



แนวปฏิบัติที่ว่าด้วย การบริหารจัดการความเสี่ยง จากบุคคลภายนอก

ศูนย์กำกับดูแลและตรวจสอบธุรกิจ
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
เวอร์ชัน 1.0 | มิถุนายน 2566

Version History

Version	Date	Description	Revised By
1.0	มิ.ย. 2566	แนวปฏิบัติว่าด้วยการบริหารจัดการความเสี่ยงจากบุคคลภายนอก สำหรับธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล	ศูนย์กำกับดูแลและตรวจสอบธุรกิจ สพธอ.

สารบัญ

หลักการ.....	4
ขอบเขตของแนวปฏิบัติ	4
แนวปฏิบัติว่าด้วยการบริหารจัดการความเสี่ยงจากบุคคลภายนอก	5
ส่วนที่ 1 : บททั่วไป.....	5
1. คำจำกัดความ	5
2. หลักการในการบริหารจัดการความเสี่ยงจากบุคคลภายนอก	6
ส่วนที่ 2 : การกำกับดูแลการบริหารจัดการความเสี่ยงจากบุคคลภายนอก (Risk governance).....	6
3. บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการ หรือผู้บริหารระดับสูง หรือบุคลากรที่ได้รับมอบหมาย.....	6
4. การจัดโครงสร้างองค์กรและหน้าที่ความรับผิดชอบ.....	7
5. การบริหารจัดการบุคลากรที่เกี่ยวข้อง.....	7
6. การคุ้มครองผู้ใช้บริการ.....	7
7. นโยบายการบริหารจัดการความเสี่ยงจากบุคคลภายนอก.....	8
8. การตรวจสอบ	8
ส่วนที่ 3 : การบริหารจัดการความเสี่ยงจากบุคคลภายนอก (Third party risk management).....	9
9. การประเมินความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก	9
10. การคัดเลือกบุคคลภายนอก	9
11. การจัดทำสัญญาหรือข้อตกลงการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก.....	10
12. การติดตามผลการปฏิบัติงานของบุคคลภายนอก	10
13. การยกเลิกและการสิ้นสุดสัญญาหรือข้อตกลง	10
14. การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก	11

หลักการ

ด้วยการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลมีการนำเทคโนโลยีสารสนเทศมาใช้เป็นกลไกหลักในการดำเนินธุรกิจ ซึ่งผู้รับใบอนุญาตอาจมีการใช้บริการจากบุคคลภายนอกเพื่อสนับสนุนการดำเนินงาน ตลอดจนมีการเชื่อมโยงหรือแลกเปลี่ยนข้อมูลกับบุคคลภายนอกมากขึ้นเพื่อเพิ่มศักยภาพในการดำเนินธุรกิจ สำนักงาน จึงเห็นถึงความจำเป็นและตระหนักถึงความเสี่ยงที่อาจเกิดขึ้นจากการใช้บริการจากบุคคลภายนอก

เพื่อให้การควบคุมดูแลการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลในมิติของการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของระบบการให้บริการมีความครอบคลุมเข้มแข็ง และรัดกุมตามมาตรฐานสากล สพธอ. จึงได้จัดทำแนวปฏิบัติว่าด้วยการบริหารจัดการความเสี่ยงจากบุคคลภายนอก (Third Party Risk Management Guideline) (แนวปฏิบัติฯ) ขึ้นเพื่อให้ผู้รับใบอนุญาตประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลใช้เป็นแนวทางในการบริหารจัดการความเสี่ยงจากการใช้บริการบุคคลภายนอกให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ บนพื้นฐานของความรับผิดชอบต่อการดำเนินธุรกิจและการให้บริการ เพื่อคงไว้ซึ่งความน่าเชื่อถือ ประสิทธิภาพ และความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของระบบการให้บริการสำหรับธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต

ขอบเขตของแนวปฏิบัติ

แนวปฏิบัติฯ ฉบับนี้ ครอบคลุมบุคคลภายนอกใน 3 กรณี ได้แก่

- (1) การใช้บริการจากผู้ให้บริการด้านเทคโนโลยีสารสนเทศ (IT Outsourcing) เช่น การใช้บริการ Cloud Computing การใช้บริการ Software
- (2) การเชื่อมต่อระบบเทคโนโลยีสารสนเทศกับบุคคลภายนอก เช่น การเชื่อมต่อระบบเทคโนโลยีสารสนเทศของผู้รับใบอนุญาตกับพันธมิตรทางธุรกิจเพื่อประโยชน์ในการให้บริการ
- (3) การให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญ หรือเข้าถึงข้อมูลผู้ให้บริการของระบบการให้บริการ

ทั้งนี้ “บุคคลภายนอก” ไม่ครอบคลุมถึงผู้ให้บริการของผู้รับใบอนุญาต ซึ่งมีการดูแลความมั่นคงปลอดภัยสารสนเทศของระบบการให้บริการตามหลักเกณฑ์ด้านการรักษาความมั่นคงปลอดภัยของระบบการให้บริการสำหรับธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาตแล้ว

