ๆ ที่เกี่ยวข้อง เพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และได้รับทราบถึงหน้าที่ความรับผิดชอบและแนวทางปฏิบัติในการควบคุมความเสี่ยงต่าง ๆ ซึ่งกำหนดแนวทางการดำเนินการของบริษัทดังต่อไปนี้

8.1 การบริหารจัดการทรัพย์สินของบริษัท

- 8.1.1 ควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ เพื่อควบคุมการเข้าถึงข้อมูลและ สิ่งอำนวยความสะดวกในการประมวลผลข้อมูล
- 8.1.2 สร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม เพื่อป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึงสถานที่ตั้งของระบบเครือข่ายคอมพิวเตอร์ ซึ่งอาจก่อให้เกิดความเสียหายต่ออุปกรณ์สารสนเทศหรือมีผลกระทบต่อข้อมูลที่เป็นความลับหรือมีความสำคัญ

8.2 การจัดการข้อมูลสารสนเทศและการรักษาความลับ

- 8.2.1 สำรองข้อมูลเพื่อป้องกันการสูญหายของข้อมูล
- 8.2.2 ควบคุมการเข้ารหัสข้อมูลเพื่อให้การใช้งานระบบการเข้ารหัสข้อมูลมีความเหมาะสม มีประสิทธิภาพ และสามารถป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลที่เป็นความลับหรือมีความสำคัญ
- 8.2.3 ควบคุมระดับการเข้าถึงระบบเทคโนโลยีสารสนเทศ ตามหน้าที่ และความรับผิดชอบ

8.3 การควบคุมดูแลบุคลากรและผู้ใช้งาน

กำหนดข้อปฏิบัติของพนักงานในการใช้งานเครือข่ายคอมพิวเตอร์

8.4 การควบคุมดูแลผู้ให้บริการภายนอก

- 8.4.1 ควบคุมความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอกเพื่อป้องกันทรัพย์สินสารสนเทศของบริษัทจากการเข้าถึงอย่างไม่เหมาะสมโดยผู้ให้บริการภายนอก

8.4.2 ควบคุมการส่งมอบงานของผู้ให้บริการภายนอก ให้เป็นไปตามข้อตกลงที่จัดทำไว้กับผู้ประกอบธุรกิจ

8.5 การป้องกันภัยคุกคามต่อระบบสารสนเทศ

กำหนดการป้องกันโปรแกรมไม่ประสงค์ดี เพื่อให้มั่นใจว่าระบบสารสนเทศได้รับการป้องกันภัยคุกคามจากโปรแกรมไม่ประสงค์ดี

8.6 การพัฒนาและดูแลรักษาระบบสารสนเทศ

กำหนดให้มีการรักษาความมั่นคงปลอดภัยในกระบวนการพัฒนาระบบสารสนเทศ เพื่อให้การพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศประ มวลผลได้อย่างถูกต้อง ครบถ้วนและเป็นไปตามความต้องการของ ผู้ใช้งาน รวมถึงการรักษาไว้ซึ่งความมั่นคงปลอดภัยของระบบสารสนเทศตลอดช่วงการพัฒนา ระบบงานสารสนเทศ

9. การควบคุมภายในสำหรับการปฏิบัติงานให้เป็นไปตามนโยบายฯ

บริษัทจัดให้มีรอบการตรวจสอบระบบสารสนเทศโดยผู้เชี่ยวชาญภายนอกที่เป็นอิสระ