

ประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
ที่ ธพส./๒๕๖๘

เรื่อง การตรวจประเมินประจำปีและจัดทำรายงานผลการตรวจประเมินธุรกิจบริการ
เกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

ตามที่ข้อกำหนดแนบท้ายประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ที่ ธพส. ๑/๒๕๖๖ ฉบับที่ ๕ หมวด ๓ การตรวจประเมินระบบการให้บริการ กำหนดให้ผู้รับใบอนุญาตต้องจัดให้มีการตรวจประเมินและจัดทำรายงานผลการตรวจประเมินระบบการให้บริการและรายงานต่อสำนักงานตามหลักเกณฑ์และระยะเวลาที่สำนักงานกำหนด

เพื่อประโยชน์ของผู้รับใบอนุญาตในการปฏิบัติตามข้อกำหนดข้างต้น อาศัยอำนาจตามความใน มาตรา ๕ และมาตรา ๒๔ แห่งพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต พ.ศ. ๒๕๖๕ ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ จึงออกประกาศกำหนดหลักเกณฑ์เกี่ยวกับการตรวจประเมินประจำปีและการจัดทำรายงานผลการตรวจประเมินระบบการให้บริการและการรายงานสำหรับผู้รับใบอนุญาตประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลไว้ ดังต่อไปนี้

ข้อ ๑ ในประกาศนี้

“ผู้รับใบอนุญาต” หมายความว่า บุคคลที่ได้รับใบอนุญาตให้ประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลตามกฎหมายว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต

“ระบบการให้บริการ” หมายความว่า ระบบและเทคโนโลยีที่ใช้สำหรับการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่มีลักษณะเป็นบริการที่ต้องได้รับใบอนุญาต และหมายรวมถึงระบบงานที่เกี่ยวข้องกับการประกอบธุรกิจบริการดังกล่าวด้วย

“หลักเกณฑ์” หมายความว่า ประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ที่ ธพส. ๑/๒๕๖๖ เรื่อง หลักเกณฑ์ในการควบคุมดูแลการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต

“พระราชกฤษฎีกา” หมายความว่า พระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต พ.ศ. ๒๕๖๕

“สำนักงาน” หมายความว่า สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ข้อ ๒ ผู้รับใบอนุญาตต้องจัดให้มีการตรวจประเมินระบบการให้บริการตามหลักเกณฑ์ในการควบคุมดูแลการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาตอย่างน้อยปีละ ๑ ครั้ง ประกอบด้วยหลักเกณฑ์ในเรื่องต่อไปนี้

- (๑) หลักเกณฑ์การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของระบบการให้บริการ
- (๒) หลักเกณฑ์การควบคุมดูแลและป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ
- (๓) หลักเกณฑ์ตามลักษณะของการให้บริการ

การกำหนดขอบเขตในการตรวจประเมินระบบให้บริการที่ได้รับใบอนุญาตตามวรรคหนึ่ง ต้องครอบคลุมการปฏิบัติงาน กระบวนการทำงาน และระบบงานด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง รวมทั้งต้องติดตามให้มีการปรับปรุงประเด็นจากการตรวจสอบ เพื่อให้มั่นใจว่ามีการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ การบริหารความเสี่ยง และการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องอย่างเพียงพอ ทั้งนี้ ผู้รับใบอนุญาตต้องดำเนินการให้สอดคล้องตามหลักเกณฑ์เกี่ยวกับมาตรฐานการให้บริการ ในส่วนที่เกี่ยวกับการตรวจประเมินระบบการให้บริการ

ข้อ ๓ การตรวจประเมินระบบการให้บริการตามข้อ ๒ ให้ผู้รับใบอนุญาตกำหนดแผนงานการตรวจประเมินให้สอดคล้องตามระดับความเสี่ยงสำหรับธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล โดยให้ผู้รับใบอนุญาตดำเนินการประเมินความเสี่ยงตามแบบประเมินความเสี่ยงประจำปีที่สำนักงานประกาศ

