ธนาคารแห่งประเทศไทย

**ประกาศธนาคารแห่งประเทศไทย**

**ที่ ๔๗ /2568**

**เรื่อง หลักเกณฑ์การกำกับดูแลให้มีกลไกให้ผู้ใช้บริการใช้สิทธิส่งข้อมูลในภาคสถาบันการเงิน**

---

**1. เหตุผลในการออกประกาศ**

เนื่องจากแนวนโยบายภูมิทัศน์ภาคการเงินไทยเพื่อเศรษฐกิจดิจิทัลและการเติบโตอย่างยั่งยืน (แนวนโยบาย Financial Landscape) ของธนาคารแห่งประเทศไทยได้วางทิศทางด้านดิจิทัลที่เปิดโอกาสให้ภาคการเงินใช้ประโยชน์จากเทคโนโลยีและข้อมูล เพื่อพัฒนานวัตกรรมและบริการทางการเงินที่สอดคล้องกับความต้องการของผู้ใช้บริการ โดยเน้นการรักษาสมดุลระหว่างการสนับสนุนนวัตกรรมเพื่อประโยชน์ของผู้ใช้บริการและการบริหารความเสี่ยงอย่างเหมาะสม ซึ่งแนวนโยบายหนึ่งที่สำคัญ คือ การเปิดกว้างให้มีการใช้ประโยชน์จากข้อมูลของผู้ใช้บริการที่ยังกระจัดกระจายอยู่กับผู้ให้บริการ และหน่วยงานต่าง ๆ อันจะทำให้ผู้ใช้บริการสามารถใช้ประโยชน์จากข้อมูลของตนเองได้มากขึ้น รวมทั้งทำให้ผู้ให้บริการทางการเงินสามารถนำข้อมูลจากหลากหลายแหล่งไปใช้ประโยชน์ในการพัฒนานวัตกรรมและบริการทางการเงิน ซึ่งจะช่วยยกระดับบริการให้มีประสิทธิภาพและตอบสนองความต้องการของผู้ใช้บริการได้ดีขึ้น นอกจากนี้ กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลมีบทบัญญัติรองรับสิทธิของเจ้าของข้อมูลส่วนบุคคลในการขอให้ส่งหรือโอนข้อมูลส่วนบุคคลของตนจากผู้ควบคุมข้อมูลส่วนบุคคลรายหนึ่งไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นได้ ดังนั้น ธนาคารแห่งประเทศไทยและหน่วยงานที่เกี่ยวข้องจึงได้ร่วมกันผลักดันให้มีกลไกที่ผู้ใช้บริการสามารถใช้สิทธิส่งข้อมูลของตนผ่านช่องทางดิจิทัลทั้งที่อยู่ในและนอกภาคสถาบันการเงิน รวมทั้งจัดทำข้อมูลให้อยู่ในรูปแบบที่สามารถอ่านหรือใช้งานโดยทั่วไปได้ด้วยเครื่องมือหรืออุปกรณ์ที่ทำงานได้โดยอัตโนมัติ (machine-readable) และสามารถส่งหรือโอนได้ด้วยวิธีอัตโนมัติทางดิจิทัล อันจะเป็นโครงสร้างพื้นฐานด้านดิจิทัลที่สำคัญสำหรับภาคการเงินและภาคส่วนอื่น ๆ ต่อไป

ธนาคารแห่งประเทศไทยจึงได้ (1) ออกหลักเกณฑ์โดยอาศัยอำนาจตามกฎหมายกำกับดูแลผู้ให้บริการทางการเงินแต่ละประเภท กำหนดให้ผู้ให้บริการทางการเงินภายใต้การกำกับของธนาคารแห่งประเทศไทยจัดทำกลไกเพื่อให้ผู้ใช้บริการสามารถใช้สิทธิส่งข้อมูลของตนผ่านช่องทางดิจิทัลได้สะดวก ปลอดภัย ไม่ถูกปิดกั้น และ (2) ประสานความร่วมมือกับหน่วยงานที่เกี่ยวข้อง[1] จัดทำมาตรฐานกลาง

---

[1] ประกอบด้วย ผู้แทนจากสมาคมธนาคารไทย สมาคมสถาบันการเงินของรัฐ สมาคมธนาคารนานาชาติ ชมรมสินเชื่อส่วนบุคคล สมาคมการค้าผู้ให้บริการชำระเงินทางอิเล็กทรอนิกส์ไทย สมาคมฟินเทคแห่งประเทศไทย สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ และผู้แทนจากหน่วยงานต่าง ๆ เป็นที่ปรึกษา

และแนวปฏิบัติเพื่อให้ใช้งานได้จริงในการรับส่งข้อมูลร่วมกัน ตามที่กฎหมายกำหนดสิทธิของเจ้าของข้อมูล อีกทั้ง ธนาคารแห่งประเทศไทยมุ่งประสงค์ให้ผู้ให้บริการทางการเงินให้บริการรับส่งข้อมูลของผู้ใช้บริการซึ่งเป็นนิติบุคคลเช่นเดียวกับบุคคลธรรมดาด้วย บนพื้นฐานที่ว่าผู้ใช้บริการที่เป็นนิติบุคคลควรจะได้รับบริการในลักษณะเดียวกันกับผู้ใช้บริการที่เป็นบุคคลธรรมดา ทั้งนี้ ในระยะแรกจะมุ่งเน้นให้ผู้ให้บริการทางการเงินที่มีข้อมูลเงินฝาก ข้อมูลสินเชื่อ และข้อมูลการชำระเงินผ่านบริการเงินอิเล็กทรอนิกส์ (e-money) และบัตรเครดิต ซึ่งเป็นข้อมูลพื้นฐานที่แสดงถึงรายรับรายจ่าย พฤติกรรมการใช้จ่ายเงิน และพฤติกรรมการชำระหนี้ของผู้ใช้บริการ อันจะเป็นประโยชน์ต่อการพัฒนานวัตกรรมหรือบริการทางการเงินให้ตอบสนองความต้องการของผู้ใช้บริการแต่ละกลุ่มได้ดีขึ้น โดยเฉพาะ (1) การเข้าถึงสินเชื่อในระบบอย่างเหมาะสม และ (2) การบริหารจัดการทางการเงินที่เหมาะกับแต่ละบุคคล โดยเฉพาะผู้ใช้บริการรายย่อยและวิสาหกิจขนาดกลางและขนาดย่อม (SMEs) ซึ่งยังเป็นช่องว่างสำคัญในการเข้าถึงบริการทางการเงินในระบบการเงินไทย รวมทั้งรองรับการต่อยอดไปยังการพัฒนาบริการอื่น ๆ ในระยะถัดไป

## 2. อำนาจตามกฎหมาย

อาศัยอำนาจตามความในมาตรา 39 มาตรา 41 มาตรา 46 มาตรา 71 และมาตรา 84 แห่งพระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. 2551 ธนาคารแห่งประเทศไทยออกหลักเกณฑ์การกำกับดูแลให้มีกลไกให้ผู้ใช้บริการใช้สิทธิส่งข้อมูลในภาคสถาบันการเงิน ให้สถาบันการเงินถือปฏิบัติตามที่กำหนดในประกาศฉบับนี้

อาศัยอำนาจตามข้อ 10 และ ข้อ 11 แห่งประกาศกระทรวงการคลัง เรื่อง กิจการที่ต้องขออนุญาตตามข้อ 5 แห่งประกาศของคณะปฏิวัติ ฉบับที่ 58 (เรื่อง ธุรกิจบัตรเครดิต) ลงวันที่ 30 กรกฎาคม 2563 ธนาคารแห่งประเทศไทยออกหลักเกณฑ์การกำกับดูแลให้มีกลไกให้ผู้ใช้บริการใช้สิทธิส่งข้อมูลในภาคสถาบันการเงิน ให้ผู้ประกอบธุรกิจบัตรเครดิตที่มิใช่สถาบันการเงินถือปฏิบัติตามที่กำหนดในประกาศฉบับนี้

อาศัยอำนาจตามข้อ 11 และ ข้อ 12 แห่งประกาศกระทรวงการคลัง เรื่อง กิจการที่ต้องขออนุญาตตามข้อ 5 แห่งประกาศของคณะปฏิวัติ ฉบับที่ 58 (เรื่อง สินเชื่อส่วนบุคคลภายใต้การกำกับ) ลงวันที่ 30 กรกฎาคม 2563 ธนาคารแห่งประเทศไทยออกหลักเกณฑ์การกำกับดูแลให้มีกลไกให้ผู้ใช้บริการใช้สิทธิส่งข้อมูลในภาคสถาบันการเงิน ให้ผู้ประกอบธุรกิจสินเชื่อส่วนบุคคลภายใต้การกำกับที่มิใช่สถาบันการเงินถือปฏิบัติตามที่กำหนดในประกาศฉบับนี้

---

ได้แก่ สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) สภาองค์กรของผู้บริโภค และสภาอุตสาหกรรมแห่งประเทศไทย

อาศัยอำนาจตามข้อ 11 และ ข้อ 12 แห่งประกาศกระทรวงการคลัง เรื่อง กิจการที่ต้องขออนุญาตตามข้อ 5 แห่งประกาศของคณะปฏิวัติ ฉบับที่ 58 (เรื่อง สินเชื่อรายย่อยเพื่อการประกอบอาชีพภายใต้การกำกับ) ลงวันที่ 30 กรกฎาคม 2563 ธนาคารแห่งประเทศไทยออกหลักเกณฑ์การกำกับดูแลให้มีกลไกให้ผู้ใช้บริการใช้สิทธิส่งข้อมูลในภาคสถาบันการเงิน ให้ผู้ประกอบธุรกิจสินเชื่อรายย่อยเพื่อการประกอบอาชีพภายใต้การกำกับที่มิใช่สถาบันการเงินถือปฏิบัติตามที่กำหนดในประกาศฉบับนี้

อาศัยอำนาจตามข้อ 9 และ ข้อ 10 แห่งประกาศกระทรวงการคลัง เรื่อง กิจการที่ต้องขออนุญาตตามข้อ 5 แห่งประกาศของคณะปฏิวัติ ฉบับที่ 58 (เรื่อง ธุรกิจระบบหรือเครือข่ายอิเล็กทรอนิกส์สำหรับธุรกรรมสินเชื่อระหว่างบุคคลกับบุคคล) ลงวันที่ 30 กรกฎาคม 2563 ธนาคารแห่งประเทศไทยออกหลักเกณฑ์การกำกับดูแลให้มีกลไกให้ผู้ใช้บริการใช้สิทธิส่งข้อมูลในภาคสถาบันการเงิน ให้ผู้ประกอบธุรกิจระบบหรือเครือข่ายอิเล็กทรอนิกส์สำหรับธุรกรรมสินเชื่อระหว่างบุคคลกับบุคคลที่มิใช่สถาบันการเงินถือปฏิบัติตามที่กำหนดในประกาศฉบับนี้

อาศัยอำนาจตามความในมาตรา 24 มาตรา 25 และมาตรา 26 แห่งพระราชบัญญัติระบบการชำระเงิน พ.ศ. 2560 ธนาคารแห่งประเทศไทยออกหลักเกณฑ์การกำกับดูแลให้มีกลไกให้ผู้ใช้บริการใช้สิทธิส่งข้อมูลในภาคสถาบันการเงิน ให้ผู้ประกอบธุรกิจบริการเงินอิเล็กทรอนิกส์ภายใต้การกำกับถือปฏิบัติตามที่กำหนดในประกาศฉบับนี้

**3. ขอบเขตการบังคับใช้**

ประกาศฉบับนี้ให้ใช้บังคับกับผู้ให้บริการทางการเงินภายใต้การกำกับของธนาคารแห่งประเทศไทย ดังนี้

3.1 สถาบันการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงินทุกแห่ง

3.2 ผู้ประกอบธุรกิจบัตรเครดิตตามประกาศกระทรวงการคลังว่าด้วยกิจการที่ต้องขออนุญาตตามข้อ 5 แห่งประกาศของคณะปฏิวัติ ฉบับที่ 58 (เรื่อง ธุรกิจบัตรเครดิต) ทุกแห่ง

3.3 ผู้ประกอบธุรกิจสินเชื่อส่วนบุคคลภายใต้การกำกับตามประกาศกระทรวงการคลังว่าด้วยกิจการที่ต้องขออนุญาตตามข้อ 5 แห่งประกาศของคณะปฏิวัติ ฉบับที่ 58 (เรื่อง สินเชื่อส่วนบุคคลภายใต้การกำกับ) ทุกแห่ง

3.4 ผู้ประกอบธุรกิจสินเชื่อรายย่อยเพื่อการประกอบอาชีพภายใต้การกำกับตามประกาศกระทรวงการคลังว่าด้วยกิจการที่ต้องขออนุญาตตามข้อ 5 แห่งประกาศของคณะปฏิวัติ ฉบับที่ 58 (เรื่อง สินเชื่อรายย่อยเพื่อการประกอบอาชีพภายใต้การกำกับ) ทุกแห่ง

3.5 ผู้ประกอบธุรกิจระบบหรือเครือข่ายอิเล็กทรอนิกส์สำหรับธุรกรรมสินเชื่อระหว่างบุคคลกับบุคคลตามประกาศกระทรวงการคลังว่าด้วยกิจการที่ต้องขออนุญาตตามข้อ 5 แห่งประกาศของคณะปฏิวัติ ฉบับที่ 58 (เรื่อง ธุรกิจระบบหรือเครือข่ายอิเล็กทรอนิกส์สำหรับธุรกรรมสินเชื่อระหว่างบุคคลกับบุคคล) ทุกแห่ง

3.6 ผู้ประกอบธุรกิจบริการเงินอิเล็กทรอนิกส์ภายใต้การกำกับตามกฎหมายว่าด้วยระบบการชำระเงินทุกแห่ง

## 4. เนื้อหา

### 4.1 คำจำกัดความ

“ผู้ให้บริการทางการเงิน” หมายความว่า ผู้ให้บริการทางการเงินภายใต้การกำกับของธนาคารแห่งประเทศไทยตามที่กำหนดในข้อ 3 ของประกาศฉบับนี้

“กลไกส่งข้อมูลทางดิจิทัล” หมายความว่า รูปแบบการส่งข้อมูลทางดิจิทัลที่ธนาคารแห่งประเทศไทยกำหนดให้ผู้ให้บริการทางการเงินต้องจัดทำหรือดำเนินการสำหรับการส่งข้อมูลแต่ละประเภท ได้แก่ (1) การจัดทำระบบดิจิทัลในการส่งข้อมูลที่ได้มาตรฐาน (2) การจัดทำช่องทางดิจิทัลในการส่งข้อมูลที่ได้มาตรฐาน และ (3) การเข้าเป็นสมาชิกบริษัทข้อมูลเครดิต แล้วแต่กรณี

“แนวปฏิบัติ” หมายความว่า แนวปฏิบัติว่าด้วยการกำกับดูแลให้มีกลไกให้ผู้ใช้บริการใช้สิทธิส่งข้อมูลในภาคสถาบันการเงินที่ออกโดยธนาคารแห่งประเทศไทย สำหรับการรับส่งข้อมูลของผู้ใช้บริการที่เป็นบุคคลธรรมดาหรือนิติบุคคล SMEs แล้วแต่กรณี

“ระบบดิจิทัลในการส่งข้อมูลที่ได้มาตรฐาน” หมายความว่า ระบบเชื่อมต่อการส่งข้อมูลจากผู้ส่งข้อมูลไปยังผู้รับข้อมูลหรือผู้ให้บริการอื่นที่สามารถรับข้อมูลตามที่กำหนดด้วยวิธีอัตโนมัติ ซึ่งเป็นไปตามแนวปฏิบัติที่ธนาคารแห่งประเทศไทยกำหนด

“ช่องทางดิจิทัลในการส่งข้อมูลที่ได้มาตรฐาน” หมายความว่า ช่องทางดิจิทัลในการส่งข้อมูลไปยังผู้ใช้บริการ ซึ่งเป็นไปตามแนวปฏิบัติที่ธนาคารแห่งประเทศไทยกำหนด

“ผู้ส่งข้อมูล” หมายความว่า ผู้มีหน้าที่ส่งข้อมูล และผู้เข้าร่วมส่งข้อมูลตามความสมัครใจตามขอบเขตของผู้ส่งข้อมูล ตามข้อ 4.3.2.1 ของประกาศฉบับนี้

“ผู้รับข้อมูล” หมายความว่า ผู้ให้บริการทางการเงินที่รับข้อมูลผ่านกลไกส่งข้อมูลทางดิจิทัล และให้รวมถึงผู้ให้บริการทางการเงินที่ประสงค์โดยชัดแจ้งว่าจะรับข้อมูลของผู้ใช้บริการที่ได้รับจากช่องทางดิจิทัลในการส่งข้อมูลที่ได้มาตรฐานอีกทอดหนึ่งตามข้อ 4.3.1 ด้วย

“สินเชื่อ” หมายความว่า การให้สินเชื่อ และการทำธุรกรรมที่มีลักษณะคล้ายการให้สินเชื่อ ตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน

“การชำระเงิน” หมายความว่า การชำระเงินผ่านบริการเงินอิเล็กทรอนิกส์ (e-money) และบัตรเครดิต

“ผู้ให้บริการรวบรวมและบริหารจัดการข้อมูลในฐานะบุคคลที่สาม” (Third Party Data Aggregator) หมายความว่า ผู้ให้บริการที่ประกอบธุรกิจรวบรวมข้อมูลของผู้ใช้บริการเพื่อให้บริการอื่นใดนอกเหนือจากการให้บริการทางการเงินของตนเอง ตามความประสงค์ของผู้ใช้บริการ

**4.2 หลักการ**

ผู้ให้บริการทางการเงินต้องจัดทำกลไกให้ผู้ใช้บริการสามารถใช้สิทธิส่งข้อมูลทางดิจิทัลของตนที่อยู่กับผู้ให้บริการทางการเงินได้อย่างสะดวก ปลอดภัย และไม่ถูกปิดกั้น เพื่อประโยชน์ในการเข้าถึงและได้รับบริการที่ดีขึ้น ภายใต้กรอบกฎหมายที่เกี่ยวข้องและหลักการ ดังนี้

4.2.1 ผู้ให้บริการทางการเงินที่เก็บข้อมูลที่มีนัยสำคัญหรือที่เป็นประโยชน์ต่อผู้ใช้บริการต้องจัดทำข้อมูลของผู้ใช้บริการและกลไกส่งข้อมูลทางดิจิทัลที่สามารถรองรับการใช้สิทธิของผู้ใช้บริการในการส่งข้อมูลได้สะดวกและปลอดภัย โดยไม่เป็นภาระต่อผู้ให้บริการทางการเงินมากเกินไป

4.2.2 ผู้ให้บริการทางการเงินและผู้ให้บริการที่อยู่ภายใต้การกำกับดูแลของหน่วยงานอื่นสามารถรับข้อมูลของผู้ใช้บริการ และนำข้อมูลดังกล่าวไปใช้พัฒนาและนำเสนอบริการที่ตอบสนองต่อความต้องการของผู้ใช้บริการ โดยเฉพาะการเข้าถึงสินเชื่อในระบบอย่างเหมาะสม และการบริหารจัดการทางการเงินที่เหมาะกับแต่ละบุคคล โดยผู้ให้บริการเหล่านี้ได้รับการกำกับดูแลให้สามารถบริหารจัดการความเสี่ยงและดูแลผู้ใช้บริการได้อย่างเหมาะสม

4.2.3 การเชื่อมต่อและการรับส่งข้อมูลระหว่างผู้ส่งข้อมูลกับผู้รับข้อมูลหรือผู้ให้บริการอื่นที่สามารถรับข้อมูลให้เป็นไปตามแนวปฏิบัติที่ธนาคารแห่งประเทศไทยกำหนด เพื่อให้การรับส่งข้อมูลได้มาตรฐาน มีประสิทธิภาพ ปลอดภัย และไม่เป็นภาระและต้นทุนเกินความจำเป็น

