ข้อกำหนดแนบท้ายประกาศ สพธอ. ที่ ธพส. ๑/๒๕๖๖
ฉบับที่ ๔
หลักเกณฑ์การควบคุมดูแลและป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ

ข้อ ๑ ผู้รับใบอนุญาตต้องมีการกำหนดบุคลากรที่ทำหน้าที่ในการกำกับดูแลการดำเนินงานเกี่ยวกับการควบคุมดูแลและป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบการให้บริการ รวมถึงรับผิดชอบในการจัดให้มีและดำเนินการตามแผนการป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ

ข้อ ๒ ผู้รับใบอนุญาตต้องจัดให้มีการดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

๒.๑ จัดให้มีแผนการป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ

๒.๒ กำหนดระดับความเสี่ยงที่ยอมรับได้สำหรับการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ

๒.๓ จัดให้มีการบริหารความเสี่ยงเกี่ยวกับการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ

๒.๔ จัดให้มีมาตรการที่เหมาะสมในการป้องกัน การตรวจจับ และจัดการกับการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ และดูแลให้มีการดำเนินการตามมาตรการดังกล่าว

ข้อ ๓ การจัดทำแผนการป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบต้องสอดคล้องกับลักษณะการให้บริการและความเสี่ยงของระบบการให้บริการ โดยประกอบด้วยข้อมูลอย่างน้อยดังนี้

๓.๑ เป้าหมายและวัตถุประสงค์

๓.๒ กลยุทธ์ในการบริหารจัดการความเสี่ยงจากการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ

๓.๓ ระดับความเสี่ยงที่ยอมรับได้

๓.๔ การระบุภัยคุกคาม ความเสี่ยง และช่องโหว่ที่เกี่ยวข้อง

๓.๕ ความพร้อมและความสามารถของบุคลากรที่เหมาะสมกับการบริหารจัดการความเสี่ยง

๓.๖ มาตรการในการควบคุมและจัดการภัยคุกคาม ความเสี่ยง และช่องโหว่

๓.๗ การสร้างความตระหนักให้กับบุคลากรที่เกี่ยวข้อง

๓.๘ การบริหารจัดการ การตรวจสอบ และการรายงานเหตุการณ์ที่เกี่ยวข้องกับการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ

๓.๙ การกำหนดโครงสร้าง บทบาท หน้าที่ และความรับผิดชอบของบุคลากรที่เกี่ยวข้องในการดำเนินการตามแผน

ข้อ ๔ ผู้รับใบอนุญาตต้องมีการทบทวนแผนการป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบอย่างน้อยปีละหนึ่งครั้งหรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ โดยคำนึงถึงความเหมาะสมของมาตรการที่มีอยู่ในปัจจุบันและความเสี่ยงหรือสภาพแวดล้อมการให้บริการที่เปลี่ยนแปลงไป

ข้อ ๕ ผู้รับใบอนุญาตต้องมีการบริหารจัดการบุคลากรอย่างเหมาะสม โดยต้องมีการดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

๕.๑ จัดให้มีบุคลากรที่ปฏิบัติหน้าที่เกี่ยวกับการป้องกันและควบคุมการทุจริตหรือฉ้อโกงซึ่งมีคุณสมบัติเหมาะสม โดยมีกระบวนการคัดเลือกบุคคลที่มีความรู้หรือประสบการณ์ที่เหมาะสม และมีปริมาณบุคลากรที่เพียงพอสอดคล้องกับลักษณะการประกอบธุรกิจ

๕.๒ มีการส่งเสริมและสร้างความตระหนักให้กับบุคลากรที่เกี่ยวข้อง ให้มีความเข้าใจและตระหนักถึงความเสี่ยงเกี่ยวกับการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ

๕.๓ จัดให้มีคู่มือหรือขั้นตอนการปฏิบัติงานสำหรับบุคลากรที่เกี่ยวข้อง ในการป้องกัน การตรวจจับ การรายงานและการจัดการกับเหตุการณ์การทุจริตหรือการฉ้อโกง

๕.๔ มีการอบรมให้ความรู้ที่จำเป็นแก่บุคลากรในองค์กรเกี่ยวกับการป้องกันและควบคุม การทุจริตหรือการฉ้อโกงทั้งก่อนการเริ่มปฏิบัติงานและอย่างน้อยปีละหนึ่งครั้ง

ข้อ ๖ ผู้รับใบอนุญาตต้องจัดให้มีคำแนะนำแก่ผู้ใช้บริการอย่างน้อยในเรื่องดังต่อไปนี้