แนวปฏิบัติว่าด้วยการบริหารจัดการความเสี่ยงจากบุคคลภายนอก

ผู้ประกอบการธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาตสามารถนำแนวปฏิบัติฯ ฉบับนี้ไปพิจารณาประยุกต์ใช้กับการบริหารจัดการบุคคลภายนอก โดยพิจารณาให้เหมาะสมและสอดคล้องตามขอบเขตการให้บริการ ระดับความเสี่ยงและนัยสำคัญของการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลของบุคคลภายนอก

ส่วนที่ 1 : บททั่วไป

1. คำจำกัดความ

“ผู้รับใบอนุญาต” หมายความว่า ผู้ประกอบธุรกิจที่ได้รับใบอนุญาตให้ประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลตามกฎหมายว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต

“ผู้ใช้บริการ” หมายความว่า ผู้ขอใช้บริการพิสูจน์ตัวตน บริการออกและบริหารจัดการสิ่งที่ยืนยันตัวตน บริการยืนยันตัวตน หรือบริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล เช่น ประชาชน นิติบุคคลที่มาขอใช้บริการ ทั้งนี้ขึ้นอยู่กับลักษณะของบริการของผู้รับใบอนุญาตแต่ละราย

“บุคคลภายนอก” หมายความว่า บุคคลหรือนิติบุคคลภายนอก ซึ่งเป็นผู้ให้บริการด้านเทคโนโลยีสารสนเทศหรือเป็นผู้ที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของผู้รับใบอนุญาต หรือเป็นผู้ที่สามารถเข้าถึงข้อมูลสำคัญของผู้รับใบอนุญาตหรือข้อมูลของผู้ใช้บริการของระบบการให้บริการ รวมถึงผู้รับดำเนินการแทนผู้รับใบอนุญาต ทั้งนี้ บุคคลภายนอกไม่ครอบคลุมถึงผู้ใช้บริการซึ่งเป็นผู้ใช้งานระบบการให้บริการของผู้รับใบอนุญาต

“การใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก” หมายความว่า การใช้บริการจากผู้ให้บริการด้านเทคโนโลยีสารสนเทศ (IT Outsourcing) หรือการเชื่อมต่อบริษัทเทคโนโลยีสารสนเทศกับบุคคลภายนอก หรือการที่บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญของผู้รับใบอนุญาต หรือข้อมูลของผู้ใช้บริการที่ควบคุมโดยผู้รับใบอนุญาตได้ เช่น การใช้บริการศูนย์คอมพิวเตอร์และงานด้านดูแลระบบ ประมวลผล การใช้บริการ Cloud Computing จากผู้ให้บริการภายนอก การเชื่อมต่อบริษัทเทคโนโลยีสารสนเทศกับพันธมิตรทางธุรกิจเพื่อให้บริการร่วมกัน การเชื่อมต่อกับผู้ให้บริการเครือข่ายสาธารณะ การว่าจ้างบุคคลภายนอกดำเนินการเก็บรักษาข้อมูล

“ระบบการให้บริการ” หมายความว่า ระบบและเทคโนโลยีที่ใช้สำหรับการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่มีลักษณะเป็นบริการที่ต้องได้รับใบอนุญาต และหมายรวมถึงระบบงานที่เกี่ยวข้องกับการประกอบธุรกิจบริการดังกล่าวด้วย

“สำนักงาน” หมายความว่า สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

2. หลักการในการบริหารจัดการความเสี่ยงจากบุคคลภายนอก

ผู้รับใบอนุญาตต้องจัดให้มีการกำกับดูแลความเสี่ยง กระบวนการบริหารความเสี่ยง และการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการรักษาความปลอดภัยจากภัยไซเบอร์ สอดคล้องตามระดับความเสี่ยงและระดับความมีนัยสำคัญ ดังนี้

- (1) มีการกำหนดบทบาท หน้าที่ และความรับผิดชอบระหว่างผู้รับใบอนุญาตและบุคคลภายนอกอย่างชัดเจน และเป็นลายลักษณ์อักษร
- (2) มีการกำกับดูแล ติดตาม และบริหารจัดการความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกที่สอดคล้องตามระดับความเสี่ยงและระดับความมีนัยสำคัญของการใช้บริการ หรือการเชื่อมต่อ เพื่อให้อยู่ในระดับความเสี่ยงที่ผู้รับใบอนุญาตยอมรับได้
- (3) มีการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการรักษาความปลอดภัยจากภัยไซเบอร์ ตามมาตรฐานสากลที่ยอมรับโดยทั่วไป และตามมาตรฐานหรือแนวทางที่ผู้รับใบอนุญาตกำหนด โดยด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ครอบคลุม การรักษาความลับของระบบและข้อมูล (Confidentiality) ความถูกต้องเชื่อถือได้ของระบบและข้อมูล (Integrity) และความพร้อมใช้งานด้านเทคโนโลยีสารสนเทศ (Availability)
- (4) มีการเตรียมความพร้อมรับมือต่อเหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบต่อผู้รับใบอนุญาต อย่างมีนัยสำคัญ ต้องสามารถดำเนินธุรกิจได้อย่างต่อเนื่อง (Business continuity) และมีข้อมูลพร้อมใช้ในการดำเนินธุรกิจและให้บริการแก่ผู้ใช้บริการ (Data availability)