4.2.4 การกำหนดเงื่อนไขและค่าธรรมเนียมที่เกี่ยวข้องกับการรับส่งข้อมูลต้องไม่เป็นอุปสรรคต่อการใช้สิทธิของผู้ใช้บริการ รวมทั้งไม่เป็นอุปสรรคต่อการเข้าร่วมรับส่งข้อมูลของผู้ให้บริการ

ขณะเดียวกันการกำหนดเงื่อนไขและค่าธรรมเนียมดังกล่าวต้องไม่ทำให้เกิดการรับส่งข้อมูลมากเกินความจำเป็น และไม่ทำให้ผู้ที่เกี่ยวข้องกับการรับส่งข้อมูลกลุ่มใดหรือรายใดรับภาระมากเกินสมควร รวมถึงคำนึงถึงการส่งเสริมให้ผู้ให้บริการทั้งรับและส่งข้อมูลระหว่างกัน (reciprocity) ด้วย

4.2.5 การกำกับดูแลที่เกี่ยวข้องกับการรับส่งข้อมูลมุ่งเน้นให้ผู้ที่เกี่ยวข้องมีการดูแลและจัดการความเสี่ยงอย่างเหมาะสมทั้งในด้านการบริหารจัดการข้อมูลให้มีความมั่นคงปลอดภัย ความเป็นส่วนบุคคลของข้อมูล และบริหารจัดการด้านการคุ้มครองผู้บริโภค โดยไม่เป็นภาระต่อผู้ให้บริการทางการเงินมากเกินไป และไม่กลายเป็นเงื่อนไขที่เป็นอุปสรรคต่อการรับส่งข้อมูล

**4.3 หลักเกณฑ์**

**4.3.1 หน้าที่ของผู้ให้บริการทางการเงิน**

ผู้ให้บริการทางการเงินทุกแห่งต้องแจ้งหรือเปิดเผยให้ผู้ใช้บริการทราบถึงบทบาทของผู้ให้บริการทางการเงินในการเป็นผู้ส่งข้อมูลและผู้รับข้อมูล ภายใน 180 วันหลังประกาศมีผลใช้บังคับ โดยต้องแจ้งหรือเปิดเผยผ่านช่องทางที่สอดคล้องกับพฤติกรรมของผู้ใช้บริการ และต้องปรับปรุงข้อมูลดังกล่าวให้เป็นปัจจุบันอยู่เสมอ เพื่อให้ผู้ใช้บริการทราบและสามารถใช้สิทธิของตนได้อย่างเหมาะสม โดยต้องแจ้งหรือเปิดเผยข้อมูล ดังนี้

**(1) ข้อมูลสถานะความเป็น “ผู้ส่งข้อมูล”** โดยผู้ให้บริการทางการเงินแต่ละรายต้องแจ้งหรือเปิดเผยให้ผู้ใช้บริการทราบว่าตนเป็นผู้มีหน้าที่ส่งข้อมูล ผู้เข้าร่วมส่งข้อมูลตามความสมัครใจ หรือไม่ได้เป็นผู้ส่งข้อมูลตามประกาศฉบับนี้

**(2) ข้อมูลสถานะความเป็น “ผู้รับข้อมูล”** โดยผู้ให้บริการทางการเงินแต่ละรายต้องแจ้งหรือเปิดเผยให้ผู้ใช้บริการทราบว่าตนเป็นผู้รับข้อมูล หรือไม่ได้เป็นผู้รับข้อมูลตามประกาศฉบับนี้

นอกจากนี้ กรณีผู้ให้บริการทางการเงินดังกล่าวเป็นผู้ส่งข้อมูลหรือผู้รับข้อมูลตามประกาศฉบับนี้ ต้องเปิดเผยข้อมูลเพิ่มเติมตามที่กำหนดในหลักเกณฑ์ข้อ 4.3.4.2 (1) ด้วย

**4.3.2 ขอบเขตและหน้าที่ของผู้ส่งข้อมูล**

**4.3.2.1 ขอบเขตของผู้ส่งข้อมูล**

**(1) ผู้มีหน้าที่ส่งข้อมูล** ประกอบด้วย

**(1.1) ผู้มีหน้าที่ส่งข้อมูลสินเชื่อ** ได้แก่ ผู้ให้บริการทางการเงินทุกแห่ง[2] ที่ให้บริการสินเชื่อแก่ผู้ใช้บริการรายย่อยและ SMEs ดังนี้

**(1.1.1) ผู้มีหน้าที่ส่งข้อมูลสินเชื่อของผู้ใช้บริการที่เป็นบุคคลธรรมดา** แบ่งออกเป็น

**(ก) ผู้ให้บริการสินเชื่อแก่ผู้ใช้บริการที่เป็นบุคคลธรรมดาอย่างมีนัยสำคัญ** ได้แก่ ผู้ให้บริการทางการเงินที่มีจำนวนบัญชีสินเชื่อที่ให้แก่ผู้ใช้บริการที่เป็นบุคคลธรรมดาตั้งแต่ 100,000 บัญชี หรือ มียอดสินเชื่อคงค้างรวมที่ให้แก่ผู้ใช้บริการที่เป็นบุคคลธรรมดาตั้งแต่ 1,000 ล้านบาท โดยให้คำนวณจากค่าเฉลี่ย 12 เดือนของจำนวนบัญชีสินเชื่อ ณ สิ้นเดือน และค่าเฉลี่ย 12 เดือนของยอดสินเชื่อคงค้าง ณ สิ้นเดือน นับย้อนขึ้นไปจากเดือนที่คำนวณ

**(ข) ผู้ให้บริการสินเชื่อแก่ผู้ใช้บริการที่เป็นบุคคลธรรมดาที่ไม่เข้าข่ายตามข้อ (1.1.1) (ก)**

**(1.1.2) ผู้มีหน้าที่ส่งข้อมูลสินเชื่อของผู้ใช้บริการที่เป็นนิติบุคคล SMEs**[3] แบ่งออกเป็น

**(ก) ผู้ให้บริการสินเชื่อแก่ผู้ใช้บริการที่เป็นนิติบุคคล SMEs อย่างมีนัยสำคัญ** ได้แก่ ผู้ให้บริการทางการเงินที่มีจำนวนบัญชีสินเชื่อที่ให้แก่ผู้ใช้บริการที่เป็นนิติบุคคล SMEs ตั้งแต่ 10,000 บัญชี[4] หรือ ยอดสินเชื่อคงค้างรวมที่ให้แก่ผู้ใช้บริการที่เป็นนิติบุคคล SMEs ตั้งแต่ 10,000 ล้านบาท โดยให้คำนวณจากค่าเฉลี่ย 12 เดือนของจำนวนบัญชีสินเชื่อ ณ สิ้นเดือน และค่าเฉลี่ย 12 เดือนของยอดสินเชื่อคงค้าง ณ สิ้นเดือน นับย้อนขึ้นไปจากเดือนที่คำนวณ

**(ข) ผู้ให้บริการสินเชื่อแก่ผู้ใช้บริการที่เป็นนิติบุคคล SMEs ที่ไม่เข้าข่ายตามข้อ (1.1.2) (ก)**

**(1.2) ผู้มีหน้าที่ส่งข้อมูลเงินฝาก** ได้แก่ ผู้ให้บริการทางการเงินที่ให้บริการเงินฝากแก่ผู้ใช้บริการรายย่อยและ SMEs อย่างมีนัยสำคัญ ดังนี้

---

[2] ได้แก่ สถาบันการเงิน ผู้ประกอบธุรกิจบัตรเครดิต ผู้ประกอบธุรกิจสินเชื่อส่วนบุคคลภายใต้การกำกับ ผู้ประกอบธุรกิจสินเชื่อรายย่อยเพื่อการประกอบอาชีพภายใต้การกำกับ และผู้ประกอบธุรกิจระบบหรือเครือข่ายอิเล็กทรอนิกส์สำหรับธุรกรรมสินเชื่อระหว่างบุคคลกับบุคคลภายใต้การกำกับ

[3] หมายถึง วิสาหกิจขนาดกลางและขนาดย่อมตามกฎหมายว่าด้วยการส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม ที่เป็นนิติบุคคลและมีวงเงินสินเชื่อ กับผู้ให้บริการทางการเงินรายหนึ่ง ๆ ไม่เกิน 500 ล้านบาท ทั้งนี้ ไม่รวมถึงตัวกลางทางการเงินและบริษัทโฮลดิ้งตามประกาศธนาคารแห่งประเทศไทยว่าด้วยหลักเกณฑ์การกำกับดูแลโครงสร้างและขอบเขตธุรกิจของกลุ่มธุรกิจทางการเงินของธนาคารพาณิชย์

[4] จำนวนบัญชีสินเชื่อที่ให้แก่นิติบุคคล SMEs คือ จำนวนบัญชีตามประเภทผลิตภัณฑ์สินเชื่อ เช่น หากผู้ใช้บริการหนึ่งราย มีบัญชีแฟ็กเตอริง 10 บัญชีให้นับรวมเป็นบัญชีประเภทแฟ็กเตอริงจำนวน 1 บัญชี

**(1.2.1) ผู้มีหน้าที่ส่งข้อมูลเงินฝากของผู้ใช้บริการที่เป็นบุคคลธรรมดา** ได้แก่ ผู้ให้บริการทางการเงินที่มีจำนวนบัญชีเงินฝากของผู้ใช้บริการที่เป็นบุคคลธรรมดาตั้งแต่ 100,000 บัญชี โดยให้คำนวณจากค่าเฉลี่ย 12 เดือนของจำนวนบัญชีเงินฝาก ณ สิ้นเดือน นับย้อนขึ้นไปจากเดือนที่คำนวณ

**(1.2.2) ผู้มีหน้าที่ส่งข้อมูลเงินฝากของผู้ใช้บริการที่เป็นนิติบุคคล SMEs** ได้แก่ ผู้ให้บริการทางการเงินที่เข้าข่ายเป็นผู้ที่มีหน้าที่ส่งข้อมูลสินเชื่อตามข้อ (1.1.2) (ก) และมีการให้บริการเงินฝากแก่ผู้ใช้บริการที่เป็นนิติบุคคล SMEs

**(1.3) ผู้มีหน้าที่ส่งข้อมูลการชำระเงิน** ได้แก่ ผู้ให้บริการทางการเงินที่ให้บริการการชำระเงินแก่ผู้ใช้บริการรายย่อยและ SMEs อย่างมีนัยสำคัญ ดังนี้

**(1.3.1) ผู้มีหน้าที่ส่งข้อมูลการชำระเงินผ่าน e-money** ได้แก่ ผู้ให้บริการทางการเงินที่ได้รับอนุญาตให้ประกอบธุรกิจบริการเงินอิเล็กทรอนิกส์[5] ที่มีจำนวนธุรกรรมตั้งแต่ 1 ล้านครั้งต่อปี และมีจำนวนบัญชีเงินอิเล็กทรอนิกส์ตั้งแต่ 100,000 บัญชี โดยกรณีจำนวนธุรกรรมให้คำนวณจากผลรวมจำนวนธุรกรรม 12 เดือน จากข้อมูล 14 เดือนล่าสุด นับย้อนขึ้นไปจากเดือนที่คำนวณ โดยไม่นับรวมเดือนที่มีจำนวนธุรกรรมมากที่สุดและเดือนที่มีจำนวนธุรกรรมน้อยที่สุดในช่วงเวลา 14 เดือนดังกล่าว ส่วนกรณีจำนวนบัญชีเงินอิเล็กทรอนิกส์ ให้คำนวณจากค่าเฉลี่ย 12 เดือนของจำนวนบัญชีเงินอิเล็กทรอนิกส์ ณ สิ้นเดือน นับย้อนขึ้นไปจากเดือนที่คำนวณ

**(1.3.2) ผู้มีหน้าที่ส่งข้อมูลการชำระเงินผ่านบัตรเครดิต** ได้แก่ ผู้ให้บริการทางการเงินที่ให้บริการบัตรเครดิตที่มีจำนวนธุรกรรมตั้งแต่ 1 ล้านครั้งต่อปี โดยให้คำนวณจากผลรวมจำนวนธุรกรรม 12 เดือน จากข้อมูล 14 เดือนล่าสุด นับย้อนขึ้นไปจากเดือนที่คำนวณ โดยไม่นับรวมเดือนที่มีจำนวนธุรกรรมมากที่สุดและเดือนที่มีจำนวนธุรกรรมน้อยที่สุดในช่วงเวลา 14 เดือนดังกล่าว

ทั้งนี้ ธนาคารแห่งประเทศไทยยกเว้นการจัดส่งข้อมูลของผู้ให้บริการทางการเงินที่มีหน้าที่ส่งข้อมูลการชำระเงินตามข้อ (1.3.1) และข้อ (1.3.2) เป็นรายผลิตภัณฑ์ หากข้อมูลดังกล่าวเป็นข้อมูลการชำระเงินของผลิตภัณฑ์ที่ให้บริการในวงจำกัดตามข้อ 2.2.1 ถึงข้อ 2.2.4 ของประกาศกระทรวงการคลัง เรื่อง การกำหนดบริการการชำระเงินภายใต้การกำกับ ลงวันที่ 17 เมษายน 2561 และที่แก้ไขเพิ่มเติม นอกจากนี้ ธนาคารแห่งประเทศไทยอาจพิจารณาผ่อนผันการจัดส่งข้อมูลการชำระเงินของผลิตภัณฑ์ที่ให้บริการในวงจำกัดอื่น ๆ ของผู้ให้บริการทางการเงินดังกล่าวเพิ่มเติม

[5] หมายถึง ธุรกรรมทั้งหมดของผู้ประกอบธุรกิจ ซึ่งรวมถึงการชำระค่าสินค้าและค่าบริการ การชำระค่าสาธารณูปโภค การเติมเงิน การถอนเงิน และการโอนเงิน

เป็นรายกรณี โดยผู้ให้บริการทางการเงินต้องขออนุญาตผ่อนผัน โดยแสดงเหตุผลและความจำเป็นมายังธนาคารแห่งประเทศไทยตามที่กำหนดในคู่มือประชาชน

อนึ่ง ผู้ให้บริการทางการเงินที่มีสถานะเป็นผู้มีหน้าที่ส่งข้อมูลตามประกาศฉบับนี้แล้ว ให้ถือว่าเป็นผู้มีหน้าที่ส่งข้อมูลต่อไป แม้ว่าในภายหลังผู้ให้บริการทางการเงินนั้นจะมีลักษณะเงื่อนไขเปลี่ยนแปลงแตกต่างไปจากที่กำหนดในข้อ 4.3.2.1 (1) ก็ตาม รวมทั้งกรณีที่ผู้มีหน้าที่ส่งข้อมูลเป็นผู้ให้บริการทางการเงินอย่างมีนัยสำคัญ แต่ต่อมามีสถานะไม่เข้าข่ายเป็นผู้ให้บริการทางการเงินอย่างมีนัยสำคัญแล้ว ไม่ถือเป็นเหตุให้เปลี่ยนแปลงหรือยกเลิกกลไกส่งข้อมูลทางดิจิทัลที่ดำเนินการให้บริการแก่ผู้ใช้บริการอยู่เดิม

กรณีผู้ให้บริการทางการเงินที่เป็นผู้มีหน้าที่ส่งข้อมูลได้ปรับเปลี่ยนกลยุทธ์หรือนโยบายการดำเนินธุรกิจแบบถาวรจนทำให้ไม่เข้าข่ายเป็นผู้มีหน้าที่ส่งข้อมูลและประสงค์ที่จะหยุดการให้บริการส่งข้อมูล ให้ผู้ให้บริการทางการเงินดังกล่าวยื่นขออนุญาตหยุดการให้บริการส่งข้อมูลต่อธนาคารแห่งประเทศไทยไม่น้อยกว่า 30 วันทำการ ก่อนหยุดให้บริการ โดยต้องดำเนินการยื่นขออนุญาตตามที่ธนาคารแห่งประเทศไทยกำหนดในคู่มือประชาชน ทั้งนี้ ธนาคารแห่งประเทศไทยจะกำหนดเงื่อนไขประกอบการอนุญาตก็ได้

ในกรณีที่เห็นสมควร ธนาคารแห่งประเทศไทยอาจพิจารณากำหนดให้ผู้ให้บริการทางการเงินที่ยังไม่เข้าข่ายเป็นผู้มีหน้าที่ส่งข้อมูลตามข้อ 4.3.2.1 (1) ส่งผลการประเมินการเป็นผู้มีหน้าที่ส่งข้อมูลให้ธนาคารแห่งประเทศไทยเป็นรายกรณี เพื่อทบทวนการเข้าข่ายเป็นผู้มีหน้าที่ส่งข้อมูลดังกล่าว

**(2) ผู้เข้าร่วมส่งข้อมูลตามความสมัครใจ** ได้แก่ ผู้ให้บริการทางการเงินที่ไม่เข้าข่ายเป็นผู้มีหน้าที่ส่งข้อมูล แต่มีความพร้อมและประสงค์ที่จะจัดทำข้อมูลประเภทหนึ่งประเภทใดตาม ฉบับนี้ให้อยู่ในรูปแบบ machine-readable และจัดทำกลไกส่งข้อมูลทางดิจิทัลสำหรับส่งข้อมูลประเภทนั้นตามที่กำหนดในประกาศฉบับนี้

ในกรณีที่ผู้เข้าร่วมส่งข้อมูลตามความสมัครใจได้เริ่มนำส่งข้อมูลแล้ว และภายหลังประสงค์จะหยุดให้บริการส่งข้อมูล ต้องแจ้งให้ธนาคารแห่งประเทศไทยทราบล่วงหน้าไม่น้อยกว่า 30 วัน ก่อนหยุดให้บริการ โดยการแจ้งหยุดให้บริการให้ดำเนินการตามที่ธนาคารแห่งประเทศไทยกำหนดในคู่มือประชาชน

**4.3.2.2 หน้าที่ของผู้ส่งข้อมูล**

**(1) กรณีผู้มีหน้าที่ส่งข้อมูล**

(1.1) ผู้มีหน้าที่ส่งข้อมูลต้องจัดทำข้อมูลเงินฝาก ข้อมูลสินเชื่อ และข้อมูลการชำระเงินให้อยู่ในรูปแบบ machine-readable ตามรายการและมาตรฐานข้อมูลที่กำหนดในแนวปฏิบัติของธนาคารแห่งประเทศไทย และจัดทำกลไกส่งข้อมูลทางดิจิทัลสำหรับส่งข้อมูลเงินฝาก ข้อมูลสินเชื่อ และข้อมูลการชำระเงิน แล้วแต่กรณี เพื่อให้ผู้ใช้บริการสามารถใช้สิทธิส่งข้อมูลของตนทางดิจิทัลได้ ดังนี้

(ก) ผู้มีหน้าที่ส่งข้อมูลเงินฝากและการชำระเงินตามข้อ 4.3.2.1 (1.2) และ (1.3) ให้ดำเนินการผ่านระบบดิจิทัลในการส่งข้อมูลที่ได้มาตรฐาน

(ข) ผู้มีหน้าที่ส่งข้อมูลสินเชื่อตามข้อ 4.3.2.1 (1.1.1) (ก) และ (1.1.2) (ก) ให้ดำเนินการผ่านวิธีใดวิธีหนึ่งดังต่อไปนี้ 1) ระบบสำหรับสมาชิกบริษัทข้อมูลเครดิตโดยให้ส่งข้อมูลตามวิธีการที่บริษัทข้อมูลเครดิตดังกล่าวกำหนด และถือปฏิบัติตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิตและหลักเกณฑ์ที่เกี่ยวข้อง หรือ 2) ระบบดิจิทัลในการส่งข้อมูลที่ได้มาตรฐาน