๖.๑ การดูแลอัตลักษณ์และข้อมูลคุณลักษณะของตน เพื่อป้องกันการทุจริตหรือการฉ้อโกงที่อาจเกิดขึ้นจากการใช้งานระบบ

๖.๒ คำแนะนำแก่ผู้ใช้บริการเพื่อหลีกเลี่ยงการหลอกลวงทางอินเทอร์เน็ตอันทำให้ได้ไปซึ่งข้อมูลเกี่ยวกับอัตลักษณ์

ข้อ ๗ ผู้รับใบอนุญาตต้องมีกลไกในการตรวจจับและเฝ้าระวังเหตุการณ์การทุจริตหรือการฉ้อโกงจากการใช้งานระบบอย่างน้อยดังนี้

๗.๑ มีกลไกในการตรวจจับเหตุการณ์การทุจริตหรือการฉ้อโกงหรือเหตุที่น่าสงสัยว่าจะเกิดการทุจริตหรือการฉ้อโกง รวมถึงจัดให้มีช่องทางที่เป็นการรักษาความลับสำหรับบุคลากรและผู้ใช้งานในการแจ้งเหตุดังกล่าว

๗.๒ ต้องจัดให้มีกลไกในการเฝ้าระวังเหตุการณ์ที่มีลักษณะคล้ายกับเหตุการณ์ที่ตรวจพบ หรือที่เกี่ยวข้องกับเหตุการณ์ที่ตรวจพบ และนำมาตรวจสอบกับการลงทะเบียนใหม่และการปรับปรุงข้อมูลของผู้ใช้งานเดิม โดยระบบจะต้องไม่อนุญาตให้มีการลงทะเบียนใหม่หรือมีการปรับปรุงข้อมูลหากพบว่าการลงทะเบียนหรือการปรับปรุงข้อมูลมีลักษณะสุ่มเสี่ยงจะก่อให้เกิดเหตุการณ์ทุจริตหรือฉ้อโกง

ข้อ ๘ ผู้รับใบอนุญาตต้องจัดให้มีกลไกในการจัดการเหตุการณ์การทุจริตหรือการฉ้อโกง หรือเหตุการณ์ที่น่าสงสัยว่าจะเกิดการทุจริตหรือการฉ้อโกงอย่างเหมาะสมและทันท่วงที โดยมีกระบวนการอย่างน้อยดังนี้

๘.๑ มีกลไกในการตรวจสอบเหตุการณ์การทุจริตหรือการฉ้อโกง หรือเหตุที่น่าสงสัยว่าจะเกิดการทุจริตหรือการฉ้อโกง

๘.๒ ในกรณีที่เกิดเหตุการณ์การทุจริตหรือการฉ้อโกง ต้องมีการบรรเทาผลกระทบจากเหตุการณ์ดังกล่าวอย่างเหมาะสม และพิจารณาจัดการความเสี่ยงที่อาจทำให้เกิดเหตุการณ์ในลักษณะเดียวกันเพื่อไม่ให้เกิดซ้ำ

๘.๓ มีขั้นตอนการปฏิบัติงานที่กำหนดหลักเกณฑ์การตัดสินใจในช่วงที่สำคัญ (critical stage) เพื่อจัดการเหตุการณ์การทุจริตหรือการฉ้อโกง หรือเหตุที่น่าสงสัยว่าจะเกิดการทุจริตหรือการฉ้อโกง

๘.๔ มีการบันทึกการตัดสินใจเกี่ยวกับการตอบสนอง การดำเนินการ หรือกรณีที่ไม่มีการดำเนินการกับเหตุการณ์ที่น่าสงสัยว่าจะเกิดการทุจริตหรือการฉ้อโกง

๘.๕ ต้องมีการรายงานเหตุการณ์การทุจริตหรือการฉ้อโกง หรือเหตุที่น่าจะสงสัยว่าจะเกิดการทุจริตหรือการฉ้อโกง โดยนำส่งพร้อมสรุปผลการดำเนินงานเกี่ยวกับการให้บริการประจำปี ซึ่งควรประกอบด้วยข้อมูลอย่างน้อย ดังนี้

๘.๕.๑ จำนวนเหตุการณ์

๘.๕.๒ ประเภทและระดับความรุนแรงของเหตุการณ์

๘.๕.๓ การตัดสินใจเกี่ยวกับการตอบสนอง การดำเนินการ หรือกรณีที่ไม่มีการดำเนินการกับเหตุการณ์ที่น่าสงสัยว่าจะเกิดการทุจริตหรือการฉ้อโกง