ส่วนที่ 2 : การกำกับดูแลการบริหารจัดการความเสี่ยงจากบุคคลภายนอก (Risk governance)

ผู้รับใบอนุญาตต้องจัดให้มีการกำกับดูแลการบริหารจัดการความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก ดังนี้

3. บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการ หรือผู้บริหารระดับสูง หรือบุคลากรที่ได้รับมอบหมาย

- 3.1 ดูแลให้การใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกสอดคล้องกับกลยุทธ์ในการดำเนินธุรกิจ มีการบริหารความเสี่ยงให้อยู่ในระดับที่ผู้รับใบอนุญาตยอมรับได้ (Risk appetite) และไม่ขัดต่อกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง
- 3.2 ดูแลให้มีนโยบายที่ครอบคลุมการบริหารจัดการความเสี่ยงจากบุคคลภายนอกซึ่งสอดคล้องกับระดับความเสี่ยงและระดับความมีนัยสำคัญของการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกอย่างชัดเจนและเป็นลายลักษณ์อักษร รวมทั้งดูแลให้มีการปฏิบัติที่สอดคล้องกับนโยบายดังกล่าว และดูแลให้มีการทบทวนและประเมินประสิทธิภาพของนโยบายและวิธีปฏิบัติดังกล่าวอย่างสม่ำเสมอ และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ
- 3.3 จัดให้มีการกำกับและควบคุมดูแลการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกให้เป็นไปตามนโยบายและวิธีปฏิบัติที่กำหนด และพิจารณาให้ความเห็นชอบต่อการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลที่มีนัยสำคัญ

4. การจัดโครงสร้างองค์กรและหน้าที่ความรับผิดชอบ

ผู้รับใบอนุญาตควรมีการจัดโครงสร้างองค์กร และจัดแบ่งหน้าที่ความรับผิดชอบเกี่ยวกับการบริหารจัดการบุคคลภายนอกอย่างเหมาะสม และสอดคล้องตามหลักการแบ่งแยกหน้าที่ความรับผิดชอบ 3 ระดับ (Three lines of defense) โดยควรพิจารณา ดังนี้

- (1) บุคลากรที่ทำหน้าที่ปฏิบัติงานกับบุคคลภายนอก ควรมีหน้าที่ครอบคลุมการประเมินความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก ก่อนเริ่มหรือต่อสัญญาอย่างเหมาะสม รวมถึงมีการติดตามการเปลี่ยนแปลงหรือเหตุการณ์ผิดปกติสำคัญอันอาจเกิดขึ้นเกี่ยวกับการเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก และรายงานต่อคณะกรรมการ หรือผู้บริหารระดับสูง หรือบุคลากรที่ได้รับมอบหมาย
- (2) บุคลากรระดับสูงหรือบุคลากรที่ได้รับมอบหมายทำหน้าที่ในการกำกับดูแลและบริหารจัดการบุคคลภายนอกให้สอดคล้องตามลักษณะการให้บริการ ปริมาณธุรกรรม และความซับซ้อนทางเทคโนโลยี เพื่อให้การให้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกมีประสิทธิภาพ โดยดูแลให้มีการบริหารจัดการความเสี่ยงและการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศตามนโยบาย มาตรฐาน และระเบียบวิธีปฏิบัติที่ผู้รับใบอนุญาตกำหนดอย่างมีประสิทธิภาพ รวมถึงการติดตามและทบทวนการบริหารจัดการความเสี่ยงอย่างสม่ำเสมอ และดูแลให้มีการปฏิบัติตามกฎหมายหรือหลักเกณฑ์ที่เกี่ยวข้อง
- (3) บุคลากรที่ทำหน้าที่ในการตรวจสอบ โดยผู้ตรวจสอบภายในหรือผู้ตรวจสอบภายนอกที่เป็นอิสระ เพื่อตรวจสอบการปฏิบัติงานที่สอดคล้องตามนโยบาย วิธีปฏิบัติ กฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง และรายงานผลการตรวจสอบต่อคณะกรรมการหรือผู้บริหารระดับสูงของผู้รับใบอนุญาต

5. การบริหารจัดการบุคลากรที่เกี่ยวข้อง

ผู้รับใบอนุญาตควรจัดสรรบุคลากรที่มีความรู้ความเข้าใจ รวมถึงพัฒนาความรู้ความเชี่ยวชาญของบุคลากรที่ปฏิบัติงานรองรับการให้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกอย่างมีประสิทธิภาพ

6. การคุ้มครองผู้ใช้บริการ

- 6.1 ดูแลและบริหารจัดการบุคคลภายนอกในการเข้าถึง การใช้ และการดูแลรักษาข้อมูลผู้ใช้บริการอย่างรัดกุม เพื่อให้ข้อมูลของผู้ใช้บริการได้รับการดูแลอย่างปลอดภัย โดยคำนึงถึงความเป็นส่วนตัว และเป็นไปตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง เช่น กฎหมายคุ้มครองข้อมูลส่วนบุคคล
- 6.2 ดูแลการแก้ไขปัญหาและจัดการเรื่องร้องเรียนให้แก่ผู้ใช้บริการอย่างเป็นธรรม และสอดคล้องตามมาตรฐานขั้นต่ำที่กำหนดในหลักเกณฑ์เกี่ยวกับการคุ้มครองผู้ใช้บริการ และมาตรการบรรเทาความเสียหายและการชดเชยหรือเยียวยาผู้ได้รับความเสียหายจากการประกอบธุรกิจ ภายใต้กฎหมายเกี่ยวกับการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนที่ต้องได้รับใบอนุญาต