ผลการประเมินระดับความเสี่ยงตามวรรคหนึ่ง ต้องผ่านการพิจารณาจากผู้บริหารระดับสูง คณะกรรมการ หรือบุคลากรที่ได้รับมอบหมายของผู้ประกอบธุรกิจให้รับผิดชอบในเรื่องดังกล่าว

ข้อ ๔ ในการกำหนดแผนงานการตรวจประเมิน ให้ผู้รับใบอนุญาตพิจารณาตามระดับความเสี่ยงดังนี้

(๑) กรณีผลการประเมินอยู่ในความเสี่ยงระดับต่ำ ให้กำหนดแผนงานและดำเนินการตรวจประเมินระบบการให้บริการครอบคลุมข้อกำหนดทั้งหมดภายใต้หลักเกณฑ์ตามข้อ ๒ แบบปีเว้นปี โดยปีที่ไม่ได้มีการตรวจประเมินครอบคลุมข้อกำหนดทั้งหมด ให้มีการตรวจประเมินเฉพาะบางข้อกำหนดแต่ต้องครบตามหลักเกณฑ์ในข้อ ๒

(๒) กรณีผลการประเมินอยู่ในความเสี่ยงระดับปานกลางหรือสูง ให้กำหนดแผนงานและดำเนินการตรวจประเมินระบบการให้บริการครอบคลุมข้อกำหนดทั้งหมดภายใต้หลักเกณฑ์ตามข้อ ๒ ทุกปี

ข้อ ๕ ให้ผู้รับใบอนุญาตจัดส่งผลการประเมินความเสี่ยงประจำปี และรายงานผลการตรวจประเมินระบบการให้บริการต่อสำนักงานภายในวันที่ ๓๑ มีนาคมของปีถัดไป โดยวิธีการทางอิเล็กทรอนิกส์ตามช่องทางที่สำนักงานกำหนด โดยถือว่าสำนักงานได้รับตามวันและเวลาที่ข้อมูลได้เข้าสู่ระบบอิเล็กทรอนิกส์ของสำนักงาน ทั้งนี้ หากเป็นการนำส่งนอกวันและเวลาทำการของสำนักงาน ถือว่าสำนักงานได้รับข้อมูลดังกล่าวในวันและเวลาทำการถัดไป

ข้อ ๖ ในการตรวจประเมินระบบการให้บริการตามข้อ ๒ และการประเมินระดับความเสี่ยงตามที่กำหนดในข้อ ๓ สำหรับปี พ.ศ. ๒๕๖๘ ให้ผู้รับใบอนุญาตดำเนินการดังต่อไปนี้

(๑) ดำเนินการประเมินและจัดส่งผลการประเมินระดับความเสี่ยงต่อสำนักงาน ภายในวันที่ ๓๐ เมษายน ๒๕๖๘

(๒) กำหนดแผนงานการตรวจประเมินและดำเนินการตรวจประเมินระบบการให้บริการ ภายในปี ๒๕๖๘ และนำส่งรายงานผลการตรวจประเมินต่อสำนักงาน ภายในวันที่ ๓๑ มีนาคม ๒๕๖๙

ข้อ ๗ ประกาศฉบับนี้ให้ใช้บังคับกับผู้ประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาตซึ่งได้ประกอบธุรกิจบริการอยู่ในวันก่อนวันที่พระราชกฤษฎีกาใช้บังคับซึ่งอยู่ระหว่างการพิจารณาดำเนินการออกใบอนุญาตด้วย

ข้อ ๘ ประกาศนี้ให้ใช้บังคับตั้งแต่วันที่ เป็นต้นไป

ร่างเอกสารสำหรับฟังความคิดเห็นเพิ่มเติม (ครั้งที่ 2) ระหว่างวันที่ 26 มีนาคม - 31 พฤษภาคม ๒๕๖๘