(ค) ผู้มีหน้าที่ส่งข้อมูลสินเชื่อตามข้อ 4.3.2.1 (1.1.1) (ข) และ (1.1.2) (ข) ให้ดำเนินการผ่านวิธีใดวิธีหนึ่งดังต่อไปนี้ 1) ระบบสำหรับสมาชิกบริษัทข้อมูลเครดิตโดยให้ส่งข้อมูลตามวิธีการที่บริษัทข้อมูลเครดิตดังกล่าวกำหนด และถือปฏิบัติตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิตและหลักเกณฑ์ที่เกี่ยวข้อง หรือ 2) ระบบดิจิทัลในการส่งข้อมูลที่ได้มาตรฐาน หรือ 3) ช่องทางดิจิทัลในการส่งข้อมูลที่ได้มาตรฐาน

อนึ่ง ข้อมูลสินเชื่อที่ผู้มีหน้าที่ส่งข้อมูลตามข้อ 4.3.2.1 (1.1.1) และ (1.1.2) ต้องจัดส่ง ให้รวมถึงข้อมูลภาระผูกพันของผู้ใช้บริการด้วย ทั้งนี้ ตามแนวปฏิบัติที่ธนาคารแห่งประเทศไทยกำหนด

(1.2) ผู้ให้บริการทางการเงินที่มีสถานะเป็นผู้มีหน้าที่ส่งข้อมูล ณ วันที่ประกาศมีผลใช้บังคับ มีกรอบระยะเวลาในการดำเนินการดังนี้

(ก) กรณีข้อมูลเงินฝากของผู้ใช้บริการที่เป็นบุคคลธรรมดา ผู้มีหน้าที่ส่งข้อมูลต้องดำเนินการข้างต้นให้แล้วเสร็จและสามารถเริ่มส่งข้อมูลได้ภายในวันที่ 31 ธันวาคม 2569

(ข) กรณีข้อมูลเงินฝากของผู้ใช้บริการที่เป็นนิติบุคคล SMEs ผู้มีหน้าที่ส่งข้อมูลต้องดำเนินการข้างต้นให้แล้วเสร็จและสามารถเริ่มส่งข้อมูลได้ภายใน 4 ไตรมาส นับจากวันที่ธนาคารแห่งประเทศไทยออกแนวปฏิบัติสำหรับการรับส่งข้อมูลของผู้ใช้บริการที่เป็นนิติบุคคล SMEs ทั้งนี้ ต้องไม่ช้ากว่าวันที่ 31 มีนาคม 2571

(ค) กรณีข้อมูลสินเชื่อและการชำระเงินของผู้ใช้บริการที่เป็นบุคคลธรรมดา ผู้มีหน้าที่ส่งข้อมูลต้องดำเนินการข้างต้นให้แล้วเสร็จและสามารถเริ่มส่งข้อมูลได้ภายในวันที่ 31 มีนาคม 2570

(ง) กรณีข้อมูลสินเชื่อและการชำระเงินของผู้ใช้บริการที่เป็นนิติบุคคล SMEs ผู้มีหน้าที่ส่งข้อมูลต้องดำเนินการข้างต้นให้แล้วเสร็จและสามารถเริ่มส่งข้อมูลได้ภายใน 5 ไตรมาสนับจากวันที่ธนาคารแห่งประเทศไทยออกแนวปฏิบัติสำหรับการรับส่งข้อมูลของผู้ใช้บริการที่เป็นนิติบุคคล SMEs ทั้งนี้ ต้องไม่ช้ากว่าวันที่ 30 มิถุนายน 2571

สำหรับผู้ให้บริการทางการเงินที่มีสถานะเป็นผู้มีหน้าที่ส่งข้อมูลภายหลังจากวันที่ประกาศมีผลใช้บังคับ จะต้องดำเนินการจัดทำข้อมูลให้อยู่ในรูปแบบ machine-readable ตามรายการและมาตรฐานข้อมูลในแนวปฏิบัติที่ธนาคารแห่งประเทศไทยกำหนด รวมถึงจัดทำกลไกส่งข้อมูลทางดิจิทัลสำหรับส่งข้อมูลแต่ละประเภทให้แล้วเสร็จภายใน 1 ปี นับแต่วันสิ้นเดือนที่ผู้ให้บริการคำนวณแล้วว่าเข้าข่ายเป็นผู้มีหน้าที่ส่งข้อมูลหรือภายในวันที่กำหนดตามข้อ (ก) ถึงข้อ (ง) ข้างต้น แล้วแต่ระยะเวลาใดจะมากกว่า

(1.3) ผู้มีหน้าที่ส่งข้อมูลต้องถือปฏิบัติตามหลักเกณฑ์ตามข้อ 4.3.4 และข้อ 4.3.5 ในส่วนที่เกี่ยวข้องกับตน

**(2) กรณีผู้เข้าร่วมส่งข้อมูลตามความสมัครใจ**

ผู้เข้าร่วมส่งข้อมูลตามความสมัครใจต้องจัดทำข้อมูลให้อยู่ในรูปแบบ machine-readable ตามรายการและมาตรฐานข้อมูลในแนวปฏิบัติที่ธนาคารแห่งประเทศไทยกำหนด และจัดทำกลไกส่งข้อมูลทางดิจิทัลสำหรับส่งข้อมูลแต่ละประเภทตามข้อ 4.3.2.2 โดยสามารถดำเนินการดังกล่าวได้ตามความพร้อม และต้องถือปฏิบัติตามหลักเกณฑ์ที่เกี่ยวข้องตามข้อ 4.3.2.2 ข้างต้นเช่นเดียวกับผู้มีหน้าที่ส่งข้อมูล โดยผู้เข้าร่วมส่งข้อมูลตามความสมัครใจจะเริ่มส่งข้อมูลเมื่อใดก็ได้เมื่อมีความพร้อมและสามารถดำเนินการได้ตามหลักเกณฑ์ที่เกี่ยวข้องตามข้อ 4.3.2.2 แล้ว

### 4.3.3 ขอบเขตของผู้ที่สามารถรับข้อมูลและหน้าที่ของผู้รับข้อมูล

#### 4.3.3.1 ขอบเขตของผู้ที่สามารถรับข้อมูล

**(1) ผู้ให้บริการที่สามารถรับข้อมูลผ่านระบบดิจิทัลในการส่งข้อมูลที่ได้มาตรฐาน** ได้แก่

(1.1) ผู้ให้บริการทางการเงินตามประกาศธนาคารแห่งประเทศไทย ว่าด้วยหลักเกณฑ์การกำกับดูแลให้มีกลไกให้ผู้ใช้บริการใช้สิทธิส่งข้อมูลในภาคสถาบันการเงิน

(1.2) สถาบันการเงินเฉพาะกิจตามประกาศธนาคารแห่งประเทศไทย ว่าด้วยหลักเกณฑ์การกำกับดูแลให้มีกลไกให้ผู้ใช้บริการใช้สิทธิส่งข้อมูลในภาคสถาบันการเงินของสถาบันการเงินเฉพาะกิจ

(1.3) ผู้ให้บริการภายใต้การกำกับดูแลของหน่วยงานอื่น ซึ่งธนาคารแห่งประเทศไทยได้เผยแพร่รายชื่อประเภทผู้ให้บริการบนเว็บไซต์ของธนาคารแห่งประเทศไทย โดยธนาคารแห่งประเทศไทยจะพิจารณาจากการกำกับดูแลผู้ให้บริการดังกล่าวว่าอยู่ภายใต้หลักเกณฑ์และแนวทางกำกับดูแลที่มีมาตรฐานในระดับเดียวกันกับประกาศฉบับนี้[6]

ทั้งนี้ ผู้ให้บริการรวบรวมและบริหารจัดการข้อมูลในฐานะบุคคลที่สาม (Third Party Data Aggregator) ไม่ถือว่าเป็นผู้ที่สามารถรับข้อมูลตามประกาศนี้ จนกว่าธนาคารแห่งประเทศไทยจะประกาศกำหนดให้ผู้ให้บริการดังกล่าวเป็นผู้ที่สามารถรับข้อมูลได้

**(2) ผู้ที่สามารถรับข้อมูลผ่านช่องทางดิจิทัลในการส่งข้อมูลที่ได้มาตรฐาน** ได้แก่ ผู้ใช้บริการซึ่งเป็นเจ้าของข้อมูลนั้นเอง และให้รวมถึงผู้ให้บริการทางการเงินที่ประสงค์โดยชัดแจ้งว่าจะรับข้อมูลของผู้ใช้บริการที่ได้รับจากช่องทางดิจิทัลในการส่งข้อมูลที่ได้มาตรฐานอีกทอดหนึ่งตามข้อ 4.3.1 ด้วย

**(3) ผู้ที่สามารถรับข้อมูลผ่านบริษัทข้อมูลเครดิต** ได้แก่ สมาชิกหรือผู้ใช้บริการของบริษัทข้อมูลเครดิตตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

#### 4.3.3.2 หน้าที่ของผู้รับข้อมูล

ผู้รับข้อมูลต้องถือปฏิบัติตามหลักเกณฑ์ตามข้อ 4.3.4 และข้อ 4.3.5 ในส่วนที่เกี่ยวข้องกับตน ทั้งนี้ ผู้รับข้อมูลที่เป็นผู้ให้บริการภายใต้การกำกับดูแลของหน่วยงานอื่นควรถือปฏิบัติตามหลักเกณฑ์กำกับดูแลที่มีมาตรฐานในระดับเดียวกันกับข้อกำหนดดังกล่าวด้วย

---

[6] หลักเกณฑ์และแนวทางกำกับดูแลที่มีมาตรฐานในระดับเดียวกันกับประกาศฉบับนี้ครอบคลุมถึง การกำกับดูแลในด้านการรับส่งข้อมูลผ่านระบบดิจิทัลในการส่งข้อมูลที่ได้มาตรฐาน การคุ้มครองผู้บริโภคที่เกี่ยวข้องกับการรับส่งข้อมูลของผู้ใช้บริการ การบริหารจัดการข้อมูลให้มีความมั่นคงปลอดภัย รวมถึงการกำหนดเงื่อนไขและค่าธรรมเนียมที่เกี่ยวข้องกับการรับส่งข้อมูล ทั้งนี้ สำหรับการกำกับดูแลด้านการกำหนดเงื่อนไขและค่าธรรมเนียม หากหน่วยงานกำกับดูแลอื่นไม่สามารถกำหนดให้มีมาตรฐานเทียบเท่าหลักเกณฑ์ฉบับนี้ ให้หมายถึงหลักเกณฑ์ที่หน่วยงานผู้กำกับดูแลนั้น ๆ สามารถกำหนดได้ตามอำนาจทางกฎหมายของแต่ละหน่วยงานโดยอนุโลม

ผู้ที่สามารถรับข้อมูลทั้งผู้ให้บริการทางการเงินและผู้ให้บริการภายใต้การกำกับดูแลของหน่วยงานอื่นควรจัดทำกลไกส่งข้อมูลทางดิจิทัลเพื่อให้ผู้ใช้บริการสามารถใช้สิทธิส่งข้อมูลที่อยู่ในความดูแลของตนไปยังผู้ให้บริการทางการเงินและผู้ให้บริการรายอื่นได้ด้วย โดยเฉพาะข้อมูลที่มีนัยสำคัญหรือที่เป็นประโยชน์ต่อผู้ใช้บริการ ซึ่งจะสนับสนุนให้มีการแลกเปลี่ยนแบ่งปันข้อมูลอย่างครบถ้วนทั่วถึงระหว่างผู้ให้บริการในภาพรวม

### 4.3.4 หลักเกณฑ์ทั่วไปเกี่ยวกับการกำกับดูแลกลไกส่งข้อมูลทางดิจิทัล

#### 4.3.4.1 การกำหนดเงื่อนไขและค่าธรรมเนียม

**(1) เงื่อนไขที่เกี่ยวข้องกับการรับส่งข้อมูล**

ผู้ส่งข้อมูลและผู้รับข้อมูลต้องไม่กำหนดเงื่อนไขหรือดำเนินการที่เป็นอุปสรรคต่อการรับส่งข้อมูล หรือต่อการใช้ประโยชน์จากข้อมูล เช่น การกำหนดขั้นตอนการเข้าใช้บริการรับส่งข้อมูลหรือการออกแบบการใช้งานที่ยุ่งยากเกินสมควร การจำกัดระยะเวลาหรือจำนวนครั้งในการใช้งานน้อยเกินไป จนเป็นอุปสรรคต่อการใช้บริการ โดยต้องถือปฏิบัติตามแนวปฏิบัติที่ธนาคารแห่งประเทศไทยกำหนด

**(2) ค่าธรรมเนียมที่เกี่ยวข้องกับการรับส่งข้อมูลของผู้ใช้บริการ**

ผู้ส่งข้อมูลสามารถเรียกเก็บค่าธรรมเนียมที่เกี่ยวข้องกับการรับส่งข้อมูลของผู้ใช้บริการจากผู้รับข้อมูลได้เฉพาะกรณีที่ผู้รับข้อมูลมีการเรียกข้อมูลจากผู้ส่งข้อมูลสูงเกินกว่าระดับที่ธนาคารแห่งประเทศไทยประกาศกำหนด[7] ในกรณีที่การเรียกข้อมูลเกินกว่าระดับที่ธนาคารแห่งประเทศไทยกำหนดนั้นเกิดจากผู้ใช้บริการเอง ผู้ส่งข้อมูลหรือผู้รับข้อมูลอาจเรียกเก็บค่าธรรมเนียมจากผู้ใช้บริการได้ โดยห้ามเรียกเก็บค่าธรรมเนียมซ้ำซ้อนกันในการรับส่งข้อมูลแต่ละรายการ ทั้งนี้ ค่าธรรมเนียมที่จะเรียกเก็บข้างต้นต้องสะท้อนต้นทุนที่เกิดขึ้นจริงและสมควรแก่เหตุตามแนวทางที่กำหนดในเอกสารแนบ 1 โดยค่าธรรมเนียมต้องไม่สูงเกินไปจนผู้ใช้บริการจำนวนมากเลือกที่จะไม่ใช้บริการ และไม่เป็นภาระต้นทุนจนผู้รับข้อมูลจำนวนมากเลือกที่จะไม่รับข้อมูลผ่านกลไกส่งข้อมูลทางดิจิทัลเพื่อนำไปพัฒนาบริการ จนไม่สามารถบรรลุเป้าประสงค์ของประกาศฉบับนี้ รวมทั้งต้องคำนึงถึงความสมดุลระหว่างประโยชน์และต้นทุนของผู้ที่เกี่ยวข้อง โดยไม่ทำให้ผู้ที่เกี่ยวข้องกับการรับส่งข้อมูลกลุ่มใดหรือรายใดรับภาระมากจนเกินไป นอกจากนี้ ให้ทบทวนค่าธรรมเนียมเป็นระยะเพื่อให้ยังคงสอดคล้องกับหลักการที่ธนาคารแห่งประเทศไทยกำหนดข้างต้น

---

[7] ก่อนธนาคารแห่งประเทศไทยออกประกาศกำหนดระดับการใช้งานและค่าธรรมเนียมที่เกี่ยวข้อง ธนาคารแห่งประเทศไทยจะดำเนินการรับฟังความคิดเห็นและหารือร่วมกับผู้ที่เกี่ยวข้อง เช่น ผู้ส่งข้อมูลและผู้รับข้อมูล

อนึ่ง เพื่อให้มีความโปร่งใสและเป็นธรรม ในการกำหนดหรือเปลี่ยนแปลงค่าธรรมเนียมระหว่างผู้ส่งข้อมูลและผู้รับข้อมูล ผู้ส่งข้อมูลต้องมีการรับฟังความคิดเห็นจากผู้ที่เกี่ยวข้อง และใช้โครงสร้างค่าธรรมเนียมเดียวกันสำหรับผู้รับข้อมูลที่เข้าเงื่อนไขเดียวกันตามที่ธนาคารแห่งประเทศไทยจะประกาศกำหนด นอกจากนี้ ในการเรียกเก็บค่าธรรมเนียมจากผู้ใช้บริการ ผู้ส่งข้อมูลหรือผู้รับข้อมูลต้องเปิดเผยข้อมูลค่าธรรมเนียมที่เกี่ยวข้องให้ผู้ใช้บริการทราบ โดยถือปฏิบัติตามประกาศธนาคารแห่งประเทศไทยว่าด้วยการปฏิบัติและการเปิดเผยข้อมูลเกี่ยวกับดอกเบี้ย ค่าบริการ และเบี้ยปรับสำหรับผลิตภัณฑ์และบริการทางการเงิน

ทั้งนี้ สำหรับการรับส่งข้อมูลอื่นหรือรายการข้อมูลอื่น[8] นอกเหนือจากที่กำหนดในประกาศฉบับนี้ ผู้ให้บริการสามารถดำเนินการได้ตามธุรกิจปกติ

#### 4.3.4.2 การคุ้มครองผู้บริโภค

เพื่อให้ผู้ส่งข้อมูลและผู้รับข้อมูล มีการบริหารจัดการความเสี่ยงที่เกี่ยวข้องกับการใช้สิทธิส่งข้อมูลของผู้ใช้บริการและมีการคุ้มครองผู้บริโภคได้อย่างเหมาะสม โดยไม่เป็นภาระและต้นทุนต่อผู้ให้บริการมากจนเกินไป หรือเป็นเงื่อนไขที่จะเป็นอุปสรรคต่อการรับส่งข้อมูล ผู้ส่งข้อมูลและผู้รับข้อมูลต้องปฏิบัติตามหลักเกณฑ์ด้านการคุ้มครองผู้บริโภค ดังนี้

(1) ผู้ส่งข้อมูลและผู้รับข้อมูลต้องให้ข้อมูลเกี่ยวกับการให้บริการรับส่งข้อมูลแก่ผู้ใช้บริการ โดยแจ้งสถานะการให้บริการรับส่งข้อมูลที่เป็นปัจจุบันให้ผู้ใช้บริการทราบผ่านช่องทางของผู้ส่งข้อมูลและผู้รับข้อมูลที่สอดคล้องกับพฤติกรรมของผู้ใช้บริการ เพื่อให้ผู้ใช้บริการสามารถใช้สิทธิส่งข้อมูลของตนได้อย่างเหมาะสม ดังนี้

(1.1) ผู้ส่งข้อมูลและผู้รับข้อมูลต้องเปิดเผยรูปแบบกลไกส่งข้อมูลทางดิจิทัลที่จะใช้ในการรับส่งข้อมูลแต่ละประเภทแก่ผู้ใช้บริการ

(1.2) ผู้ส่งข้อมูลและผู้รับข้อมูลต้องแจ้งหรือเปิดเผยรายชื่อประเภทข้อมูลที่ผู้ใช้บริการสามารถใช้สิทธิส่งข้อมูลผ่านกลไกดังกล่าวได้

(1.3) ในกรณีที่ผู้ส่งข้อมูลจะหยุดให้บริการส่งข้อมูลตามข้อ 4.3.2.1 (1) และ (2) ผู้ส่งข้อมูลต้องแจ้งให้ผู้ใช้บริการทราบล่วงหน้าไม่น้อยกว่า 30 วัน ก่อนหยุดให้บริการส่งข้อมูล

---

[8] ข้อมูลอื่น หมายถึง ข้อมูลชุดอื่นนอกเหนือจากข้อมูลเงินฝาก สินเชื่อ และการชำระเงิน ส่วนรายการข้อมูลอื่น หมายถึง รายละเอียดข้อมูลอื่นในชุดข้อมูลเงินฝาก สินเชื่อ และการชำระเงิน ที่อยู่นอกเหนือจากที่กำหนดในแนวปฏิบัติของธนาคารแห่งประเทศไทย

(2) ผู้ส่งข้อมูลและผู้รับข้อมูลต้องปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับการคุ้มครองผู้บริโภคและความเป็นส่วนบุคคลของข้อมูลที่ใช้บังคับอยู่สำหรับผู้ให้บริการทางการเงินแต่ละประเภท[9]