7. นโยบายการบริหารจัดการความเสี่ยงจากบุคคลภายนอก

- 7.1 ผู้รับใบอนุญาตต้องกำหนดนโยบายที่ครอบคลุมถึงการบริหารจัดการความเสี่ยงจากบุคคลภายนอกอย่างชัดเจนเป็นลายลักษณ์อักษร โดยอาจเป็นนโยบายที่จัดทำขึ้นเฉพาะหรือรวมอยู่ในนโยบายที่ผู้รับใบอนุญาตมีอยู่แล้ว
- 7.2 นโยบายการบริหารจัดการความเสี่ยงจากบุคคลภายนอกควรสอดคล้องกับนโยบายอื่นที่เกี่ยวข้องของผู้รับใบอนุญาต เช่น นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
- 7.3 นโยบายการบริหารจัดการความเสี่ยงจากบุคคลภายนอกต้องได้รับอนุมัติจากคณะกรรมการ หรือผู้บริหารระดับสูง หรือบุคลากรที่ได้รับมอบหมาย และได้รับการทบทวนอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ รวมทั้งควรจัดชี้แจงและสื่อสารนโยบายให้ผู้เกี่ยวข้องได้รับทราบอย่างทั่วถึงและควบคุมดูแลให้ปฏิบัติตามนโยบาย
- 7.4 นโยบายการบริหารจัดการความเสี่ยงจากบุคคลภายนอก ควรครอบคลุม
 - (1) โครงสร้างการกำกับดูแล บทบาทหน้าที่ของผู้เกี่ยวข้องในการกำกับดูแลและบริหารจัดการความเสี่ยงจากบุคคลภายนอก
 - (2) หลักเกณฑ์การจัดระดับความเสี่ยงและระดับความมีนัยสำคัญของการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก
 - (3) การบริหารจัดการความเสี่ยงที่ครอบคลุมวงจรการบริหารจัดการบุคคลภายนอก (Third party management life cycle) และแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่ครอบคลุมตามหลัก CIA
 - (4) หลักเกณฑ์การขออนุมัติ และการรายงานต่อคณะกรรมการ หรือผู้บริหารระดับสูง หรือบุคลากรที่ได้รับมอบหมาย
 - (5) การตรวจสอบการให้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก
 - (6) การเตรียมความพร้อมรับมือต่อเหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบต่อระบบ การให้บริการอย่างมีนัยสำคัญ เพื่อให้ผู้รับใบอนุญาตสามารถดำเนินธุรกิจได้อย่างต่อเนื่อง
 - (7) การคุ้มครองผู้ใช้บริการ
- 7.5 ควรจัดให้มีแนวทางหรือวิธีปฏิบัติเพื่อสนับสนุนการดำเนินการตามนโยบายการบริหารจัดการความเสี่ยงจากบุคคลภายนอกให้สอดคล้องกับระดับความเสี่ยงตามลักษณะการให้บริการ

8. การตรวจสอบ

ผู้รับใบอนุญาตควรดำเนินการให้สำนักงาน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบภายนอก สามารถเข้าตรวจสอบการดำเนินงาน ระบบการควบคุมภายในต่าง ๆ รวมถึงการเรียกดูข้อมูลที่เกี่ยวข้องกับการตรวจสอบการดำเนินงานของบุคคลภายนอก รวมถึงการจัดเตรียมข้อมูลที่เกี่ยวข้องกับการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกให้มีความถูกต้องและเป็นปัจจุบันให้สามารถตรวจสอบได้

ส่วนที่ 3 : การบริหารจัดการความเสี่ยงจากบุคคลภายนอก (Third party risk management)

ผู้รับใบอนุญาตต้องจัดให้มีการกำกับดูแลการบริหารจัดการความเสี่ยงจากบุคคลภายนอกอย่างเหมาะสม และสอดคล้องตามกรอบการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของผู้รับใบอนุญาต เพื่อให้ความเสี่ยงอยู่ในระดับที่ผู้รับใบอนุญาตยอมรับได้ โดยครอบคลุมกระบวนการประเมินความเสี่ยง การจัดการความเสี่ยง การติดตามและทบทวนความเสี่ยง และการรายงานความเสี่ยง

9. การประเมินความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก

9.1 ผู้รับใบอนุญาตต้องประเมินความเสี่ยงและผลกระทบทั้งก่อนการให้บริการ การเชื่อมต่อหรือการเข้าถึงจากบุคคลภายนอก และเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ รวมถึงประเมินตามรอบระยะเวลาที่สอดคล้องกับระดับความเสี่ยงและความมีนัยสำคัญของการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูล ซึ่งมีการจัดทำรายงานผลการประเมินความเสี่ยง โดยคำนึงถึงความเสี่ยงดังต่อไปนี้