๘.๕.๔ การให้ความช่วยเหลือเยียวยาแก่ผู้ที่ได้รับผลกระทบหรืออาจได้รับผลกระทบจากการทุจริตหรือการฉ้อโกง

ข้อ ๙ ในกรณีที่เกิดหรือคาดว่าจะเกิดปัญหาหรือเหตุการณ์ที่มีนัยสำคัญที่เกี่ยวกับการทุจริตหรือการฉ้อโกงในระบบให้บริการและเป็นปัญหาสำคัญที่ผู้รับใบอนุญาตต้องรายงานต่อผู้บริหารระดับสูง คณะกรรมการหรือบุคลากรที่ได้รับมอบหมาย ให้ผู้รับใบอนุญาตรายงานมายังสำนักงานเมื่อเกิดหรือรับทราบปัญหาหรือเหตุการณ์ดังกล่าวโดยเร็ว และให้แจ้งสาเหตุและการแก้ไขปัญหาเพิ่มเติมภายหลัง

ข้อ ๑๐ ผู้รับใบอนุญาตต้องจัดให้มีมาตรการ ช่องทาง และการให้ความช่วยเหลือ เยียวยาแก่ผู้ที่ได้รับผลกระทบหรืออาจได้รับผลกระทบจากการทุจริตหรือการฉ้อโกง อย่างน้อยดังนี้

๑๐.๑ มีช่องทางในการแจ้งเหตุในกรณีที่มีข้อสงสัยว่าอัตลักษณ์ หรือสิ่งที่ใช้ยืนยันตัวตน ของผู้ใช้บริการถูกนำไปใช้งานโดยไม่ชอบ

๑๐.๒ ให้ความช่วยเหลือผู้ใช้บริการในกรณีที่อัตลักษณ์ หรือสิ่งที่ใช้ยืนยันตัวตนของผู้ใช้บริการรั่วไหล หรือถูกล่วงรู้โดยบุคคลอื่น

๑๐.๓ มีมาตรการป้องกันการใช้งานอัตลักษณ์ และ/หรือสิ่งที่ใช้ยืนยันตัวตนของผู้ใช้บริการ เมื่อผู้รับใบอนุญาตมีเหตุสงสัยว่าอาจเกิดการทุจริตหรือการฉ้อโกง

๑๐.๔ ในกรณีที่ผู้รับใบอนุญาตตรวจพบหรือผู้เสียหายแจ้งต่อผู้รับใบอนุญาต ว่าบุคคลดังกล่าวเป็นเหยื่อของการทุจริตหรือการฉ้อโกง ผู้รับใบอนุญาตต้องจัดให้มีการพิสูจน์ตัวตนของบุคคลนั้นใหม่โดยอย่างน้อยต้องใช้ระดับความน่าเชื่อถือในการพิสูจน์ตัวตนที่เทียบเท่าหรือสูงกว่ากระบวนการที่เคยทำไว้

ข้อ ๑๑ ในกรณีที่เกิดเหตุการณ์ซึ่งส่งผลกระทบหรือขัดขวางความสามารถของผู้รับใบอนุญาตในการปฏิบัติตามหลักเกณฑ์ที่กำหนด ผู้รับใบอนุญาตต้องพิจารณาดำเนินการดังต่อไปนี้

๑๑.๑ แจ้งให้สำนักงานทราบถึงเหตุการณ์ซึ่งส่งผลให้ไม่สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดโดยเร็ว

๑๑.๒ บันทึกการตัดสินใจเกี่ยวกับการบริหารจัดการการทุจริตหรือฉ้อโกงจากการใช้งานระบบ และการแก้ไขหรือเยียวยา (ถ้ามี) โดยนำส่งพร้อมสรุปผลการดำเนินงานเกี่ยวกับการให้บริการประจำปี

๑๑.๓ ผู้รับใบอนุญาตอาจเปลี่ยนแปลงการบริหารจัดการการทุจริตหรือฉ้อโกงจากการใช้งานระบบได้ภายในระยะเวลาจำกัดเพื่อรับมือเหตุการณ์ที่เกิดขึ้น ทั้งนี้ การเปลี่ยนแปลงดังกล่าวต้องไม่ทำให้ระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศสูงกว่าระดับความเสี่ยงที่ยอมรับได้