(3) ก่อนให้บริการ ผู้รับข้อมูลต้องจัดให้มีกระบวนการรู้จักผู้ใช้บริการ (Know Your Customer: KYC) ตามระดับความเสี่ยงของประเภทธุรกรรมและช่องทางการให้บริการ และจัดให้มีวิธีการยืนยันตัวตนผู้ใช้บริการ (authentication) เพื่อพิสูจน์ให้ได้ว่าผู้ใช้บริการที่ประสงค์จะขอใช้บริการเป็นผู้ใช้บริการรายนั้นจริง ทั้งนี้ หากมีการกำหนดหลักเกณฑ์ที่เกี่ยวข้องกับการทำ KYC หรือ authentication สำหรับบริการใดไว้เป็นการเฉพาะ ให้ผู้รับข้อมูลถือปฏิบัติตามหลักเกณฑ์ดังกล่าวด้วย นอกจากนี้ ผู้ส่งข้อมูลต้องจัดให้มีกระบวนการตรวจสอบว่าผู้ใช้บริการที่ประสงค์จะขอให้ส่งข้อมูลเป็นเจ้าของข้อมูลจริง หรือมีกระบวนการยืนยันการใช้สิทธิของผู้ใช้บริการที่เป็นเจ้าของข้อมูลในการดำเนินการส่งข้อมูล เพื่อป้องกันการเรียกหรือใช้ข้อมูลเกินกว่าความประสงค์ของผู้ใช้บริการหรือเกิดการสวมรอยใช้สิทธิโดยผู้ที่ไม่ใช่ผู้ใช้บริการ

#### 4.3.4.3 การบริหารจัดการข้อมูลให้มีความมั่นคงปลอดภัย

เพื่อให้ข้อมูลของผู้ใช้บริการมีความมั่นคงปลอดภัยตลอดทั้งกระบวนการตั้งแต่ก่อน ระหว่าง และหลังการรับส่งข้อมูล ผู้ส่งข้อมูลและผู้รับข้อมูลต้องปฏิบัติตามหลักเกณฑ์ด้านการบริหารจัดการข้อมูลให้มีความมั่นคงปลอดภัย ดังนี้

**(1) ธรรมาภิบาลในการบริหารจัดการข้อมูล**

ผู้ส่งข้อมูลและผู้รับข้อมูลต้องมีธรรมาภิบาลในการบริหารจัดการข้อมูลที่ดีเพื่อให้มั่นใจว่าข้อมูลที่ผู้ให้บริการรับส่งและขั้นตอนต่าง ๆ ที่เกี่ยวข้องตามประกาศฉบับนี้มีการดูแลด้านความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูลตลอดทั้งกระบวนการตั้งแต่ก่อน ระหว่าง และหลังการรับส่งข้อมูล โดยคณะกรรมการของผู้ส่งข้อมูลและผู้รับข้อมูลต้องให้ความสำคัญกับการใช้สิทธิในข้อมูลของผู้ใช้บริการ การรักษาความมั่นคงปลอดภัยของข้อมูล และความเป็นส่วนบุคคลของข้อมูล และทำหน้าที่กำกับดูแลให้มีการดำเนินการในเรื่องดังกล่าวอย่างเคร่งครัดและต่อเนื่อง รวมทั้งผู้บริหารระดับสูงของผู้ส่งข้อมูลและผู้รับข้อมูลต้องผลักดันและดูแลให้มีการดำเนินการตามนโยบาย

---

[9] กฎหมายหรือหลักเกณฑ์อื่น ๆ ในส่วนที่เกี่ยวกับการคุ้มครองผู้บริโภคตลอดกระบวนการใช้สิทธิส่งข้อมูลตามประกาศฉบับนี้ เช่น กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ประกาศธนาคารแห่งประเทศไทยว่าด้วยเรื่องการบริหารจัดการด้านการให้บริการแก่ลูกค้าอย่างเป็นธรรม ประกาศธนาคารแห่งประเทศไทยว่าด้วยหลักเกณฑ์ทั่วไปในการกำกับดูแลการประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับ และประกาศธนาคารแห่งประเทศไทยว่าด้วยการกำหนดหลักเกณฑ์ วิธีการ และเงื่อนไขในการประกอบธุรกิจของผู้ประกอบธุรกิจที่ไม่ใช่สถาบันการเงินตามแต่ละประเภท

ที่ได้รับอนุมัติจากคณะกรรมการอย่างเคร่งครัดและต่อเนื่อง โดยถือปฏิบัติตามหลักเกณฑ์ที่กำหนดในเอกสารแนบ 2

**(2) การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับการจัดการข้อมูล**

ผู้ส่งข้อมูลและผู้รับข้อมูลต้องดูแลระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับการบริหารจัดการและการรับส่งข้อมูลตามประกาศฉบับนี้ให้มีความมั่นคงปลอดภัย สามารถดูแลข้อมูลผู้ใช้บริการได้อย่างเหมาะสม และสามารถป้องกันและรับมือภัยคุกคามทางไซเบอร์และเหตุการณ์ข้อมูลรั่วไหลที่สำคัญได้อย่างมีประสิทธิภาพ ลดความเสี่ยงหรือผลกระทบต่อผู้ใช้บริการและต่อระบบดิจิทัลในการส่งข้อมูลโดยรวม โดยต้องกำหนดนโยบายและกระบวนการที่เกี่ยวข้องอย่างเพียงพอเหมาะสมกับความเสี่ยงของตน

กรณีที่ผู้ส่งข้อมูลและผู้รับข้อมูลเป็นสถาบันการเงินที่ถือปฏิบัติตามประกาศธนาคารแห่งประเทศไทยว่าด้วยหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ และกรณีที่ผู้ส่งข้อมูลและผู้รับข้อมูลเป็นผู้ประกอบธุรกิจบริการการชำระเงินที่ถือปฏิบัติตามหลักเกณฑ์ทุกข้อของประกาศธนาคารแห่งประเทศไทยว่าด้วยหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ตามกฎหมายว่าด้วยระบบการชำระเงินอยู่แล้ว[10] ให้ถือว่าได้ปฏิบัติตามหลักเกณฑ์ในวรรคแรกข้างต้นแล้ว

**(3) การจัดเก็บข้อมูลกิจกรรมการรับส่งข้อมูลของผู้ใช้บริการย้อนหลัง (audit trail)**

เพื่อประโยชน์ในการตรวจสอบและดำเนินการทางกฎหมายกรณีเกิดการละเมิดข้อมูลของผู้ใช้บริการหรือข้อมูลรั่วไหล ผู้ส่งข้อมูลและผู้รับข้อมูลต้องจัดเก็บข้อมูลกิจกรรมการรับส่งข้อมูลของผู้ใช้บริการย้อนหลัง (audit trail) ในแต่ละกิจกรรมที่ดำเนินการ โดยมีประเภทข้อมูลและระยะเวลาในการจัดเก็บ audit trail ตามที่กำหนดในเอกสารแนบ 4 และเอกสารแนบ 5 แล้วแต่กรณี

---

[10] ประกาศธนาคารแห่งประเทศไทยว่าด้วยหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ตามกฎหมายว่าด้วยระบบการชำระเงิน กำหนดขอบเขตการบังคับใช้ของแต่ละหลักเกณฑ์ตามคุณสมบัติของผู้ประกอบธุรกิจ

**(4) การบริหารจัดการเมื่อเกิดเหตุการณ์ผิดปกติหรือปัญหาเกี่ยวกับการใช้สิทธิส่งข้อมูลของผู้ใช้บริการ**

ผู้ส่งข้อมูลและผู้รับข้อมูลต้องมีการบริหารจัดการเหตุการณ์ผิดปกติและปัญหาที่เกิดจากการใช้สิทธิส่งข้อมูลของผู้ใช้บริการ เช่น ข้อมูลรั่วไหล และการถูกโจมตีจากภัยคุกคามทางไซเบอร์อย่างเหมาะสมทันการณ์ ทั้งในด้านระบบเทคโนโลยีสารสนเทศและการบริหารความเสี่ยงด้านปฏิบัติการอื่น ๆ โดยมีกระบวนการที่รัดกุมในการรับมือและตอบสนองเมื่อเกิดเหตุการณ์ผิดปกติหรือปัญหาให้สอดคล้องกับระดับความเสี่ยง รวมทั้งมีการรายงานเหตุการณ์ผิดปกติหรือปัญหาต่อผู้บริหารระดับสูงและ/หรือคณะกรรมการที่เกี่ยวข้องอย่างเหมาะสมกับระดับความเสี่ยง รวมถึงการแก้ไขปัญหาและจัดการเรื่องร้องเรียน นอกจากนี้ กรณีผู้ส่งข้อมูลและผู้รับข้อมูลที่เป็นผู้กระทำผิดหรือเป็นผู้มีหน้าที่ความรับผิดชอบในเรื่องนั้น ต้องเป็นผู้รับผิดชอบปัญหาหรือเหตุการณ์ผิดปกติดังกล่าว รวมทั้งต้องดำเนินการดูแล แก้ไข และเยียวยาแก่ลูกค้าอย่างเหมาะสม ทั้งนี้ ให้ถือปฏิบัติตามหลักเกณฑ์ที่กำหนดในเอกสารแนบ 3 และตามแนวปฏิบัติที่ธนาคารแห่งประเทศไทยกำหนด

อนึ่ง เมื่อเกิดเหตุการณ์ผิดปกติที่มีนัยสำคัญหรือปัญหาเกี่ยวกับการใช้สิทธิส่งข้อมูลหรือข้อพิพาทกับผู้ใช้บริการ ผู้ส่งข้อมูลและผู้รับข้อมูลต้องรายงานปัญหาหรือเหตุการณ์ดังกล่าว รวมถึงสาเหตุ แนวทางการแก้ไข และแนวทางการป้องกันการเกิดเหตุการณ์ผิดปกติหรือปัญหามิให้เกิดขึ้นซ้ำอีก ให้ธนาคารแห่งประเทศไทยทราบโดยเร็วเมื่อเกิดเหตุการณ์หรือเมื่อรับรู้ถึงการเกิดเหตุการณ์ โดยเหตุการณ์ผิดปกติที่มีนัยสำคัญหรือปัญหาเกี่ยวกับการใช้สิทธิส่งข้อมูลหรือข้อพิพาทกับผู้ใช้บริการที่ต้องรายงานแก่ธนาคารแห่งประเทศไทยอย่างน้อยต้องครอบคลุมปัญหาหรือเหตุการณ์ ดังนี้

(4.1) ปัญหาหรือเหตุการณ์ซึ่งอาจส่งผลกระทบอย่างมีนัยสำคัญต่อระบบงานหรือการให้บริการรับส่งข้อมูลตามประกาศฉบับนี้ หรือปัญหาฐานะหรือการดำเนินงานอันอาจเป็นเหตุให้เกิดความเสียหายแก่ประโยชน์ของประชาชน

(4.2) ปัญหาหรือเหตุการณ์ที่เกี่ยวข้องกับการให้บริการรับส่งข้อมูลตามประกาศฉบับนี้ที่นโยบายภายในของผู้ส่งข้อมูลและผู้รับข้อมูลกำหนดให้ต้องรายงานต่อผู้บริหารในตำแหน่งสูงสุดและ/หรือคณะกรรมการที่เกี่ยวข้อง

(4.3) เหตุการณ์ที่ระบบเทคโนโลยีสารสนเทศของผู้ส่งข้อมูลและผู้รับข้อมูลที่ใช้ในการดำเนินการตามประกาศฉบับนี้ถูกโจมตีหรือถูกขู่โจมตี

**4.3.4.4 การรับส่งข้อมูลทางดิจิทัลที่ได้มาตรฐาน**

ผู้ส่งข้อมูลและผู้รับข้อมูลต้องปฏิบัติตามแนวปฏิบัติที่ธนาคารแห่งประเทศไทยกำหนด ซึ่งรวมถึงมาตรฐานข้อมูล มาตรฐานความปลอดภัย มาตรฐานอื่นที่จำเป็นต่อการรับส่งข้อมูล เพื่อให้การเชื่อมต่อและรับส่งข้อมูลมีความปลอดภัยและเป็นมาตรฐานเดียวกัน รวมทั้งช่วยลดต้นทุนและความซ้ำซ้อนที่เกิดจากการพัฒนามาตรฐานที่แตกต่างกันและการเชื่อมต่อกับหลายหน่วยงานด้วยหลายมาตรฐาน

**4.3.4.5 การใช้บริการจากบุคคลภายนอก**

ผู้ส่งข้อมูลและผู้รับข้อมูลที่ประสงค์จะใช้บริการจากบุคคลภายนอกเพื่อดำเนินการใด ๆ ที่เกี่ยวข้องกับการรับส่งข้อมูลตามประกาศฉบับนี้ ต้องปฏิบัติตามหลักเกณฑ์ที่เกี่ยวข้อง รวมทั้งยังคงมีความรับผิดชอบต่อผู้ใช้บริการเสมือนผู้ส่งข้อมูลหรือผู้รับข้อมูลเป็นผู้ดำเนินการเอง

**4.3.4.6 การรายงานข้อมูลต่อธนาคารแห่งประเทศไทย**

ผู้ส่งข้อมูลและผู้รับข้อมูลต้องจัดส่งแบบรายงานในรูปแบบและตามระยะเวลาที่ธนาคารแห่งประเทศไทยกำหนด รวมถึงต้องจัดส่งรายงานและข้อมูลอื่นที่เกี่ยวข้องกับการรับส่งข้อมูลและการดำเนินการตามประกาศฉบับนี้เพิ่มเติมเป็นรายกรณีตามที่ธนาคารแห่งประเทศไทยร้องขอ เพื่อประโยชน์ในการติดตามพัฒนาการของการใช้งาน ปัญหาอุปสรรคที่เกิดขึ้น และการกำกับดูแลการให้บริการ

**4.3.5 หลักเกณฑ์ที่ใช้บังคับกับผู้ส่งข้อมูลและผู้รับข้อมูลผ่านกลไกส่งข้อมูลทางดิจิทัลแต่ละประเภท**

**4.3.5.1 ผู้ส่งข้อมูลและผู้รับข้อมูลผ่านระบบดิจิทัลในการส่งข้อมูลที่ได้มาตรฐาน** ให้ถือปฏิบัติตามหลักเกณฑ์ภายใต้ข้อ 4.3.4 ทุกข้อ โดยในเรื่องการคุ้มครองผู้บริโภคตามข้อ 4.3.4.2 (3) การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับการจัดการข้อมูลตามข้อ 4.3.4.3 (2) การจัดเก็บข้อมูลกิจกรรมการรับส่งข้อมูลของผู้ใช้บริการย้อนหลัง (audit trail) ตามข้อ 4.3.4.3 (3) และการรับส่งข้อมูลทางดิจิทัลที่ได้มาตรฐานตามข้อ 4.3.4.4 ให้ผู้ส่งข้อมูลและผู้รับข้อมูลถือปฏิบัติตามหลักเกณฑ์ในรายละเอียดตามเอกสารแนบ 4

**4.3.5.2 ผู้ส่งข้อมูลผ่านช่องทางดิจิทัลในการส่งข้อมูลที่ได้มาตรฐาน** ให้ถือปฏิบัติตามหลักเกณฑ์ภายใต้ข้อ 4.3.4 ทุกข้อ โดยในเรื่องการคุ้มครองผู้บริโภคตามข้อ 4.3.4.2 (3) การจัดเก็บข้อมูลกิจกรรมการรับส่งข้อมูลของผู้ใช้บริการย้อนหลัง (audit trail) ตามข้อ 4.3.4.3 (3)

และการรับส่งข้อมูลทางดิจิทัลที่ได้มาตรฐานตามข้อ 4.3.4.4 ให้ถือปฏิบัติตามหลักเกณฑ์ในรายละเอียดตามเอกสารแนบ 5

**4.3.5.3 ผู้ให้บริการทางการเงินที่ประสงค์โดยชัดแจ้งว่าจะรับข้อมูลของผู้ใช้บริการที่ได้รับจากช่องทางดิจิทัลในการส่งข้อมูลที่ได้มาตรฐานอีกทอดหนึ่ง**เพื่อนำไปใช้ในการให้บริการแก่ผู้ใช้บริการ ให้ปฏิบัติตามหลักเกณฑ์ภายใต้ข้อ 4.3.4 เฉพาะเรื่องการคุ้มครองผู้บริโภคตามข้อ 4.3.4.2 (1) และ (2) การบริหารจัดการเมื่อเกิดเหตุการณ์ผิดปกติหรือปัญหาเกี่ยวกับการใช้สิทธิส่งข้อมูลของผู้ใช้บริการตามข้อ 4.3.4.3 (4) การใช้บริการจากบุคคลภายนอกตามข้อ 4.3.4.5 และการรายงานข้อมูลต่อธนาคารแห่งประเทศไทยตามข้อ 4.3.4.6

**4.3.5.4 ผู้ส่งข้อมูลและผู้รับข้อมูลสินเชื่อผ่านระบบสำหรับสมาชิกบริษัทข้อมูลเครดิต** ให้ผู้ส่งข้อมูลและผู้รับข้อมูลปฏิบัติตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต ทั้งนี้ หากไม่มีข้อกำหนดเรื่องใดไว้เป็นการเฉพาะ ให้ผู้ส่งข้อมูลและผู้รับข้อมูลถือปฏิบัติตามหลักเกณฑ์ภายใต้ข้อ 4.3.4 โดยอนุโลม

**4.3.6 การกำหนดเงื่อนไขเพิ่มเติม สั่งให้แก้ไข ชะลอ หรือระงับการให้บริการรับส่งข้อมูลผ่านกลไกส่งข้อมูลทางดิจิทัล**

ธนาคารแห่งประเทศไทยอาจพิจารณากำหนดเงื่อนไขเพิ่มเติม สั่งให้แก้ไข ชะลอ หรือระงับการให้บริการบางส่วนหรือทั้งหมด ในกรณีดังต่อไปนี้

(1) ผู้ให้บริการทางการเงินฝ่าฝืนหรือไม่ปฏิบัติตามหลักเกณฑ์ที่กำหนดตามประกาศฉบับนี้

(2) กรณีที่ธนาคารแห่งประเทศไทยเห็นว่า ผู้ให้บริการทางการเงินมีการดำเนินธุรกิจที่ส่งผลกระทบจนเกิดความเสียหายต่อประชาชนในวงกว้าง หรือผู้ให้บริการทางการเงินจำเป็นต้องพัฒนาหรือปรับปรุงกลไกส่งข้อมูลทางดิจิทัลที่ให้บริการแก่ผู้ใช้บริการ

(3) กรณีอื่น ๆ ที่ธนาคารแห่งประเทศไทยเห็นว่ากระทบกับความปลอดภัยหรือความผาสุกของประชาชน

ทั้งนี้ ตามที่กฎหมายกำหนดให้อำนาจธนาคารแห่งประเทศไทยดำเนินการในเรื่องดังกล่าว

**4.4 การขอผ่อนผันการปฏิบัติตามหลักเกณฑ์**

ในกรณีมีเหตุจำเป็นหรือพฤติการณ์พิเศษซึ่งทำให้ผู้ให้บริการทางการเงินที่เป็นผู้มีหน้าที่ส่งข้อมูลไม่สามารถจัดทำกลไกส่งข้อมูลทางดิจิทัลได้ตามที่กำหนดในประกาศฉบับนี้ ผู้ให้บริการทางการเงินดังกล่าวต้องยื่นขออนุญาตผ่อนผันการปฏิบัติตามหลักเกณฑ์เป็นรายกรณี โดยแสดงเหตุผลและความจำเป็น แผนการดำเนินการเพื่อให้สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนด และรายละเอียดที่เกี่ยวข้องอื่น ๆ มายังธนาคารแห่งประเทศไทยตามที่กำหนดในคู่มือประชาชน ทั้งนี้ ธนาคารแห่งประเทศไทยอาจพิจารณาอนุญาตหรือไม่ก็ได้ หรือกำหนดเงื่อนไขใด ๆ ให้ผู้ให้บริการทางการเงินถือปฏิบัติเพิ่มเติมตามความเหมาะสมด้วยก็ได้