- (1) ความเสี่ยงด้านกลยุทธ์ (Strategic risk)
- (2) ความเสี่ยงด้านการปฏิบัติการของบุคคลภายนอก (Operational risk)
- (3) ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (information technology risk)
- (4) ความเสี่ยงด้านชื่อเสียง (Reputation risk) เช่น ระบบการให้บริการที่ดำเนินการร่วมกับบุคคลภายนอกเกิดขัดข้อง ส่งผลกระทบต่อการให้บริการ รวมถึงชื่อเสียงและความน่าเชื่อถือของผู้ให้บริการ
- (5) ความเสี่ยงด้านการปฏิบัติตามหลักเกณฑ์ (Compliance risk)
- (6) ความเสี่ยงจากการกำกับดูแลและบริหารจัดการบุคคลภายนอกที่ไม่ครอบคลุมและรัดกุมเพียงพอ
- (7) ความเสี่ยงในกรณีบุคคลภายนอกให้บริการแก่ผู้รับใบอนุญาตอื่นหลายรายพร้อมกัน
- (8) ความเสี่ยงที่เกี่ยวข้องกับสัญญาหรือข้อตกลง เช่น ความครอบคลุม ชัดเจน และความครบถ้วนสมบูรณ์ของสัญญาหรือข้อตกลง

9.2 ผู้รับใบอนุญาตต้องจัดให้มีการควบคุมและบริหารจัดการความเสี่ยงจากบุคคลภายนอกซึ่งครอบคลุมตั้งแต่กระบวนการคัดเลือก การทำสัญญาหรือข้อตกลง การติดตามผลการปฏิบัติงาน ตลอดจนการแก้ไขเปลี่ยนแปลง ยกเลิก หรือสิ้นสุดสัญญา และการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

10. การคัดเลือกบุคคลภายนอก

ผู้รับใบอนุญาตควรกำหนดแนวทางการคัดเลือกบุคคลภายนอกอย่างชัดเจนและเหมาะสมก่อนตัดสินใจใช้บริการ โดยพิจารณาประเมินให้ครอบคลุมตามระดับความมีนัยสำคัญและความเสี่ยงที่เกี่ยวข้องกับการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก ซึ่งครอบคลุมประเด็นสำคัญดังต่อไปนี้

- (1) ความสามารถทางด้านเทคนิค ความเชี่ยวชาญ ประสบการณ์ และความพร้อมในการดำเนินงาน
- (2) การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
- (3) การบริหารจัดการความต่อเนื่องทางธุรกิจ และความพร้อมรับมือภัยหรือเหตุการณ์ต่าง ๆ
- (4) การปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง
- (5) การใช้เทคโนโลยีแบบเปิด (Open technology) เพื่อให้สามารถนำระบบไปใช้งานหรือเชื่อมโยงกับระบบอื่นได้ (Interoperability) และลดข้อจำกัดในการย้ายหรือเปลี่ยนแปลงเทคโนโลยี รวมถึงข้อจำกัดในการนำระบบหรือข้อมูลกลับมาดำเนินการเอง เช่น การใช้รูปแบบการรับส่งข้อมูลกับบุคคลภายนอกที่เป็นมาตรฐานแบบเปิด (Open standard หรือ Open source)

11. การจัดทำสัญญาหรือข้อตกลงการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก

- 11.1 ผู้รับใบอนุญาตต้องจัดทำสัญญาหรือข้อตกลงการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกอย่างเป็นลายลักษณ์อักษร และจัดเก็บสัญญาหรือข้อตกลงดังกล่าวไว้พร้อมสำหรับการตรวจสอบ หรือเมื่อร้องขอโดยสำนักงาน
- 11.2 ผู้รับใบอนุญาตต้องระบุรายละเอียดและกำหนดเงื่อนไขที่สำคัญในสัญญาหรือข้อตกลงกับบุคคลภายนอกอย่างชัดเจน โดยพิจารณาให้ครอบคลุมตามระดับความเสี่ยงและความมีนัยสำคัญของการใช้บริการการเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก ดังนี้
 - (1) ขอบเขตการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก
 - (2) บทบาท หน้าที่ และความรับผิดชอบระหว่างบุคคลภายนอก และผู้รับใบอนุญาต
 - (3) มาตรฐานการปฏิบัติงานขั้นต่ำของบุคคลภายนอก เช่น ความพร้อมใช้งานของระบบเทคโนโลยีสารสนเทศ
 - (4) แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศสำหรับการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกควรสอดคล้องกับแผนการบริหารความต่อเนื่องทางธุรกิจของผู้รับใบอนุญาต
 - (5) การติดตามและรายงานผลการปฏิบัติงานของบุคคลภายนอก
 - (6) การรักษาความปลอดภัยของข้อมูล การรักษาความลับ และความเป็นส่วนตัวของผู้ใช้บริการและผู้รับใบอนุญาต
 - (7) การทำลายข้อมูลเมื่อสิ้นสุดหรือยกเลิกการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก
 - (8) สิทธิและหน้าที่ของผู้รับใบอนุญาตในการเปลี่ยนแปลง แก้ไข ยุติหรือยกเลิกสัญญาหรือข้อตกลง
 - (9) ขอบเขตความรับผิดชอบในกรณีเกิดปัญหาหรือข้อขัดข้องในการให้บริการ เช่น การให้บริการล่าช้า หรือมีข้อผิดพลาดในการให้บริการ รวมถึงแนวทางการแก้ไขปัญหาและการชดเชยค่าเสียหายที่อาจเกิดขึ้น
 - (10) การกำหนดเงื่อนไขในสัญญาหรือข้อตกลงเกี่ยวกับการให้ผู้ตรวจสอบภายใน ผู้ตรวจสอบภายนอก และสำนักงาน มีสิทธิเข้าตรวจสอบการดำเนินการด้านเทคโนโลยีสารสนเทศของบุคคลภายนอก

12. การติดตามผลการปฏิบัติงานของบุคคลภายนอก

ผู้รับใบอนุญาตต้องจัดให้มีการติดตามผลการปฏิบัติงานของบุคคลภายนอกอย่างต่อเนื่อง โดยพิจารณาตามระดับความเสี่ยงและระดับความมีนัยสำคัญของการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก รวมถึงการรายงานเหตุการณ์ผิดปกติที่เกิดขึ้นระหว่างการดำเนินงานที่เกี่ยวข้องกับการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก

13. การยกเลิกและการสิ้นสุดสัญญาหรือข้อตกลง

ผู้รับใบอนุญาตควรประเมินผลกระทบและความเสี่ยงที่อาจเกิดขึ้นจากการยกเลิกและการสิ้นสุดสัญญาหรือข้อตกลง เพื่อให้มั่นใจได้ว่าการยกเลิกหรือสิ้นสุดสัญญาหรือข้อตกลงเป็นไปอย่างมีประสิทธิภาพและได้เตรียมความพร้อมต่อผลกระทบที่อาจเกิดขึ้น เช่น การหยุดให้บริการของระบบที่ส่งผลกระทบต่อลูกค้าหรือผู้ให้บริการ การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

14. การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในการให้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก

ผู้รับใบอนุญาตควรดูแลให้มั่นใจว่าการให้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก มีการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เป็นไปตามภายใต้หลักการดังต่อไปนี้

- (1) การรักษาความลับของข้อมูล
- (2) ความถูกต้องเชื่อถือได้ของระบบสารสนเทศ
- (3) การรักษาสภาพความพร้อมใช้งานของการให้บริการซึ่งสอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของผู้รับใบอนุญาต และสอดคล้องตามระดับความเสี่ยงและระดับความมีนัยสำคัญของการให้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก โดยครอบคลุมหัวข้ออย่างน้อยดังต่อไปนี้

14.1 การจัดทำทะเบียนการให้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกและทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง

ผู้รับใบอนุญาตต้องบริหารจัดการสินทรัพย์ด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม ครอบคลุมการจัดทำทะเบียนรายการทรัพย์สิน การปรับปรุงทะเบียนรายการทรัพย์สิน การบำรุงรักษาทรัพย์สินอย่างสม่ำเสมอ การยกเลิกและเรียกคืนทรัพย์สิน โดยทะเบียนรายการสินทรัพย์ด้านเทคโนโลยีสารสนเทศต้องมีการระบุฮาร์ดแวร์ (Hardware) ซอฟต์แวร์ (Software) ข้อมูลที่ถือครอง รวมถึงการจัดประเภทและระดับความสำคัญของข้อมูล และเจ้าของทรัพย์สิน (Owner) เป็นอย่างน้อย นอกจากนี้ ต้องมีการวางแผนรองรับทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ใกล้จะสิ้นสุดอายุการใช้งาน (End of life) หรือสิ้นสุดการให้บริการ (End of support) จากผู้ผลิตด้วย

14.2 การรักษาความมั่นคงปลอดภัยของข้อมูล (Information security)

ผู้รับใบอนุญาตต้องมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่อยู่บนอุปกรณ์ที่ใช้ปฏิบัติงาน (Data at endpoint) ข้อมูลที่อยู่ระหว่างการรับส่งผ่านเครือข่าย (Data in transit) และข้อมูลที่อยู่บนระบบงานและสื่อบันทึกข้อมูล (Data at rest) โดยครอบคลุม

- (1) แนวทางการรักษาความมั่นคงปลอดภัยของข้อมูลที่สอดคล้องตามระดับความสำคัญ ซึ่งครอบคลุมถึงการกำหนดสิทธิผู้เข้าถึงข้อมูล วิธีการรับส่ง การประมวลผล และการจัดเก็บข้อมูล และการทำลายข้อมูล
- (2) การเข้ารหัสลับข้อมูล (Cryptography) ตามระดับความสำคัญของข้อมูล รวมถึงวิธีการเข้ารหัสลับข้อมูล (Cryptographic algorithm) และการบริหารจัดการกุญแจเข้ารหัสลับ (Key management) โดยครอบคลุมทุกขั้นตอนของวงจรการบริหารจัดการกุญแจเข้ารหัสลับ (Lifecycle of cryptographic keys) ตลอดกระบวนการสร้าง แจกจ่าย จัดเก็บ ใช้งาน การสำรอง เพิกถอน การต่ออายุ รวมถึงการบันทึกและตรวจสอบกิจกรรมที่สำคัญ

14.3 การควบคุมการเข้าถึง (Access control)