**5. วันเริ่มต้นบังคับใช้**

ประกาศฉบับนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

**ประกาศ ณ วันที่ 25 กันยายน 2568**

(นายเศรษฐพุฒิ สุทธิวาทนฤพุฒิ)
ผู้ว่าการ
ธนาคารแห่งประเทศไทย

ฝ่ายกลยุทธ์สถาบันการเงิน
โทรศัพท์ 0 2283 5191

**เอกสารแนบ 1**

**แนวทางการนำต้นทุนมาใช้ในการพิจารณากำหนดค่าธรรมเนียมที่เกี่ยวข้องกับการรับส่งข้อมูล**

ต้นทุนที่นำมาใช้ในการพิจารณากำหนดค่าธรรมเนียมที่เกี่ยวข้องกับการรับส่งข้อมูลของผู้ใช้บริการต้องสะท้อนต้นทุนที่เกิดขึ้นจริงและพอสมควรแก่เหตุ ตามแนวทางดังต่อไปนี้

1. ต้นทุนส่วนเพิ่มเฉพาะที่เกิดกับผู้ส่งข้อมูลหรือผู้รับข้อมูลอันเนื่องมาจากการดำเนินการเพื่อให้สามารถให้บริการรับส่งข้อมูลของผู้ใช้บริการตามประกาศฉบับนี้เท่านั้น โดยไม่รวมถึงต้นทุนส่วนที่สามารถนำไปใช้เพื่อประโยชน์อื่นของผู้ส่งข้อมูลหรือผู้รับข้อมูล

2. ต้นทุนที่เป็นผลลัพธ์ที่คำนวณได้ตามแนวทางข้อ 1 ซึ่งเป็นตัวแทนของอุตสาหกรรมหรือได้รับการยอมรับจากผู้ที่เกี่ยวข้อง เช่น ใช้ค่าเฉลี่ยของต้นทุนที่คำนวณตามข้อ 1 ของทั้งอุตสาหกรรม หรือค่าที่คำนวณได้จากต้นทุนตามข้อ 1 ที่ได้มีการรับฟังความคิดเห็น มีการหารือ หรือมีข้อตกลงร่วมกันกับผู้ที่เกี่ยวข้องแล้ว

**เอกสารแนบ 2**

## หลักเกณฑ์ธรรมาภิบาลในการบริหารจัดการข้อมูล

ผู้ส่งข้อมูลและผู้รับข้อมูลต้องมีการกำกับดูแลกิจการด้านธรรมาภิบาลในการบริหารจัดการข้อมูล ดังนี้

1. คณะกรรมการของผู้ส่งข้อมูลและผู้รับข้อมูลต้องให้ความสำคัญกับการใช้สิทธิในข้อมูลของผู้ใช้บริการ การรักษาความมั่นคงปลอดภัยของข้อมูล และความเป็นส่วนบุคคลของข้อมูล และทำหน้าที่กำกับดูแลให้มีการดำเนินการในเรื่องดังกล่าวอย่างเคร่งครัดและต่อเนื่อง โดยต้องดำเนินการดังต่อไปนี้

1.1 กำหนดและอนุมัตินโยบายที่ให้ความสำคัญกับการใช้สิทธิส่งข้อมูลของผู้ใช้บริการ การรักษาความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล ซึ่งครอบคลุมการบริหารจัดการตลอดวงจรชีวิตข้อมูล และทบทวนนโยบายดังกล่าวตามความถี่ที่เหมาะสม หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

1.2 รับผิดชอบในการกำกับดูแลในภาพรวม และกำกับดูแลให้มีโครงสร้างองค์กรที่สามารถรองรับการดำเนินการให้ผู้ใช้บริการใช้สิทธิส่งข้อมูลของผู้ใช้บริการได้อย่างเป็นรูปธรรม มีการสอบทานและถ่วงดุลการปฏิบัติงานอย่างเหมาะสม โดยพิจารณารูปแบบและแนวทางการดำเนินการให้เหมาะสมกับขนาด ลักษณะการดำเนินธุรกิจ ความซับซ้อนของธุรกิจ และความเสี่ยงด้านข้อมูลของผู้ส่งข้อมูลหรือผู้รับข้อมูล

1.3 กำกับดูแลให้ผู้บริหารระดับสูงสื่อสารนโยบายเกี่ยวกับธรรมาภิบาลในการจัดการข้อมูลให้ผู้ที่เกี่ยวข้องภายในองค์กรตระหนักถึงความสำคัญและเข้าใจบทบาทหน้าที่ความรับผิดชอบ และผลักดันให้ผู้ที่เกี่ยวข้องดำเนินการตามนโยบายที่กำหนดอย่างเคร่งครัดและต่อเนื่อง

1.4 กำกับดูแลให้เกิดการจัดสรรทรัพยากร เพื่อสนับสนุนการดำเนินการด้านการใช้สิทธิส่งข้อมูลของผู้ใช้บริการ การรักษาความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูลให้ได้ผลสัมฤทธิ์ตามที่กำหนดไว้

1.5 ติดตามและกำกับดูแลภาพรวมการดำเนินการให้ผู้ใช้บริการใช้สิทธิส่งข้อมูล การรักษาความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล ให้เป็นไปตามหลักเกณฑ์ที่เกี่ยวข้องและนโยบายที่กำหนด โดยกำกับดูแลให้ฝ่ายจัดการดำเนินการ ดังนี้

1.5.1 รายงานการดำเนินงานและความเสี่ยงต่อผู้บริหารระดับสูงอย่างสม่ำเสมอ และรายงานเรื่องดังกล่าวต่อคณะกรรมการอย่างน้อยปีละครั้ง เพื่อใช้ประกอบการพิจารณาทบทวนนโยบายและแผนกลยุทธ์ในส่วนที่เกี่ยวข้อง

1.5.2 รายงานความเสี่ยงที่สำคัญและประเด็นที่อาจส่งผลอย่างมีนัยสำคัญต่อการให้บริการ ฐานะการดำเนินงาน หรือชื่อเสียงของผู้ส่งข้อมูลหรือผู้รับข้อมูลต่อคณะกรรมการโดยไม่ชักช้า เพื่อพิจารณาสั่งการป้องกันหรือให้มีการแก้ไขปัญหาสำคัญในเวลาที่เหมาะสม

ทั้งนี้ เพื่อเพิ่มประสิทธิภาพและประสิทธิผลในการปฏิบัติงาน คณะกรรมการอาจมอบหมายให้คณะกรรมการชุดย่อยหรือผู้ที่ได้รับมอบหมายดำเนินการ ดังนี้

(ก) ทบทวนนโยบายแทนคณะกรรมการ โดยต้องรายงานให้คณะกรรมการทราบ และหากมีการเปลี่ยนแปลงที่มีนัยสำคัญ ต้องเสนอคณะกรรมการพิจารณาอนุมัติ

(ข) ดูแลการจัดโครงสร้างองค์กรและการกำหนดบทบาทหน้าที่ในรายละเอียดตามโครงสร้างองค์กรในภาพรวมที่คณะกรรมการได้เคยอนุมัติไว้แล้ว

(ค) ติดตามการรายงานการดำเนินงานและประเด็นความเสี่ยงสำคัญจากฝ่ายจัดการ โดยต้องรายงานสรุปภาพรวมการดำเนินงานให้คณะกรรมการทราบอย่างน้อยปีละครั้ง และรายงานประเด็นความเสี่ยงสำคัญต่อคณะกรรมการโดยไม่ชักช้า

ในกรณีที่มีการมอบหมายข้างต้น คณะกรรมการต้องกำหนดบทบาทหน้าที่ ความรับผิดชอบและอำนาจของคณะกรรมการชุดย่อยหรือผู้ที่ได้รับมอบหมายดังกล่าวให้ชัดเจน และต้องติดตามการดำเนินงานในภาพรวมและประเด็นความเสี่ยงสำคัญที่ได้รับรายงานจากคณะกรรมการชุดย่อยหรือผู้ที่ได้รับมอบหมายจากคณะกรรมการอย่างสม่ำเสมอ เพื่อกำกับดูแลผู้ส่งข้อมูลและผู้รับข้อมูลให้สามารถดำเนินการปรับปรุงแก้ไขกรณีที่เกิดปัญหาได้อย่างเหมาะสมและทันการณ์ รวมทั้งมีการพิจารณาสาเหตุของปัญหาและปรับปรุงเพื่อป้องกันมิให้เกิดปัญหาซ้ำอีกในอนาคต

2. ผู้บริหารระดับสูงของผู้ส่งข้อมูลและผู้รับข้อมูลต้องทำหน้าที่ผลักดันและดูแลให้มีการดำเนินการตามนโยบายที่ได้รับอนุมัติจากคณะกรรมการอย่างเคร่งครัดและต่อเนื่อง โดยต้องดำเนินการดังต่อไปนี้

2.1 นำนโยบายที่ได้รับอนุมัติจากคณะกรรมการไปสื่อสารและผลักดันให้ผู้ที่เกี่ยวข้องในองค์กรดำเนินการตามนโยบายดังกล่าวอย่างเป็นรูปธรรมและเคร่งครัด

2.2 จัดให้มีโครงสร้างองค์กร กำหนดผู้รับผิดชอบและบทบาทหน้าที่ในรายละเอียดที่ชัดเจนตามโครงสร้างองค์กรที่คณะกรรมการได้เคยอนุมัติไว้ และผลักดันให้เกิดการจัดสรรทรัพยากรอย่างเพียงพอที่จะสนับสนุนการดำเนินการด้านการใช้สิทธิส่งข้อมูลของผู้ใช้บริการ การรักษาความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล ให้ได้ผลสัมฤทธิ์ตามที่กำหนดไว้

2.3 ติดตามการดำเนินการเกี่ยวกับการให้ผู้ใช้บริการ ใช้สิทธิส่งข้อมูล การรักษาความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล ให้เป็นไปตามนโยบายที่คณะกรรมการกำหนดและหลักเกณฑ์ที่หน่วยงานกำกับดูแลกำหนดในส่วนที่เกี่ยวข้อง รวมทั้งรายงานเรื่องดังกล่าวต่อคณะกรรมการ คณะกรรมการชุดย่อยหรือผู้ที่ได้รับมอบหมายจากคณะกรรมการอย่างน้อยปีละครั้ง และรายงานความเสี่ยงที่สำคัญและประเด็นที่อาจส่งผลอย่างมีนัยสำคัญต่อการให้บริการ ฐานะการดำเนินงาน หรือชื่อเสียงของผู้ส่งข้อมูลหรือผู้รับข้อมูลต่อคณะกรรมการโดยไม่ชักช้า

ทั้งนี้ ผู้ส่งข้อมูลและผู้รับข้อมูลที่เป็นสาขาของธนาคารพาณิชย์ต่างประเทศหรือของผู้ให้บริการทางการเงินต่างประเทศในประเทศไทยให้ถือปฏิบัติเฉพาะส่วนของผู้บริหารระดับสูงของผู้ส่งข้อมูลและผู้รับข้อมูลตามข้อ 2

**เอกสารแนบ 3**

## หลักเกณฑ์การบริหารจัดการเมื่อเกิดเหตุการณ์ผิดปกติหรือปัญหาเกี่ยวกับการใช้สิทธิส่งข้อมูลของผู้ใช้บริการ

ผู้ส่งข้อมูลและผู้รับข้อมูลต้องมีการบริหารจัดการเหตุการณ์ผิดปกติและปัญหาที่เกิดจากการใช้สิทธิส่งข้อมูลของผู้ใช้บริการอย่างเหมาะสมและทันท่วงที ทั้งในด้านระบบเทคโนโลยีสารสนเทศและการบริหารความเสี่ยงด้านปฏิบัติการอื่น ๆ ดังนี้

**1. มีกระบวนการที่รัดกุมในการรับมือและตอบสนองเมื่อเกิดเหตุการณ์ผิดปกติหรือปัญหาให้สอดคล้องกับระดับความเสี่ยง** เพื่อให้สามารถรับมือและตอบสนองต่อเหตุการณ์ได้อย่างเหมาะสมและทันการณ์ และมีการแก้ไขปัญหาโดยไม่ชักช้า ตลอดจนมีแนวทางในการตรวจสอบ วิเคราะห์หาสาเหตุและประเมินผลกระทบ รวมทั้งมีแนวทางหรือแผนดำเนินการเพื่อป้องกันเหตุการณ์ผิดปกติหรือมิให้เกิดปัญหาซ้ำอีกในอนาคต

**2. มีการรายงานเหตุการณ์ผิดปกติหรือปัญหาต่อผู้บริหารระดับสูงและ/หรือคณะกรรมการที่เกี่ยวข้องอย่างเหมาะสมกับระดับความเสี่ยง** โดยในกรณีที่เกิดปัญหาหรือเหตุการณ์ที่รุนแรงหรืออาจส่งผลกระทบอย่างมีนัยสำคัญต่อการให้บริการ ฐานะการดำเนินงาน หรือชื่อเสียงของผู้ส่งข้อมูลหรือผู้รับข้อมูล ต้องมีการรายงานให้คณะกรรมการของผู้ส่งข้อมูลหรือผู้รับข้อมูลทราบอย่างทันท่วงทีด้วย

**3. มีการแก้ไขปัญหาและจัดการเรื่องร้องเรียน** โดยผู้ส่งข้อมูลและผู้รับข้อมูลต้องปฏิบัติตามหลักเกณฑ์ที่เกี่ยวข้องกับการแก้ไขปัญหาและจัดการเรื่องร้องเรียนที่บังคับใช้อยู่แล้วในปัจจุบัน เช่น มาตรฐานขั้นต่ำสำหรับการแก้ไขปัญหาและจัดการเรื่องร้องเรียนตามประกาศธนาคารแห่งประเทศไทยว่าด้วยการบริหารจัดการด้านการให้บริการแก่ลูกค้าอย่างเป็นธรรม และข้อกำหนดเกี่ยวกับการปฏิบัติเมื่อมีข้อร้องเรียนตามประกาศธนาคารแห่งประเทศไทยว่าด้วยการกำหนดหลักเกณฑ์ วิธีการ และเงื่อนไขในการประกอบธุรกิจของผู้ประกอบธุรกิจที่ไม่ใช่สถาบันการเงินแต่ละประเภท ซึ่งครอบคลุมประเด็นสำคัญ เช่น การกำหนดให้มีบุคลากรที่ทำหน้าที่รับเรื่องร้องเรียนและช่องทางรับเรื่องร้องเรียนโดยแจ้งให้ผู้ใช้บริการทราบช่องทางดังกล่าว กำหนดให้มีกระบวนการรับและดำเนินการเกี่ยวกับปัญหาและเรื่องร้องเรียนที่เป็นมาตรฐาน มีการแก้ไขด้วยความเป็นธรรม มีการติดตามการแก้ไขปัญหาและเรื่องร้องเรียนอย่างสม่ำเสมอ มีมาตรการเยียวยาหรือชดเชยให้แก่ผู้ใช้บริการ รวมทั้งมีการป้องกันไม่ให้เกิดปัญหาหรือเรื่องร้องเรียนซ้ำอีก

ทั้งนี้ ผู้ส่งข้อมูลและผู้รับข้อมูลที่ไม่อยู่ภายใต้ขอบเขตการบังคับใช้ของประกาศธนาคารแห่งประเทศไทยว่าด้วยการบริหารจัดการด้านการให้บริการแก่ลูกค้าอย่างเป็นธรรม[11] ให้ถือปฏิบัติตามข้อกำหนด

---

[11] ปัจจุบัน ได้แก่ ผู้ประกอบธุรกิจบริการเงินอิเล็กทรอนิกส์ และผู้ประกอบธุรกิจระบบหรือเครือข่ายอิเล็กทรอนิกส์สำหรับธุรกรรมสินเชื่อระหว่างบุคคลกับบุคคล

ว่าด้วยการแก้ไขและจัดการเรื่องร้องเรียนสำหรับผู้ประกอบธุรกิจที่ไม่ใช่สถาบันการเงินที่มียอดสินเชื่อคงค้างรวมต่ำกว่าระดับที่มีนัยสำคัญตามประกาศธนาคารแห่งประเทศไทยว่าด้วยการบริหารจัดการด้านการให้บริการแก่ลูกค้าอย่างเป็นธรรม โดยอนุโลม

**เอกสารแนบ 4**

**หลักเกณฑ์ในรายละเอียดสำหรับผู้ส่งข้อมูลและผู้รับข้อมูลผ่านระบบดิจิทัลในการส่งข้อมูลที่ได้มาตรฐาน**

ผู้ส่งข้อมูลและผู้รับข้อมูลผ่านระบบดิจิทัลในการส่งข้อมูลที่ได้มาตรฐานต้องถือปฏิบัติตามหลักเกณฑ์ในรายละเอียดในเรื่องการคุ้มครองผู้บริโภคตามข้อ 4.3.4.2 (3) การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับการจัดการข้อมูลตามข้อ 4.3.4.3 (2) การจัดเก็บข้อมูลกิจกรรมการรับส่งข้อมูลของผู้ใช้บริการย้อนหลัง (audit trail) ตามข้อ 4.3.4.3 (3) การรับส่งข้อมูลทางดิจิทัลที่ได้มาตรฐานตามข้อ 4.3.4.4 ดังต่อไปนี้

**1. การคุ้มครองความเป็นส่วนบุคคลของข้อมูลตลอดทั้งกระบวนการใช้สิทธิส่งข้อมูลของผู้ใช้บริการ**

เพื่อป้องกันการเรียกหรือใช้ข้อมูลโดยไม่ได้รับความยินยอมจากผู้ใช้บริการหรือเกิดการสวมรอยใช้สิทธิโดยผู้ที่ไม่ใช่ผู้ใช้บริการซึ่งเป็นเจ้าของข้อมูล ผู้ส่งข้อมูลและผู้รับข้อมูลผ่านระบบดิจิทัลในการส่งข้อมูลที่ได้มาตรฐานต้องปฏิบัติตามหลักเกณฑ์ด้านการคุ้มครองความเป็นส่วนบุคคลของข้อมูลตลอดทั้งกระบวนการใช้สิทธิส่งข้อมูลของผู้ใช้บริการ ดังต่อไปนี้

**1.1 เมื่อผู้ใช้บริการขอใช้บริการ** ให้ผู้รับข้อมูลจัดให้มีกระบวนการรู้จักลูกค้า (Know Your Customer: KYC) ตามระดับความเสี่ยงของประเภทธุรกรรมและช่องทางการให้บริการ อย่างไรก็ดี ในกรณีที่ผู้ใช้บริการได้เคยทำ KYC กับผู้รับข้อมูลไว้แล้ว ผู้รับข้อมูลต้องจัดให้มีวิธีการยืนยันตัวตนผู้ใช้บริการ (authentication) เพื่อพิสูจน์ให้ได้ว่าผู้ใช้บริการที่ประสงค์จะขอใช้บริการเป็นผู้ใช้บริการรายนั้นจริง ทั้งนี้ หากมีการกำหนดหลักเกณฑ์ที่เกี่ยวข้องกับการทำ KYC หรือ authentication สำหรับบริการประเภทใดไว้เป็นการเฉพาะ ให้ผู้รับข้อมูลถือปฏิบัติตามหลักเกณฑ์ดังกล่าวด้วย

**1.2 เมื่อผู้รับข้อมูลจะเรียกข้อมูลของผู้ใช้บริการ** ตามคำขอใช้สิทธิส่งข้อมูลของผู้ใช้บริการเพื่อประกอบการเสนอบริการแก่ผู้ใช้บริการดังกล่าว ผู้รับข้อมูลต้องขอให้ผู้ใช้บริการให้ความยินยอม (consent) ต่อผู้ส่งข้อมูลในการเปิดเผยข้อมูลของผู้ใช้บริการแก่ผู้รับข้อมูล โดยผู้รับข้อมูลต้องจัดให้มีการทำ authentication สำหรับการให้ consent ของผู้ใช้บริการ เพื่อให้มั่นใจว่าผู้ที่ประสงค์จะขอใช้สิทธิส่งข้อมูลเป็นผู้ใช้บริการรายนั้นจริง

**1.3 เมื่อผู้ส่งข้อมูลจะส่งข้อมูลของผู้ใช้บริการ** ผู้ส่งข้อมูลต้องพิจารณาและนำผลการทำ authentication มาใช้ในกระบวนการยืนยันการใช้สิทธิส่งข้อมูลของผู้ใช้บริการ (authorization) เพื่อดำเนินการส่งข้อมูลตาม consent ของผู้ใช้บริการ

**1.4 เมื่อผู้ใช้บริการใช้สิทธิแล้ว** ผู้ส่งข้อมูลและผู้รับข้อมูลต้องจัดให้ผู้ใช้บริการสามารถดำเนินการบริหารจัดการและตรวจสอบ consent และ authorization ของตนได้ง่ายและสะดวก โดยผู้ส่งข้อมูลและ

ผู้รับข้อมูลต้องจัดให้มี หรือพิจารณาและนำผลการทำ authentication มาใช้ในการดำเนินการบริหารจัดการและตรวจสอบ consent และ authorization ของผู้ใช้บริการ แล้วแต่กรณี นอกจากนี้ ในกรณีที่ผู้ใช้บริการมีการเปลี่ยนแปลงการให้ consent หรือ authorization ให้ผู้ส่งข้อมูลและผู้รับข้อมูลแจ้งให้ผู้ที่เกี่ยวข้องทราบด้วย

ทั้งนี้ การดำเนินการเกี่ยวกับ consent และ authorization รวมทั้ง authentication ต้องเป็นไปตามหลักเกณฑ์ที่กำหนดในเอกสารแนบ 4.1 และตามแนวปฏิบัติที่ธนาคารแห่งประเทศไทยกำหนด

อนึ่ง สำหรับข้อมูลผู้ใช้บริการที่เป็นนิติบุคคล SMEs ให้ผู้ส่งข้อมูลและผู้รับข้อมูลถือปฏิบัติตามแนวปฏิบัติสำหรับการรับส่งข้อมูลของผู้ใช้บริการที่เป็นนิติบุคคล SMEs ที่ธนาคารแห่งประเทศไทยจะกำหนดเป็นการเฉพาะต่อไป

**2. การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับการจัดการข้อมูล**

ผู้ส่งข้อมูลและผู้รับข้อมูลผ่านระบบดิจิทัลในการส่งข้อมูลที่ได้มาตรฐานต้องจัดให้มีการบริหารจัดการระบบเทคโนโลยีสารสนเทศและข้อมูลอย่างเพียงพอเหมาะสม เพื่อควบคุมดูแลระบบเทคโนโลยีสารสนเทศและข้อมูลที่เกี่ยวข้องกับการบริหารจัดการและการรับส่งข้อมูลตามประกาศฉบับนี้ ให้มีความมั่นคงปลอดภัย ถูกต้องเชื่อถือได้ และพร้อมใช้งาน โดยกำหนดให้ผู้ส่งข้อมูลและผู้รับข้อมูลซึ่งเป็นผู้ให้บริการทางการเงินแต่ละประเภทถือปฏิบัติตามหลักเกณฑ์ ดังนี้

2.1 ผู้ส่งข้อมูลและผู้รับข้อมูลที่เป็นสถาบันการเงิน ให้ถือปฏิบัติตามประกาศธนาคารแห่งประเทศไทยว่าด้วยหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ และหลักเกณฑ์อื่นที่เกี่ยวข้อง

2.2 ผู้ส่งข้อมูลและผู้รับข้อมูลที่เป็นผู้ประกอบธุรกิจบริการการชำระเงินที่ต้องถือปฏิบัติตามหลักเกณฑ์ทุกข้อตามประกาศธนาคารแห่งประเทศไทยว่าด้วยหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ตามกฎหมายว่าด้วยระบบการชำระเงิน[12] ให้ถือปฏิบัติตามหลักเกณฑ์ดังกล่าว และหลักเกณฑ์อื่นที่เกี่ยวข้อง

2.3 ผู้ส่งข้อมูลและผู้รับข้อมูลที่มิใช่สถาบันการเงินและมิใช่ผู้ประกอบธุรกิจบริการการชำระเงินตามข้อ 2.2 ให้ถือปฏิบัติตามมาตรฐานขั้นต่ำด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับการจัดการข้อมูลสำหรับการรับส่งข้อมูลผ่านระบบดิจิทัลในการส่งข้อมูลที่ได้มาตรฐานตามที่กำหนดในเอกสารแนบ 4.2

---

[12]ประกาศธนาคารแห่งประเทศไทยว่าด้วยหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ตามกฎหมายว่าด้วยระบบการชำระเงิน กำหนดขอบเขตการบังคับใช้ของแต่ละหลักเกณฑ์ตามคุณสมบัติของผู้ประกอบธุรกิจ

**3. การจัดเก็บข้อมูลกิจกรรมการรับส่งข้อมูลของผู้ใช้บริการย้อนหลัง (audit trail)**

ผู้ส่งข้อมูลและผู้รับข้อมูลผ่านระบบดิจิทัลในการส่งข้อมูลที่ได้มาตรฐานต้องจัดเก็บ audit trail ในแต่ละกิจกรรมที่ดำเนินการ เพื่อประโยชน์ในการตรวจสอบและดำเนินการทางกฎหมายกรณีเกิดการละเมิดข้อมูลของผู้ใช้บริการหรือข้อมูลรั่วไหล โดยมีประเภทข้อมูลและระยะเวลาในการจัดเก็บ audit trail ดังตารางด้านล่างนี้ รวมทั้งต้องถือปฏิบัติตามแนวปฏิบัติที่ธนาคารแห่งประเทศไทยกำหนด

| | **ประเภทข้อมูลที่ต้องจัดเก็บ audit trail** | **ระยะเวลาการจัดเก็บ audit trail** |
|---|---|---|
| ผู้ส่งข้อมูลผ่านระบบดิจิทัลในการส่งข้อมูลที่ได้มาตรฐาน | (1) ข้อมูลกิจกรรมการให้ การเปลี่ยนแปลง และการถอน authorization<br>(2) ข้อมูลกิจกรรมการส่งข้อมูลของผู้ใช้บริการไปยังผู้รับข้อมูล | ไม่น้อยกว่า 10 ปี นับตั้งแต่วันที่ได้ดำเนินการเกี่ยวกับ consent authorization การรับส่งข้อมูล แล้วแต่กรณี |
| ผู้รับข้อมูลผ่านระบบดิจิทัลในการส่งข้อมูลที่ได้มาตรฐาน | (1) ข้อมูลกิจกรรมการให้ การเปลี่ยนแปลง และการถอน consent<br>(2) ข้อมูลกิจกรรมการรับข้อมูลของผู้ใช้บริการจากผู้ส่งข้อมูล | |

**4. การรับส่งข้อมูลผ่านระบบดิจิทัลในการส่งข้อมูลที่ได้มาตรฐาน**

**4.1 การปฏิบัติตามมาตรฐาน** ผู้ส่งข้อมูลและผู้รับข้อมูลผ่านระบบดิจิทัลในการส่งข้อมูลที่ได้มาตรฐานต้องถือปฏิบัติตามมาตรฐานที่กำหนดในแนวปฏิบัติของธนาคารแห่งประเทศไทย ซึ่งรวมถึงมาตรฐานข้อมูล มาตรฐานความปลอดภัย และมาตรฐานอื่นที่จำเป็นต่อการรับส่งข้อมูล เพื่อให้การเชื่อมต่อและการรับส่งข้อมูลผ่านระบบดิจิทัลในการส่งข้อมูลที่ได้มาตรฐานมีความปลอดภัยและเป็นมาตรฐานเดียวกัน รวมทั้งช่วยลดต้นทุนและความซ้ำซ้อนที่อาจเกิดขึ้น หากมาตรฐานที่ผู้ส่งข้อมูลและผู้รับข้อมูลแต่ละรายใช้งานมีความแตกต่างกัน

**4.2 ก่อนเริ่มให้บริการรับส่งข้อมูล** ผู้ส่งข้อมูลและผู้รับข้อมูลผ่านระบบดิจิทัลในการส่งข้อมูลที่ได้มาตรฐานต้องดำเนินการดังต่อไปนี้ เพื่อประเมินคุณสมบัติและความพร้อมของผู้ส่งข้อมูลและผู้รับข้อมูลก่อนการให้บริการ เพื่อให้มั่นใจว่าผู้ส่งข้อมูลและผู้รับข้อมูลสามารถรับส่งข้อมูลของผู้ใช้บริการและเป็นไปตามมาตรฐานและแนวปฏิบัติที่ธนาคารแห่งประเทศไทยกำหนด

### 4.2.1 การตกลงการใช้บริการกับผู้ให้บริการระบบทะเบียน[13]

ผู้ส่งข้อมูลและผู้รับข้อมูลต้องมีการตกลงการใช้บริการกับผู้ให้บริการระบบทะเบียนที่มีคุณสมบัติและเงื่อนไขการให้บริการ และได้รับการรับรองจากคณะกรรมการขับเคลื่อนโครงการ Your Data ตามที่กำหนดในเอกสารแนบ 4.3 เพื่อให้มั่นใจว่าผู้ให้บริการระบบทะเบียนสามารถให้บริการ รวมทั้งสามารถทดสอบและประเมินผลให้ผู้ส่งข้อมูลและผู้รับข้อมูลสามารถปฏิบัติตามมาตรฐานและแนวปฏิบัติที่ธนาคารแห่งประเทศไทยกำหนดได้

กรณีผู้ส่งข้อมูลและผู้รับข้อมูลได้รับแจ้งการยกเลิกคำรับรองผู้ให้บริการระบบทะเบียนจากธนาคารแห่งประเทศไทย ให้ผู้ส่งข้อมูลและผู้รับข้อมูลยุติการใช้บริการกับผู้ให้บริการระบบทะเบียนที่ถูกยกเลิกคำรับรองดังกล่าวตามที่ได้รับแจ้ง และดำเนินการตกลงใช้บริการกับผู้ให้บริการระบบทะเบียนรายอื่นที่ได้รับการรับรองจากคณะกรรมการขับเคลื่อนโครงการ Your Data ตามที่กำหนดในเอกสารแนบ 4.3 เพื่อให้การให้บริการรับส่งข้อมูลดำเนินการได้อย่างต่อเนื่อง

### 4.2.2 การเข้ารับการทดสอบและประเมินคุณสมบัติและความพร้อม

ผู้ส่งข้อมูลและผู้รับข้อมูลผ่านระบบดิจิทัลในการส่งข้อมูลที่ได้มาตรฐานต้องมีคุณสมบัติและความพร้อมที่จะให้บริการแก่ผู้ใช้บริการตามหลักเกณฑ์และแนวปฏิบัติที่ธนาคารแห่งประเทศไทยกำหนด โดยต้องผ่านการทดสอบและประเมิน ดังนี้

(1) เข้ารับการทดสอบกับผู้ให้บริการระบบทะเบียน โดยเข้ารับการทดสอบในส่วนที่เกี่ยวข้องกับการปฏิบัติตามมาตรฐานข้อมูล มาตรฐานการรับส่งข้อมูล มาตรฐานการรักษาความปลอดภัยในการรับส่งข้อมูล และการพัฒนาระบบให้บริการรับส่งข้อมูลที่กำหนดในแนวปฏิบัติของธนาคารแห่งประเทศไทย รวมถึงที่กำหนดในข้อตกลงร่วมกันระหว่างผู้ให้บริการและผู้ให้บริการระบบทะเบียน

(2) เข้ารับการประเมินคุณสมบัติและความพร้อมกับผู้ให้บริการระบบทะเบียนในส่วนที่เกี่ยวข้องกับการบริหารจัดการและดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ การปฏิบัติตามมาตรฐานอื่นที่กำหนดโดยหน่วยงานที่เกี่ยวข้อง ตามแนวทางที่ผู้ให้บริการระบบทะเบียนกำหนด

(3) เข้ารับการประเมินจากธนาคารแห่งประเทศไทยเกี่ยวกับคุณสมบัติและความพร้อมในการรับส่งข้อมูลตามหลักเกณฑ์ที่กำหนดในประกาศฉบับนี้และตามแนวปฏิบัติที่ธนาคารแห่งประเทศไทยกำหนด โดยยื่นเอกสารที่เกี่ยวข้องมายังธนาคารแห่งประเทศไทยตามรายการและช่องทางที่กำหนดใน

---

[13]ระบบทะเบียนผู้ส่งข้อมูลและผู้รับข้อมูลที่ผ่านการประเมินผลการปฏิบัติตามหลักเกณฑ์และแนวปฏิบัติที่ธนาคารแห่งประเทศไทยกำหนด ซึ่งใช้ตรวจสอบตัวตนของผู้ให้บริการแต่ละฝ่ายก่อนการรับส่งข้อมูลผ่านระบบดิจิทัลในการส่งข้อมูลที่ได้มาตรฐาน

คู่มือประชาชน ทั้งนี้ ธนาคารแห่งประเทศไทยจะพิจารณาด้วยว่าผู้ส่งข้อมูลและผู้รับข้อมูลมีการตกลงหรือใช้บริการผู้ให้บริการระบบทะเบียนที่มีคุณสมบัติและเงื่อนไขการให้บริการตามเอกสารแนบ 4.3 ด้วย

เมื่อผู้ส่งข้อมูลและผู้รับข้อมูลผ่านการทดสอบและการประเมินคุณสมบัติและความพร้อมตามข้อ (1) ถึงข้อ (3) แล้ว ให้ผู้ส่งข้อมูลและผู้รับข้อมูลขึ้นทะเบียนเป็นสมาชิกในระบบทะเบียนกับผู้ให้บริการระบบทะเบียน จึงจะสามารถเริ่มให้บริการรับส่งข้อมูลของผู้ใช้บริการตามประกาศฉบับนี้ได้ ทั้งนี้ เพื่อประโยชน์ในการคุ้มครองผู้บริโภค ธนาคารแห่งประเทศไทยจะเผยแพร่รายชื่อผู้ส่งข้อมูลและผู้รับข้อมูลให้ผู้ใช้บริการทราบ

**เอกสารแนบ 4.1**

**หลักเกณฑ์เกี่ยวกับการขอความยินยอม (consent) การยืนยันการใช้สิทธิส่งข้อมูล (authorization) และการยืนยันตัวตน (authentication) ที่ได้มาตรฐาน สำหรับการรับส่งข้อมูลผ่านระบบดิจิทัลในการส่งข้อมูลที่ได้มาตรฐาน**

**1. การขอ consent จากผู้ใช้บริการ**

เมื่อผู้รับข้อมูลจะเรียกข้อมูลของผู้ใช้บริการจากผู้ส่งข้อมูลตามคำขอใช้สิทธิส่งข้อมูลของผู้ใช้บริการ ผู้รับข้อมูลต้องขอ consent จากผู้ใช้บริการ โดยดำเนินการอย่างน้อยดังต่อไปนี้

1.1 ผู้รับข้อมูลต้องแยกข้อความการขอ consent ให้ส่งข้อมูล ออกจากข้อความอื่น และการขอ consent ในเรื่องอื่น ๆ อย่างชัดเจน

1.2 ผู้รับข้อมูลต้องระบุข้อมูลอย่างน้อยดังต่อไปนี้ในข้อความการขอ consent

1.2.1 ประเภทและรายการข้อมูลที่ขอให้ผู้ใช้บริการให้ consent รวมถึงชื่อผู้ส่งข้อมูลและผู้รับข้อมูลที่จะส่งหรือรับข้อมูลนั้น

1.2.2 วัตถุประสงค์การใช้ข้อมูล โดยต้องจัดให้มีการระบุวัตถุประสงค์เกี่ยวข้องกับการให้บริการหรือการทำธุรกรรมที่ผู้ใช้บริการขอใช้บริการกับผู้รับข้อมูล และต้องอยู่ภายใต้ขอบเขตธุรกิจที่กำหนดในกฎหมายที่ใช้กำกับดูแลผู้รับข้อมูล หรือภายใต้ขอบเขตธุรกิจที่ได้รับอนุญาตจากหน่วยงานกำกับดูแลเท่านั้น

1.2.3 ระยะเวลาการขอ consent โดยต้องจัดให้มีการระบุระยะเวลาให้สอดคล้องกับวัตถุประสงค์การใช้ข้อมูล โดยอาจขอ consent เพื่อรองรับการเรียกข้อมูลของผู้ใช้บริการครั้งเดียวหรือไม่จำกัดจำนวนครั้งภายในช่วงเวลาที่กำหนดก็ได้ โดยในกรณีที่ขอ consent แบบเป็นช่วงเวลา ต้องมีกำหนดเวลาสิ้นสุดที่ไม่ยาวนานเกินไป เพื่อให้ผู้ใช้บริการได้มีโอกาสทบทวนความจำเป็นและความเหมาะสมของการให้ consent ดังกล่าว

ทั้งนี้ รูปแบบและมาตรฐานกลางในการขอ consent ให้เป็นไปตามแนวปฏิบัติที่ธนาคารแห่งประเทศไทยกำหนด

1.3 กรณีที่ผู้รับข้อมูลมีการใช้บริการบุคคลอื่นเพื่อสนับสนุนการดำเนินการรับข้อมูลผ่านระบบส่งข้อมูลดิจิทัลที่ได้มาตรฐาน ผู้รับข้อมูลต้องแจ้งให้ผู้ใช้บริการทราบถึงชื่อและบทบาทของบุคคลดังกล่าวในการบริหารจัดการข้อมูลของผู้ใช้บริการในส่วนที่เกี่ยวข้องกับผู้รับข้อมูล เช่น บุคคลภายนอกที่ผู้รับข้อมูล

ว่าจ้างมาทำหน้าที่เก็บรวบรวม ประมวลผลข้อมูลของผู้ใช้บริการ หรือช่วยเชื่อมต่อกับระบบหรือผู้ให้บริการรายอื่นเพื่อรับส่งข้อมูลตามคำขอใช้สิทธิส่งข้อมูลและ consent ของผู้ใช้บริการโดยดำเนินการดังนี้

1.3.1 แจ้งชื่อและบทบาทของบุคคลที่เกี่ยวข้องดังกล่าว โดยต้องมีความครบถ้วน ถูกต้อง ชัดเจน เข้าใจได้ง่าย และปรับให้เป็นปัจจุบันอยู่เสมอ

1.3.2 ในการแจ้งให้ผู้ใช้บริการทราบข้อมูลตามข้อ 1.3.1 ผู้รับข้อมูลต้องแจ้งให้ผู้ใช้บริการทราบผ่านช่องทางที่ผู้ใช้บริการสามารถเข้าถึงได้โดยง่าย เห็นได้อย่างชัดเจน และไม่เกิดความสับสนหรือปะปนกับข้อมูลอื่น ๆ เช่น หากผู้รับข้อมูลมีการแจ้งข้อมูลผู้ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลของผู้ใช้บริการผ่านประกาศความเป็นส่วนตัว (privacy notice) อยู่แล้ว ผู้รับข้อมูลควรแยกการแจ้งข้อมูลตาม 1.3.1 ออกจากการแจ้งในเรื่องอื่น ๆ ทั้งนี้ ในกรณีที่ผู้รับข้อมูลมีช่องทางที่ใช้ในการเผยแพร่ชื่อและบทบาทของผู้ที่เกี่ยวข้องดังกล่าว (เช่น เว็บไซต์ของผู้รับข้อมูล) และเป็นช่องทางที่ผู้ใช้บริการเข้าถึงข้อมูลดังกล่าวได้โดยง่ายอยู่แล้ว ผู้รับข้อมูลอาจแจ้งให้ผู้ใช้บริการทราบถึงการมีและวิธีการเข้าถึงช่องทางการเผยแพร่ข้อมูลดังกล่าว โดยแจ้งผ่านช่องทางที่การใช้บริการหรือช่องทางหลักที่ผู้ใช้บริการใช้ในการติดต่อกับผู้รับข้อมูล