- (1) มีกระบวนการควบคุมการเข้าถึงสารสนเทศอย่างเหมาะสม
- (2) กำหนดบทบาท หน้าที่ และความรับผิดชอบของผู้มีสิทธิเข้าใช้งานระบบและผู้ใช้งานที่ได้รับสิทธิสูงให้ชัดเจน
- (3) ควบคุมดูแลการให้สิทธิแก่บุคคลภายนอก โดยจำกัดสิทธิตามบทบาทหน้าที่ และความจำเป็นในการใช้งาน มีการอนุมัติการเบิกใช้งาน เพื่อไม่ให้บุคคลใดบุคคลหนึ่งปฏิบัติงานได้ตั้งแต่ต้นจนจบกระบวนการ

- (4) กำหนดวิธีการระบุและพิสูจน์ตัวตนผู้ใช้งานด้วยวิธีการที่รัดกุมเพียงพอ
 - (5) ในกรณีที่บุคคลภายนอกเชื่อมต่อเพื่อเข้าถึงระบบงานของผู้รับใบอนุญาตผ่านทางช่องทางเข้าถึงระบบงานระยะไกล (System remote access) ควรมีกระบวนการบริหารจัดการการเข้าถึงระยะไกลด้วยวิธีการที่ปลอดภัย ดังนี้
 - (5.1) มีการขออนุมัติก่อนการเข้าถึงระบบงานระยะไกล (System remote access) ของบัญชีผู้ใช้งานสิทธิสูงอย่างเคร่งครัด โดยให้ใช้เฉพาะกรณีที่มีความจำเป็นเท่านั้น และจำกัดระยะเวลาในการเข้าถึงระบบงาน
 - (5.2) มีการพิสูจน์ตัวตนผู้ใช้งานแบบ Two-Factors authentication และการเชื่อมต่อผ่าน Virtual private Network (VPN)
 - (5.3) มีการควบคุมการเข้าใช้งาน โดยจำกัดการเข้าใช้งานได้เฉพาะอุปกรณ์ที่ได้รับอนุญาตเท่านั้น หรือใช้เทคโนโลยีบริหารจัดการเครื่องคอมพิวเตอร์แบบเสมือน (Virtual desktops infrastructure) เพื่อลดความเสี่ยงจากการติด Malware หรือการเข้าถึงระบบงานที่ไม่เหมาะสม
 - (5.4) สามารถระบุและสอบทานแหล่งที่มาของอุปกรณ์หรือระบบปลายทางที่เข้าเชื่อมต่อกับระบบเครือข่ายของผู้รับใบอนุญาตแบบระยะไกล
 - (5.5) มีการสอบทานการเข้าถึงระบบงานระยะไกล โดยบัญชีผู้ใช้งานสิทธิสูงด้วยบุคคลหรือหน่วยงานที่มีความเป็นอิสระและมีความรู้ความเชี่ยวชาญเพียงพอ
 - (6) ดูแลให้บุคคลภายนอกจัดเก็บบันทึกข้อมูลประวัติของการพิสูจน์ตัวตนและการเข้าถึง (Access log) บันทึกการดำเนินงาน (Activity log) ตามระยะเวลาที่กฎหมายกำหนดโดยมีการสอบทานข้อมูลการบันทึกเหตุการณ์ตามรอบระยะเวลาที่สอดคล้องกับความเสี่ยงและความสำคัญอย่างเป็นประจำ
- 14.4 การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (Communications security)
- มีการรักษาความมั่นคงปลอดภัยของการสื่อสารข้อมูลกับบุคคลภายนอกเพื่อให้ข้อมูลที่รับส่งผ่านเครือข่ายมีความมั่นคงปลอดภัย โดยอย่างน้อยต้องมีการดำเนินการ ดังนี้
- (1) การออกแบบเครือข่ายอย่างมั่นคงปลอดภัย
 - (2) การป้องกันการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต
 - (3) การป้องกันการดักจับข้อมูล
 - (4) การรักษาความถูกต้องของข้อมูลที่รับส่งบนเครือข่าย
 - (5) การควบคุมและจัดการสิทธิการใช้ระบบสารสนเทศระยะไกล
 - (6) มาตรการป้องกันการเชื่อมต่อกับระบบเครือข่ายภายนอก
- 14.5 การบริหารจัดการการเปลี่ยนแปลง (Change management)
- (1) กำหนดกระบวนการและแนวทางบริหารจัดการการเปลี่ยนแปลงร่วมกับบุคคลภายนอกเพื่อให้ผู้รับใบอนุญาตสามารถประเมินผลกระทบและเตรียมแนวทางรองรับ เช่น เมื่อมีการเปลี่ยนแปลงระบบของผู้ให้บริการ Cloud computing และกระทบกับการให้บริการของผู้รับใบอนุญาต
 - (2) ให้บุคคลภายนอกแจ้งการเปลี่ยนแปลงด้านเทคโนโลยีสารสนเทศที่มีผลกระทบกับการให้บริการของผู้รับใบอนุญาต เพื่อให้ผู้รับใบอนุญาตได้ทราบล่วงหน้าในระยะเวลาที่ตกลงร่วมกันและสามารถพิจารณาแนวทางลดผลกระทบต่อการให้บริการ