1.3.3 เมื่อมีการเปลี่ยนแปลงชื่อบุคคลที่เกี่ยวข้องตามข้อ 1.3.1 ให้ผู้รับข้อมูลแจ้งให้ผู้ใช้บริการทราบถึงชื่อที่เป็นปัจจุบันล่วงหน้าในระยะเวลาที่เพียงพอ

1.4 ผู้รับข้อมูลต้องแจ้งสิทธิและช่องทางการถอนและเปลี่ยนแปลง consent ให้ผู้ใช้บริการทราบผ่านช่องทางเดียวกับการแจ้งข้อมูลในข้อ 1.3.2

**2. การขอ authorization จากผู้ใช้บริการ**

**เมื่อผู้ส่งข้อมูลจะส่งข้อมูลตามคำขอใช้สิทธิส่งข้อมูลที่ผู้ใช้บริการได้ให้ consent แล้ว** ผู้ส่งข้อมูลต้องขอ authorization จากผู้ใช้บริการ โดยดำเนินการอย่างน้อยดังต่อไปนี้

2.1 ผู้ส่งข้อมูลต้องแยกข้อความการขอ authorization ภายใต้ประกาศฉบับนี้ออกจากข้อความอื่นและการขอ authorization ในเรื่องอื่น ๆ อย่างชัดเจน

2.2 ผู้ส่งข้อมูลต้องระบุข้อมูลอย่างน้อยในลักษณะเดียวกับข้อ 1.2.1 และ 1.2.2 ในข้อความการขอ authorization และมีการกำหนดระยะเวลาการให้ authorization ที่เหมาะสมกับวัตถุประสงค์การใช้ข้อมูลและสอดคล้องกับช่วงเวลาการให้ consent ตามข้อ 1.2.3

2.3 กรณีที่ผู้ส่งข้อมูลมีการใช้บริการบุคคลอื่นเพื่อสนับสนุนการดำเนินการส่งข้อมูลผ่านระบบส่งข้อมูลดิจิทัลที่ได้มาตรฐาน ผู้ส่งข้อมูลต้องแจ้งให้ผู้ใช้บริการทราบถึงชื่อและบทบาทของบุคคลที่เกี่ยวข้องในการบริหารจัดการข้อมูลของผู้ใช้บริการในส่วนของผู้ส่งข้อมูล โดยให้นำข้อ 1.3 มาใช้บังคับโดยอนุโลม

**3. การบริหารจัดการและตรวจสอบ consent และ authorization**

เมื่อผู้ใช้บริการใช้สิทธิส่งข้อมูลของผู้ใช้บริการแล้ว ผู้ส่งข้อมูลและผู้รับข้อมูลต้องดำเนินการให้ผู้ใช้บริการสามารถบริหารจัดการและตรวจสอบ consent และ authorization ของตนได้ง่ายและสะดวก รวมทั้งต้องแจ้งให้ผู้ที่เกี่ยวข้องทราบถึงการดำเนินการของผู้ใช้บริการที่เกี่ยวกับการเปลี่ยนแปลงและการถอน consent และ authorization ด้วย ดังนี้

3.1 ผู้ส่งข้อมูลและผู้รับข้อมูลต้องให้หลักฐานการให้ การเปลี่ยนแปลง และการถอน consent และ authorization แก่ผู้ใช้บริการ แล้วแต่กรณี ตามช่องทางที่ผู้ใช้บริการได้แจ้งไว้ เช่น อีเมล แอปพลิเคชันมือถือ หรือช่องทางให้บริการของผู้ส่งข้อมูลและผู้รับข้อมูล เพื่อให้ผู้ใช้บริการสามารถตรวจสอบได้

3.2 ผู้ส่งข้อมูลและผู้รับข้อมูลต้องจัดให้มีช่องทางที่ง่ายและสะดวกให้ผู้ใช้บริการบริหารจัดการ consent และ authorization ของผู้ใช้บริการ ในแต่ละกรณี เพื่อรองรับการเปลี่ยนแปลงและ/หรือการถอน consent และ authorization ดังกล่าว รวมทั้งมีช่องทางให้ผู้ใช้บริการสามารถตรวจสอบถึงการมีอยู่และการหมดอายุของ consent และ authorization ทั้งนี้ ผู้ส่งข้อมูลและผู้รับข้อมูลต้องแจ้งให้ผู้ใช้บริการทราบถึงการหมดอายุของ consent และ authorization แล้วแต่กรณี โดยรูปแบบและระยะเวลาในการแจ้งให้ผู้ใช้บริการทราบให้ถือปฏิบัติตามแนวปฏิบัติที่ธนาคารแห่งประเทศไทยกำหนด

3.3 ผู้ส่งข้อมูลและผู้รับข้อมูลต้องแจ้งให้อีกฝ่ายทราบเมื่อ consent และ authorization มีการเปลี่ยนแปลงหรือถูกถอน แล้วแต่กรณี เพื่อไม่ให้มีการเรียก ใช้ หรือส่งข้อมูลของผู้ใช้บริการ โดยที่ผู้ใช้บริการไม่ได้ยินยอม หรือไม่ได้ยืนยันการใช้สิทธิในการส่งข้อมูล ทั้งนี้ รูปแบบและระยะเวลาในการแจ้งให้ผู้ให้บริการอีกฝ่ายทราบให้ถือปฏิบัติตามแนวปฏิบัติที่ธนาคารแห่งประเทศไทยกำหนด

**4. การ authentication ผู้ใช้บริการ**

ในการดำเนินการตามคำขอใช้สิทธิส่งข้อมูล รวมถึงการขอและบริหารจัดการ consent และ authorization ของผู้ใช้บริการ ผู้ให้บริการต้องจัดให้มีกระบวนการ authentication ที่ได้มาตรฐาน มีความน่าเชื่อถือ ตรวจสอบได้ เช่น ดำเนินการผ่านระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ได้รับการรับรองมาตรฐานจากหน่วยงานที่น่าเชื่อถือหรือได้รับการยอมรับจากผู้ให้บริการและมีการใช้งานระบบดังกล่าวในวงกว้าง รวมทั้ง ในกระบวนการดังกล่าวผู้ให้บริการต้องจัดให้มีการกำหนดความรับผิดที่ชัดเจนด้วย ทั้งนี้ ต้องมีระดับการพิสูจน์และยืนยันตัวตนที่ไม่สูงเกินไปจนเป็นอุปสรรคต่อการใช้สิทธิของผู้ใช้บริการและไม่ต่ำเกินไปจนทำให้เกิดความเสี่ยงที่ผู้ทำธุรกรรมไม่ใช่ผู้ใช้บริการรายที่เป็นเจ้าของข้อมูลจริง

**เอกสารแนบ 4.2**

**มาตรฐานขั้นต่ำเรื่องการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ**
**ที่เกี่ยวข้องกับการจัดการข้อมูลสำหรับการรับส่งข้อมูลผ่านระบบดิจิทัลในการส่งข้อมูลที่ได้มาตรฐาน**

ผู้ส่งข้อมูลและผู้รับข้อมูลผ่านระบบดิจิทัลในการส่งข้อมูลที่ได้มาตรฐานที่มิใช่สถาบันการเงินและมิใช่ผู้ประกอบธุรกิจบริการการชำระเงินที่ต้องถือปฏิบัติตามหลักเกณฑ์ทุกข้อตามประกาศธนาคารแห่งประเทศไทยว่าด้วยหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ตามกฎหมายว่าด้วยระบบการชำระเงิน ให้ถือปฏิบัติตามมาตรฐานขั้นต่ำเรื่องการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับการจัดการข้อมูลสำหรับการรับส่งข้อมูลผ่านระบบดิจิทัลในการส่งข้อมูลที่ได้มาตรฐานที่ธนาคารแห่งประเทศไทยกำหนด ดังนี้

**1. การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT asset management)**

บริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม โดยต้องจัดทำทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศให้ครบถ้วน เช่น อุปกรณ์คอมพิวเตอร์ ระบบปฏิบัติการ และระบบงาน (hardware and software) เพื่อให้สามารถนำไปใช้กำหนดแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศได้อย่างเหมาะสม นอกจากนี้ ต้องบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ รวมถึงบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ใกล้หมดอายุการใช้งานหรือสิ้นสุดการให้บริการอย่างเหมาะสมและเท่าทันกับความเสี่ยง

**2. การรักษาความมั่นคงปลอดภัยของข้อมูล (information security)**

รักษาความมั่นคงปลอดภัยของข้อมูล ทั้งการรับส่งข้อมูลผ่านระบบเครือข่ายสื่อสารและการจัดเก็บข้อมูลบนระบบงานและสื่อบันทึกข้อมูลต่าง ๆ มีการจัดชั้นความลับของข้อมูล (information classification) เก็บรักษาและทำลายข้อมูลให้เหมาะสมตามระดับชั้นความลับ รวมทั้งจัดให้มีกระบวนการบริหารจัดการการเข้ารหัสข้อมูล (cryptography) ที่เชื่อถือได้และเป็นมาตรฐานสากลที่ยอมรับโดยทั่วไป เพื่อรักษาความมั่นคงปลอดภัยและความลับของข้อมูล

**3. การควบคุมการเข้าถึง (access control)**

ควบคุมการเข้าถึงระบบปฏิบัติการ (operating system) ระบบงาน (application) และระบบฐานข้อมูล (database system) โดยกำหนดให้มีการบริหารจัดการสิทธิตามความจำเป็นในการใช้งานและระดับความเสี่ยง (least privilege) และตรวจสอบยืนยันตัวตนตามสิทธิที่กำหนดไว้ เพื่อป้องกันการเข้าถึงและเปลี่ยนแปลงระบบหรือข้อมูลโดยผู้ที่ไม่มีสิทธิ โดยต้องครอบคลุมอย่างน้อย ดังนี้

3.1 การบริหารจัดการบัญชีผู้ใช้งานที่มีสิทธิสูง (privileged user management) ต้องมีการกำหนดมาตรการควบคุมและจำกัดการใช้บัญชีอย่างเข้มงวด เช่น การมอบหมายสิทธิ การเบิกใช้ การกำหนดระยะเวลาการใช้งาน และการสอบทานหลังการใช้ เพื่อป้องกันการเข้าถึงและเปลี่ยนแปลงระบบหรือข้อมูลโดยผู้ที่ไม่มีสิทธิหรือไม่ได้รับอนุญาต

3.2 จัดให้มีการพิสูจน์ตัวตนแบบ multi-factor authentication ในกรณีดังต่อไปนี้

3.2.1 บัญชีผู้ใช้งานที่มีสิทธิสูง (privileged user) ทุกบัญชีของระบบปฏิบัติการ ระบบงาน ระบบฐานข้อมูล อุปกรณ์เครือข่ายและอุปกรณ์รักษาความปลอดภัยเครือข่าย

3.2.2 บัญชีผู้ใช้งาน (user) ทุกบัญชีที่สามารถเข้าถึงข้อมูลของผู้ใช้บริการและเชื่อมต่อมาจากระบบเครือข่ายสื่อสารสาธารณะ (internet facing)

ในกรณีที่ระบบปฏิบัติการ ระบบงาน ระบบฐานข้อมูล อุปกรณ์เครือข่ายและอุปกรณ์รักษาความปลอดภัยเครือข่าย ไม่รองรับการพิสูจน์ตัวตนแบบ multi-factor authentication ผู้ส่งข้อมูลและผู้รับข้อมูลต้องจัดให้มีวิธีการอื่นใดที่มีประสิทธิภาพเทียบเท่าทดแทน เพื่อลดความเสี่ยงจากการถูกโจมตีการพิสูจน์ตัวตนได้โดยง่าย

อย่างไรก็ตาม กรณีที่ไม่สามารถปฏิบัติตามได้ในบางระบบหรืออุปกรณ์ ต้องจัดให้มีกระบวนการขออนุมัติยกเว้นและดำเนินการประเมินความเสี่ยง รวมทั้งพิจารณาแนวทางควบคุมความเสี่ยงอย่างเพียงพอเหมาะสม

**4. การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (communications security)**

จัดให้มีการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร เพื่อให้ระบบเครือข่ายสื่อสารและข้อมูลที่รับส่งผ่านระบบเครือข่ายสื่อสารมีความมั่นคงปลอดภัย สามารถป้องกันการบุกรุกหรือภัยคุกคามที่อาจเกิดขึ้น

**5. การรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงานของผู้ใช้เทคโนโลยีสารสนเทศ (endpoint)**

จัดให้มีการรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงานของผู้ใช้เทคโนโลยีสารสนเทศ (endpoint) ให้สามารถป้องกันภัยจากโปรแกรมไม่ประสงค์ดี (malware) รวมทั้งติดตามปรับปรุงให้เป็นปัจจุบันและเท่าทันภัยคุกคามใหม่อย่างสม่ำเสมอ เพื่อเป็นการลดความเสี่ยงจากการถูกโจมตี และป้องกันการรั่วไหลของข้อมูลหรือการเข้าใช้งานโดยไม่ได้รับอนุญาต

**6. การกำหนดมาตรฐานด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (security baseline and hardening)**

จัดให้มีการกำหนดมาตรฐานการรักษาความมั่นคงปลอดภัยขั้นต่ำ (minimum security baseline) และกระบวนการตั้งค่าการรักษาความมั่นคงปลอดภัยที่สอดคล้องกับมาตรฐานดังกล่าว (security hardening) ครอบคลุมระบบปฏิบัติการ ระบบงาน ระบบฐานข้อมูล อุปกรณ์เครือข่ายและอุปกรณ์รักษาความปลอดภัยเครือข่ายที่รองรับการให้บริการ ให้ชัดเจนและเป็นลายลักษณ์อักษร รวมทั้งดำเนินการตั้งค่าและสอบทานการตั้งค่าอย่างสม่ำเสมอตามที่ได้กำหนดไว้ เพื่อให้มั่นใจว่าระบบงานที่รองรับการให้บริการมีการรักษาความมั่นคงปลอดภัยขั้นต่ำตามมาตรฐานที่กำหนดไว้

ในกรณีที่ผู้ส่งข้อมูลและผู้รับข้อมูลไม่สามารถปฏิบัติตามมาตรฐานที่ตนได้กำหนดไว้ข้างต้น ต้องจัดให้มีกระบวนการขออนุมัติยกเว้นสำหรับระบบหรืออุปกรณ์ที่มีข้อจำกัดในการดำเนินการ และดำเนินการประเมินความเสี่ยง รวมทั้งพิจารณาแนวทางควบคุมความเสี่ยงอย่างเพียงพอเหมาะสม

**7. การสำรองข้อมูล (data backup)**

สำรองข้อมูลด้วยวิธีการและระยะเวลาที่เหมาะสม เช่น การสำรองข้อมูลประจำวัน เพื่อให้มีข้อมูลสำรองที่มีความพร้อมใช้งานในกรณีที่ระบบและข้อมูลหลักเกิดเหตุขัดข้องหรือได้รับความเสียหาย

**8. การบริหารจัดการการเปลี่ยนแปลงด้านระบบเทคโนโลยีสารสนเทศ (IT change management)**

จัดให้มีกระบวนการบริหารจัดการการเปลี่ยนแปลงและควบคุมการเปลี่ยนแปลงอย่างรัดกุมและเพียงพอ เช่น การนำระบบขึ้นใช้งานจริง (system deployment) การตั้งค่าระบบ (system configuration) และการติดตั้ง patch เพื่อให้การเปลี่ยนแปลงเป็นไปตามวัตถุประสงค์ที่กำหนดไว้อย่างถูกต้องครบถ้วน และป้องกันการเปลี่ยนแปลงโดยไม่ได้รับอนุญาต

**9. การบริหารจัดการ security patch (security patch management)**

จัดให้มีกระบวนการบริหารจัดการ security patch สำหรับทุกระบบงานและอุปกรณ์ที่รองรับการให้บริการ เพื่อลดความเสี่ยงที่ระบบเทคโนโลยีสารสนเทศถูกโจมตีจากช่องโหว่ใหม่ ๆ โดยต้องดำเนินการให้แล้วเสร็จในระยะเวลาที่เหมาะสมตามระดับความเสี่ยงของช่องโหว่และระดับความสำคัญของระบบงาน

ในกรณีที่ผู้ผลิตระบบงานหรืออุปกรณ์ยังไม่แจ้งการปรับปรุง security patch อย่างเป็นทางการเพื่อปิดช่องโหว่ใหม่ ๆ ที่เพิ่งค้นพบ ผู้ส่งข้อมูลและผู้รับข้อมูลต้องจัดให้มีการควบคุมอื่นทดแทน เพื่อลดความเสี่ยงจากการถูกโจมตีจากช่องโหว่นั้น ๆ

นอกจากนี้ กรณีที่ไม่สามารถติดตั้ง security patch ได้ ต้องจัดให้มีกระบวนการขออนุมัติยกเว้นและดำเนินการประเมินความเสี่ยง รวมทั้งพิจารณาแนวทางควบคุมความเสี่ยงอย่างเพียงพอเหมาะสม เพื่อลดความเสี่ยงที่ระบบเทคโนโลยีสารสนเทศจะถูกโจมตี

**10. การติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม (security monitoring)**

จัดให้มีการติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม โดยมีกระบวนการหรือเครื่องมือสำหรับติดตามภัยคุกคามใหม่ ๆ และตรวจจับเหตุการณ์ผิดปกติหรือภัยคุกคามที่มีผลกระทบต่อความมั่นคงปลอดภัยของระบบที่รองรับการให้บริการ เช่น เครื่องมือติดตามและวิเคราะห์ภัยคุกคามทางไซเบอร์ เพื่อให้สามารถตรวจจับ ป้องกัน และรับมือเหตุการณ์ผิดปกติและภัยคุกคามได้อย่างทันท่วงที

**11. การบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ (vulnerability management and penetration testing)**

จัดให้มีการประเมินช่องโหว่ (vulnerability assessment) สำหรับทุกระบบงานตามระดับความเสี่ยง โดยต้องดำเนินการอย่างน้อยปีละ 1 ครั้ง สำหรับระบบงานสำคัญ และต้องดำเนินการเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ รวมทั้งจัดให้มีการทดสอบเจาะระบบ (penetration testing) โดยผู้เชี่ยวชาญภายในหรือภายนอกที่มีความเป็นอิสระ ซึ่งอย่างน้อยครอบคลุมระบบงานและระบบเครือข่ายที่มีการเชื่อมต่อกับเครือข่ายสื่อสารสาธารณะ (internet facing) เช่น ระบบที่ให้หรือใช้บริการ API ในการเชื่อมต่อและรับส่งข้อมูลกับภายนอกสม่ำเสมออย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญของระบบ ความเสี่ยง หรือมาตรฐานสากลด้านเทคโนโลยีสารสนเทศ เพื่อให้ทราบถึงช่องโหว่และสามารถดำเนินการแก้ไขและป้องกันภัยคุกคามที่อาจเกิดขึ้นได้อย่างทันการณ์

ทั้งนี้ ในกรณีที่ธนาคารแห่งประเทศไทยเห็นว่าผลการทดสอบเจาะระบบ มีข้อมูลรายงานไม่ครบถ้วน ขอบเขตหรือวิธีการทดสอบเจาะระบบไม่ครอบคลุมช่องโหว่สำคัญที่เป็นความเสี่ยงที่ได้รับการยอมรับโดยทั่วไป หรือในกรณีที่ธนาคารแห่งประเทศไทยเห็นว่าจำเป็นหรือสมควร ธนาคารแห่งประเทศไทยอาจสั่งให้ผู้ส่งข้อมูลหรือผู้รับข้อมูลแต่งตั้งผู้เชี่ยวชาญภายนอกที่มีความเป็นอิสระดำเนินการทดสอบเจาะระบบเพิ่มเติมได้

**12. การจัดหาและการพัฒนาระบบ (system acquisition and development)**

**12.1 การจัดหาระบบ (system acquisition)**

กำหนดหลักเกณฑ์ที่ชัดเจนและเหมาะสมในการคัดเลือกระบบและบุคคลภายนอกที่ให้บริการ เช่น ความน่าเชื่อถือของระบบ ความมั่นคงปลอดภัยของระบบ การสนับสนุนและการบำรุงรักษาระบบ บุคคลภายนอกที่ให้บริการที่ได้รับการรับรองตามมาตรฐานสากลที่ได้รับการยอมรับโดยทั่วไป (certificate)

เพื่อให้มั่นใจว่าระบบและบุคคลภายนอกที่ให้บริการสามารถตอบสนองต่อความต้องการในการดำเนินการได้ รวมถึงต้องคำนึงถึงความยืดหยุ่นในการเปลี่ยนแปลงผู้ให้บริการที่เป็นบุคคลภายนอก การเปลี่ยนแปลงเทคโนโลยีสารสนเทศ หรือการเปลี่ยนแปลงกลยุทธ์ในการให้บริการหรือดำเนินธุรกิจในอนาคต

**12.2 การพัฒนาระบบ (system development)**

ออกแบบ พัฒนา และทดสอบระบบ เพื่อให้มั่นใจว่าระบบมีการรักษาความลับของระบบและข้อมูลมีความถูกต้องเชื่อถือได้ พร้อมใช้งาน และมีความยืดหยุ่นเพียงพอที่จะรองรับการปรับปรุงเปลี่ยนแปลงระบบในอนาคต โดยต้องดำเนินการอย่างน้อยในเรื่องต่อไปนี้

- มีรายละเอียดคุณสมบัติทางเทคนิค (technical specification) โดยครอบคลุมถึงเรื่องการรักษาความมั่นคงปลอดภัย ซึ่งรวมถึงกระบวนการทดสอบ การดูแล และการติดตามความมั่นคงปลอดภัยในการใช้งาน

- มีกระบวนการหรือเครื่องมือควบคุมเวอร์ชันของคำสั่งเขียนโปรแกรม (source code version control)

- แบ่งแยกบทบาทหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องในกระบวนการพัฒนาระบบ เช่น การแบ่งแยกระหว่างผู้พัฒนาระบบและผู้นำระบบขึ้นใช้งานจริง

- แบ่งแยกสภาพแวดล้อมของระบบงานที่ใช้สำหรับการพัฒนา (development) และการทดสอบ (testing) ออกจากระบบงานที่ให้บริการจริง (production)

- ทดสอบระบบก่อนการใช้งานจริง เช่น ทดสอบการทำงานของแต่ละระบบ (unit test) ทดสอบการทำงานร่วมกันของระบบต่าง ๆ (system integration test) ทดสอบความต้องการของผู้ใช้งาน (user acceptance test) และทดสอบความปลอดภัยของระบบ (security test) ตามกระบวนการรักษาความมั่นคงปลอดภัยที่กำหนดในเอกสารรายละเอียดคุณสมบัติทางเทคนิค (technical specification)

- มีแนวทางควบคุมการรักษาความมั่นคงปลอดภัยและความลับของข้อมูลสำคัญที่นำไปใช้ทดสอบระบบ

- จัดทำคู่มือและอบรมผู้ใช้งานระบบและผู้ดูแลระบบ

**13. การบริหารจัดการความเสี่ยงจากบุคคลภายนอก (third party risk management)**

ในกรณีที่ผู้ส่งข้อมูลและผู้รับข้อมูลดำเนินการดังต่อไปนี้ (1) ใช้บริการงานด้านเทคโนโลยีสารสนเทศจากบุคคลภายนอก (IT outsourcing) (2) เชื่อมต่อระบบเทคโนโลยีสารสนเทศกับบุคคลภายนอก หรือ

(3) ให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญ หรือเข้าถึงข้อมูลผู้ใช้บริการ ผู้ส่งข้อมูลและผู้รับข้อมูลต้องกำกับดูแลความเสี่ยง การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการรักษาความปลอดภัยจากภัยไซเบอร์ ให้สอดคล้องตามระดับความเสี่ยงบนพื้นฐานที่ต้องรับผิดชอบต่อการให้บริการหรือดำเนินธุรกิจแก่ผู้ใช้บริการและคงไว้ซึ่งความน่าเชื่อถือ ชื่อเสียง ประสิทธิภาพในการให้บริการ ตามหลักการดังนี้

13.1 กำหนดบทบาท หน้าที่ และความรับผิดชอบระหว่างผู้ส่งข้อมูลหรือผู้รับข้อมูลกับบุคคลภายนอกอย่างชัดเจนและเป็นลายลักษณ์อักษร และพร้อมสำหรับการตรวจสอบหรือเมื่อร้องขอโดยธนาคารแห่งประเทศไทย สำหรับกรณีบุคคลภายนอกที่ให้บริการงานด้านเทคโนโลยีสารสนเทศ (IT outsourcing) ที่มีนัยสำคัญ ต้องระบุให้ผู้ตรวจสอบภายใน ผู้ตรวจสอบภายนอก และธนาคารแห่งประเทศไทยมีสิทธิเข้าตรวจสอบการดำเนินการด้านเทคโนโลยีสารสนเทศของบุคคลภายนอกรายดังกล่าวเป็นเงื่อนไขในสัญญาหรือข้อตกลง ระหว่างผู้ส่งข้อมูลหรือผู้รับข้อมูลกับบุคคลภายนอกดังกล่าวด้วย

สำหรับกรณีที่ไม่สามารถระบุสิทธิให้ผู้ตรวจสอบภายใน ผู้ตรวจสอบภายนอก มีสิทธิเข้าตรวจสอบการดำเนินการด้านเทคโนโลยีสารสนเทศของบุคคลภายนอกที่ให้บริการงานด้านเทคโนโลยีสารสนเทศ (IT outsourcing) ในเงื่อนไขสัญญาหรือข้อตกลงกับบุคคลภายนอก ผู้ส่งข้อมูลและผู้รับข้อมูลต้องมั่นใจว่าบุคคลภายนอกรายดังกล่าวมีผลการตรวจสอบจากผู้ตรวจสอบภายนอกที่เป็นอิสระทดแทน

13.2 กำกับดูแล ติดตาม และบริหารจัดการความเสี่ยงจากการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก สอดคล้องตามระดับความเสี่ยงและระดับความมีนัยสำคัญ

13.3 รักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ที่สอดคล้องกับมาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการรักษาความปลอดภัยจากภัยไซเบอร์ของผู้ส่งข้อมูลและผู้รับข้อมูล และสอดคล้องกับมาตรฐานสากลที่ได้รับการยอมรับโดยทั่วไป

13.4 เตรียมความพร้อมรับมือต่อเหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบอย่างมีนัยสำคัญ เพื่อให้สามารถให้บริการหรือดำเนินธุรกิจได้อย่างต่อเนื่อง รวมถึงมีข้อมูลพร้อมใช้สำหรับการให้บริการหรือดำเนินธุรกิจแก่ผู้ใช้บริการ

**14. การจัดเก็บข้อมูลบันทึกเหตุการณ์ (logging)**

จัดเก็บ logging ของเครื่องแม่ข่าย ระบบงาน และอุปกรณ์เครือข่ายที่สำคัญ เช่น การจัดเก็บและสอบทานบันทึกการเข้าถึงระบบ (access log) และบันทึกการดำเนินงาน (activity log) เพื่อให้สามารถใช้ติดตามและตรวจสอบร่องรอยการเข้าถึงและการใช้งานระบบหรือข้อมูลที่รองรับการให้บริการ รวมทั้งสามารถใช้เป็นหลักฐานการทำธุรกรรมทางอิเล็กทรอนิกส์ได้ตามที่กฎหมายกำหนด

**เอกสารแนบ 4.3**

**คุณสมบัติและเงื่อนไขการให้บริการของผู้ให้บริการระบบทะเบียน**

ผู้ส่งข้อมูลและผู้รับข้อมูลต้องเลือกใช้บริการและเข้ารับการทดสอบและประเมินคุณสมบัติและความพร้อมกับผู้ให้บริการระบบทะเบียนที่มีคุณสมบัติและเงื่อนไขในการให้บริการอย่างน้อยดังต่อไปนี้ เพื่อให้มั่นใจว่าผู้ให้บริการระบบทะเบียนสามารถให้บริการ รวมทั้งสามารถทดสอบและประเมินผลให้ผู้ส่งข้อมูลและผู้รับข้อมูลสามารถปฏิบัติตามมาตรฐานและแนวปฏิบัติที่ธนาคารแห่งประเทศไทยกำหนดได้

1. ผู้ให้บริการระบบทะเบียนต้องมีมาตรการในการกำกับดูแลความเสี่ยงที่เกี่ยวข้องกับบริการระบบทะเบียน เช่น มาตรการดูแลความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security) มาตรการดูแลความปลอดภัยของข้อมูล (data security) รวมถึงมีกระบวนการตรวจสอบด้านเทคโนโลยีสารสนเทศโดยผู้เชี่ยวชาญภายนอกที่มีความเป็นอิสระ

2. ผู้ให้บริการระบบทะเบียนต้องมีความผูกพันที่จะรับผิดต่อความเสียหายที่เกิดขึ้นจากความบกพร่องหรือความผิดพลาดของการให้บริการตามบทบาทและหน้าที่ที่มีการตกลงกับผู้ส่งข้อมูลและผู้รับข้อมูลหรือบุคคลอื่นที่เกี่ยวข้องกับการให้บริการรับส่งข้อมูลตามประกาศฉบับนี้

3. ผู้ให้บริการระบบทะเบียนต้องพร้อมรองรับให้ผู้ส่งข้อมูลและผู้รับข้อมูลทุกแห่งที่เป็นผู้ให้บริการทางการเงิน รวมถึงผู้ให้บริการภายใต้การกำกับดูแลของหน่วยงานอื่น ที่มีคุณสมบัติและความพร้อมสามารถเข้าร่วมเป็นสมาชิกระบบทะเบียนดังกล่าว รวมทั้งต้องมีความสามารถและความพร้อมในการให้บริการภายใต้ประกาศฉบับนี้แก่สมาชิกระบบทะเบียนด้วย ตลอดจนมีแนวทางที่ผู้ส่งข้อมูลและผู้รับข้อมูลขนาดกลางและขนาดเล็กสามารถใช้บริการได้สะดวกด้วยภาระที่เหมาะสมกับขนาดและลักษณะธุรกิจของผู้ส่งข้อมูลและผู้รับข้อมูล

4. ผู้ให้บริการระบบทะเบียนต้องไม่กำหนดเงื่อนไขหรือเรียกเก็บค่าธรรมเนียมการให้บริการที่สร้างภาระต้นทุนต่อผู้ส่งข้อมูลและผู้รับข้อมูลมากเกินความจำเป็น จนผู้รับข้อมูลจำนวนมากเลือกที่จะไม่รับข้อมูลผ่านกลไกส่งข้อมูลทางดิจิทัลเพื่อนำไปพัฒนาบริการและทำให้ไม่สามารถบรรลุเป้าประสงค์ของประกาศฉบับนี้ ทั้งนี้ ค่าธรรมเนียมที่จะเรียกเก็บข้างต้นต้องสะท้อนต้นทุนที่เกิดขึ้นจริงและสมควรแก่เหตุ โดยนำเฉพาะต้นทุนส่วนเพิ่มอันเนื่องมาจากการให้บริการภายใต้ประกาศฉบับนี้มาใช้ในการพิจารณากำหนดค่าธรรมเนียมดังกล่าว ซึ่งไม่รวมถึงต้นทุนส่วนที่สามารถนำไปใช้เพื่อประโยชน์อื่นของผู้ให้บริการระบบทะเบียน รวมทั้งยังต้องมีการทบทวนค่าธรรมเนียมเป็นระยะเพื่อให้ยังคงสอดคล้องกับหลักการที่กำหนดข้างต้น

นอกจากนี้ ในการกำหนดหรือเปลี่ยนแปลงค่าธรรมเนียม ผู้ให้บริการระบบทะเบียนต้องมีการรับฟังและนำความคิดเห็นจากสมาชิกระบบทะเบียนที่เป็นผู้รับข้อมูลและผู้ส่งข้อมูลภายใต้ประกาศฉบับนี้ไปประกอบการพิจารณากำหนดหรือเปลี่ยนแปลงค่าธรรมเนียมด้วย และต้องใช้โครงสร้างค่าธรรมเนียมเดียวกันสำหรับผู้ให้บริการที่เข้าเงื่อนไขเดียวกัน

5. ผู้ให้บริการระบบทะเบียนต้องมีความสามารถให้บริการทดสอบและประเมินความสามารถของผู้ส่งข้อมูลและผู้รับข้อมูลในการปฏิบัติตามมาตรฐานและแนวปฏิบัติที่ธนาคารแห่งประเทศไทยกำหนด รวมทั้งเมื่อมาตรฐานและแนวปฏิบัติดังกล่าวมีการเปลี่ยนแปลง และต้องกำหนดข้อตกลงหรือสัญญากับผู้ส่งข้อมูลและผู้รับข้อมูลให้ผู้ให้บริการระบบทะเบียนทดสอบและประเมินผู้ส่งข้อมูลและผู้รับข้อมูลเป็นระยะได้ ทั้งนี้ เพื่อให้มั่นใจว่าผู้ให้บริการระบบทะเบียนสามารถทดสอบและประเมินผลให้ผู้ส่งข้อมูลและผู้รับข้อมูลสามารถปฏิบัติตามมาตรฐานและแนวปฏิบัติที่ธนาคารแห่งประเทศไทยกำหนดได้อย่างต่อเนื่อง

6. ผู้ให้บริการระบบทะเบียนต้องมีระบบที่รองรับการตรวจสอบตัวตนและข้อมูลที่เกี่ยวข้องกับผู้ส่งข้อมูลและผู้รับข้อมูล

7. ผู้ให้บริการระบบทะเบียนต้องสามารถสนับสนุนการกำกับดูแลของธนาคารแห่งประเทศไทย โดยต้องสามารถระงับการรับส่งข้อมูลของผู้ส่งข้อมูลหรือผู้รับข้อมูลเป็นการชั่วคราว หรือถอนรายชื่อผู้ส่งข้อมูลหรือผู้รับข้อมูลออกจากระบบทะเบียน ในกรณีที่ปรากฏข้อเท็จจริงว่า ผู้ส่งข้อมูลหรือผู้รับข้อมูลไม่ปฏิบัติตามหลักเกณฑ์หรือคำสั่งการของธนาคารแห่งประเทศไทย หรือกรณีอื่นที่ธนาคารแห่งประเทศไทยเห็นสมควรและธนาคารแห่งประเทศไทยได้แจ้งให้ผู้ให้บริการระบบทะเบียนดำเนินการ ทั้งนี้ ผู้ให้บริการระบบทะเบียนต้องกำหนดสิทธิในการดำเนินการในข้อนี้ในการตกลงให้บริการแก่ผู้ส่งข้อมูลหรือผู้รับข้อมูลด้วย

ผู้ที่จะสามารถให้บริการระบบทะเบียนในฐานะผู้ให้บริการระบบทะเบียนตามประกาศนี้จะต้องได้รับการรับรองจากคณะกรรมการขับเคลื่อนโครงการ Your Data ซึ่งแต่งตั้งโดยธนาคารแห่งประเทศไทยว่าเป็นผู้มีคุณสมบัติและมีเงื่อนไขการให้บริการข้างต้นครบถ้วน ทั้งนี้ คณะกรรมการขับเคลื่อนโครงการ Your Data อาจพิจารณายกเลิกการรับรองได้ หากปรากฏในภายหลังว่าผู้ให้บริการระบบทะเบียนซึ่งได้รับการรับรองแล้วมีคุณสมบัติหรือมีเงื่อนไขการให้บริการไม่เป็นไปตามเอกสารแนบ 4.3 นี้ โดยในระหว่างที่ยังไม่สามารถหาผู้ให้บริการที่มีคุณสมบัติและเงื่อนไขตามข้างต้นได้ ให้ผู้ส่งข้อมูลและผู้รับข้อมูลยื่นขอผ่อนผันต่อธนาคารแห่งประเทศไทยเพื่อพิจารณาตามสมควรต่อไป

**เอกสารแนบ 5**

**หลักเกณฑ์ในรายละเอียดสำหรับผู้ส่งข้อมูลผ่านช่องทางดิจิทัลในการส่งข้อมูลที่ได้มาตรฐาน**

ผู้ส่งข้อมูลผ่านช่องทางดิจิทัลในการส่งข้อมูลที่ได้มาตรฐานต้องถือปฏิบัติตามหลักเกณฑ์ในรายละเอียดเกี่ยวกับการคุ้มครองผู้บริโภคตามข้อ 4.3.4.2 (3) การจัดเก็บข้อมูลกิจกรรมการรับส่งข้อมูลของผู้ใช้บริการย้อนหลัง (audit trail) ตามข้อ 4.3.4.3 (3) และการรับส่งข้อมูลทางดิจิทัลที่ได้มาตรฐานตามข้อ 4.3.4.4 ตามประกาศฉบับนี้ ดังต่อไปนี้

**1. การให้ความรู้แก่ผู้ใช้บริการ**

ผู้ส่งข้อมูลผ่านช่องทางดิจิทัลในการส่งข้อมูลที่ได้มาตรฐานต้องมีการให้ความรู้ผู้ใช้บริการให้ทราบถึงแนวทางการจัดการข้อมูลของตนที่ได้รับมาจากช่องทางนี้ให้ปลอดภัย เพื่อป้องกันความเสี่ยงที่ข้อมูลของผู้ใช้บริการรั่วไหลหรือส่งไปยังผู้อื่นโดยไม่ตั้งใจหรือไม่ตรงตามเจตนาของตนด้วย

**2. การยืนยันตัวตนผู้ใช้บริการ**

ก่อนการให้บริการส่งข้อมูล ผู้ส่งข้อมูลต้องจัดให้มีวิธีการยืนยันตัวตนผู้ใช้บริการ (authentication) เพื่อพิสูจน์ว่าผู้ใช้บริการที่ประสงค์จะขอใช้บริการเป็นเจ้าของข้อมูลจริงตามแนวปฏิบัติที่ธนาคารแห่งประเทศไทยกำหนด

**3. การจัดเก็บข้อมูลกิจกรรมส่งข้อมูลของผู้ใช้บริการย้อนหลัง (audit trail)**

ผู้ส่งข้อมูลผ่านช่องทางดิจิทัลในการส่งข้อมูลที่ได้มาตรฐานต้องจัดเก็บ audit trail ในแต่ละกิจกรรมที่ดำเนินการ เพื่อประโยชน์ในการตรวจสอบและดำเนินการทางกฎหมายกรณีเกิดการละเมิดข้อมูลของผู้ใช้บริการหรือข้อมูลรั่วไหล โดยต้องจัดเก็บข้อมูลกิจกรรมการร้องขอข้อมูลของผู้ใช้บริการ และข้อมูลกิจกรรมการส่งข้อมูลของผู้ใช้บริการให้ผู้ใช้บริการที่เป็นเจ้าของข้อมูล ทั้งนี้ รายละเอียดและระยะเวลาในการจัดเก็บ audit trail ให้ถือปฏิบัติตามแนวปฏิบัติที่ธนาคารแห่งประเทศไทยกำหนด

**4. การรับส่งข้อมูลผ่านช่องทางดิจิทัลในการส่งข้อมูลที่ได้มาตรฐาน**

ผู้ส่งข้อมูลผ่านช่องทางดิจิทัลในการส่งข้อมูลที่ได้มาตรฐานต้องปฏิบัติตามมาตรฐานที่กำหนดในแนวปฏิบัติของธนาคารแห่งประเทศไทย ซึ่งรวมถึงมาตรฐานข้อมูล มาตรฐานการป้องกันการแก้ไขหรือปลอมแปลงข้อมูล และมาตรฐานอื่นที่จำเป็นต่อการส่งข้อมูล