- 14.6 การบริหารจัดการการตั้งค่าระบบ (System configuration management)
มีการกำหนดมาตรฐานการตั้งค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security baseline configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่าย มีกระบวนการควบคุมการตั้งค่าของระบบที่ใช้งานจริง มีการสอบทานการใช้มาตรฐานการตั้งค่าขั้นต่ำด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ และมีการทบทวนมาตรฐานการตั้งค่าขั้นต่ำด้านความมั่นคงปลอดภัยอย่างน้อยปีละหนึ่งครั้งหรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ
- 14.7 การบริหารจัดการขีดความสามารถของระบบ (Capacity management)
มีกระบวนการติดตาม ประเมินประสิทธิภาพและความเพียงพอของทรัพยากรด้านเทคโนโลยีสารสนเทศ ของการให้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกอย่างเพียงพอ และต่อเนื่อง ตลอดจนรายงานผลการติดตามและประเมินดังกล่าวให้คณะกรรมการ หรือผู้บริหารระดับสูง หรือบุคลากรที่ได้รับมอบหมายทราบอย่างสม่ำเสมอ
- 14.8 การจัดเก็บข้อมูลบันทึกเหตุการณ์ (Logging)
ดูแลให้มั่นใจว่าบุคคลภายนอกมีการจัดเก็บข้อมูลบันทึกเหตุการณ์ที่ครบถ้วนเพียงพอและปลอดภัย เพื่อให้ผู้รับใบอนุญาตใช้ติดตามตรวจสอบร่องรอยการเข้าถึงและการใช้งานระบบหรือข้อมูลของผู้ใช้งาน รวมทั้งใช้เป็นข้อมูลหรือหลักฐานตามที่กฎหมายกำหนด
- 14.9 การติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม (Security monitoring)
ดูแลบุคคลภายนอกให้ติดตามดูแลระบบและเฝ้าระวังภัยคุกคามอย่างรัดกุมเพียงพอและต่อเนื่อง รวมทั้งระบบหรือบริการที่มีนัยสำคัญ โดยควรมีกลไกการตรวจจับเหตุการณ์ผิดปกติที่กระทบต่อความปลอดภัยทั้งในระดับ System, Network และ Application เพื่อรับมือภัยคุกคามได้อย่างทันการณ์
- 14.10 การบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ (Vulnerability management and penetration testing)
ดูแลให้บุคคลภายนอกมีการบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ (Vulnerability management and penetration testing) ตามมาตรฐานสากลที่เป็นที่ยอมรับโดยทั่วไป และสอดคล้องกับนโยบายและแนวปฏิบัติของผู้รับใบอนุญาต โดยควรมีขอบเขตการทดสอบที่ครอบคลุมระบบทั้งหมดที่ผู้รับใบอนุญาตให้บริการหรือเชื่อมต่อกับบุคคลภายนอก
- 14.11 การสำรองข้อมูล (Data backup)
กรณีที่ผู้รับใบอนุญาตให้บริการหรือเชื่อมต่อกับบุคคลภายนอก ซึ่งมีการจัดเก็บข้อมูลของผู้รับใบอนุญาต หรือข้อมูลของผู้ให้บริการ ผู้รับใบอนุญาตควรกำหนดมาตรฐานวิธีปฏิบัติในการสำรองข้อมูลที่สอดคล้องกับนโยบายและแนวปฏิบัติของผู้รับใบอนุญาต
- 14.12 การบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ (IT incident management)
- (1) มีการระบุหน้าที่และความรับผิดชอบของผู้รับใบอนุญาต และบุคคลภายนอกอย่างชัดเจน ในการบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ รวมถึงกำหนดระดับความรุนแรงของเหตุการณ์ผิดปกติดังกล่าว และกำหนดให้แจ้งผู้รับใบอนุญาตทราบเหตุการณ์ผิดปกติที่เกิดขึ้นและเกี่ยวข้องกับผู้รับใบอนุญาตอย่างเพียงพอและทันการณ์
 - (2) กำหนดให้มีช่องทางการติดต่อสื่อสารเมื่อมีการตรวจพบและรายงานเหตุการณ์ผิดปกติ

14.13 การบริหารความต่อเนื่องทางธุรกิจ (Business continuity management)

- (1) มีแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business continuity plan) และแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (Disaster recovery plan) ที่ครอบคลุมถึงการใช้บริการการเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก โดยคำนึงถึงปัจจัยสำคัญหรือความเสี่ยงที่อาจเกิดขึ้นและส่งผลกระทบต่อหยุดชะงักจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก
- (2) ประเมินและทดสอบการปฏิบัติตามแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง และแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ เพื่อให้สามารถใช้อย่างได้จริง รวมถึงสอบทานแผนของบุคคลภายนอก เพื่อพิจารณาความสอดคล้องกับแผนของผู้รับใบอนุญาต



สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

อาคารเดอะ โนนี ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี)

ชั้น 20-22 เลขที่ 33/4 ถนนพระราม 9 แขวงห้วยขวาง

เขตห้วยขวาง กรุงเทพฯ 10310

โทรศัพท์ : 02 123 1234 | โทรสาร : 02 123 1200

     : ETDA THAILAND