(ร่าง) หลักเกณฑ์การควบคุมดูแลและป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบให้บริการ

<u>เค้าโครงร่างหลักเกณฑ์</u>

1. บุคลากรผู้รับผิดชอบ
2. การควบคุมดูแล ที่ต้องดำเนินการ
   (1) แผนการป้องกันการทุจริตหรือการฉ้อโกง
   (2) กำหนดระดับความเสี่ยงที่ยอมรับได้
   (3) การบริหารความเสี่ยง
   (4) มาตรการที่เหมาะสมในการป้องกัน การตรวจจับ (Detect) และจัดการ
3. รายละเอียดของแผนการป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ
4. การทบทวนแผน
5. การบริหารจัดการบุคลากร
6. การให้คำแนะนำแก่ผู้ใช้บริการ
7. กลไกในการติดตามและเฝ้าระวังเหตุการณ์การทุจริตหรือการฉ้อโกงจากการใช้งานระบบ
8. กลไกในการจัดการเหตุการณ์การทุจริตหรือการฉ้อโกงในระบบ
9. การรายงานเหตุการณ์สำคัญ
10. การคุ้มครองผู้ใช้บริการ
11. การแจ้งเหตุการณ์ที่ทำให้ไม่สามารถปฏิบัติตามหลักเกณฑ์ได้

(ร่าง) หลักเกณฑ์การควบคุมดูแลและป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบให้บริการ

1. ผู้รับใบอนุญาตต้องมีการกำหนดบุคลากรที่ทำหน้าที่รับผิดชอบในการกำกับดูแลการดำเนินงานตามหลักเกณฑ์การควบคุมดูแลและป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบให้บริการ รวมถึงรับผิดชอบในการจัดให้มีและดำเนินการตามแผนการป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ
2. ผู้รับใบอนุญาตต้องจัดให้มีการดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้
   (1) จัดให้มีแผนการป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ
   (2) กำหนดระดับความเสี่ยงที่ยอมรับได้สำหรับการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ
   (3) จัดให้มีการบริหารความเสี่ยงเกี่ยวกับการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ
   (4) จัดให้มีมาตรการที่เหมาะสมในการป้องกัน การตรวจจับ และจัดการกับการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ และดูแลให้มีการดำเนินการตามมาตรการดังกล่าว
3. การจัดทำแผนการป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบต้องสอดคล้องกับลักษณะการให้บริการและความเสี่ยงของระบบให้บริการ โดยประกอบด้วยข้อมูลอย่างน้อย ดังนี้
   (1) เป้าหมายและวัตถุประสงค์ในการป้องกันและจัดการ
   (2) กลยุทธ์ในการบริหารจัดการความเสี่ยงจากการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ
   (3) ระดับความเสี่ยงที่ยอมรับได้
   (4) การระบุภัยคุกคาม ความเสี่ยง และช่องโหว่ที่เกี่ยวข้อง
   (5) ความพร้อมและความสามารถของบุคลากรที่เหมาะสมกับการบริหารจัดการความเสี่ยง
   (6) มาตรการในการควบคุมและจัดการภัยคุกคาม ความเสี่ยง และช่องโหว่
   (7) การสร้างความตระหนักให้กับบุคลากรที่เกี่ยวข้อง
   (8) การบริหารจัดการ การตรวจสอบ และการรายงานเหตุการณ์ที่เกี่ยวข้องกับการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ
   (9) การกำหนดโครงสร้าง บทบาท หน้าที่ และความรับผิดชอบของบุคลากรที่เกี่ยวข้องในการดำเนินการตามแผน
4. ผู้รับใบอนุญาตต้องมีการทบทวนแผนการป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบอย่างน้อยปีละหนึ่งครั้งหรือเมื่อมีการเปลี่ยนแปลงที่มีนัยยะสำคัญ โดยคำนึงถึงความเหมาะสมของมาตรการการควบคุมดูแลและป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบในปัจจุบัน และความเสี่ยงหรือสภาพแวดล้อมการให้บริการที่เปลี่ยนแปลงไป
5. ผู้รับใบอนุญาตต้องมีการบริหารจัดการบุคลากรอย่างเหมาะสม โดยต้องมีการดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้
   5.1 จัดให้มีบุคลากรที่ปฏิบัติหน้าที่เกี่ยวข้องกับการป้องกันและควบคุมการทุจริตหรือฉ้อโกงซึ่งมีคุณสมบัติเหมาะสม โดยมีกระบวนการคัดเลือกบุคคลที่มีความรู้หรือประสบการณ์เหมาะสมในการปฏิบัติหน้าที่และมีปริมาณบุคลากรที่เพียงพอสอดคล้องกับลักษณะการดำเนินธุรกิจ
   5.2 มีการส่งเสริมและสร้างความตระหนักให้กับบุคลากรที่ปฏิบัติหน้าที่เกี่ยวข้อง ให้มีความเข้าใจและตระหนักถึงความเสี่ยงเกี่ยวกับการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ

5.3 จัดให้มีคู่มือหรือขั้นตอนการปฏิบัติงานสำหรับบุคลากรที่ปฏิบัติหน้าที่เกี่ยวข้อง ในการป้องกัน การตรวจจับ การรายงานและการจัดการกับเหตุการณ์การทุจริตหรือการฉ้อโกง

5.4 มีการอบรมให้ความรู้ที่จำเป็นแก่บุคลากรในองค์กรเกี่ยวกับการป้องกันและควบคุมการทุจริตหรือการฉ้อโกงทั้งก่อนการเริ่มปฏิบัติงานและอย่างน้อยหนึ่งครั้งต่อปี

6. ผู้รับใบอนุญาตต้องจัดให้มีคำแนะนำแก่ผู้ใช้บริการอย่างน้อยในเรื่องดังต่อไปนี้

6.1 การดูแลอัตลักษณ์และข้อมูลคุณลักษณะของตน เพื่อป้องกันการทุจริตหรือการฉ้อโกงที่อาจเกิดขึ้นจากการใช้งานระบบ

6.2 คำแนะนำแก่ผู้ใช้บริการเพื่อหลีกเลี่ยงการหลอกลวงทางอินเทอร์เน็ตอันทำให้ได้ไปซึ่งข้อมูลเกี่ยวกับอัตลักษณ์

7. ผู้รับใบอนุญาตต้องมีกลไกในการติดตามและเฝ้าระวังเหตุการณ์การทุจริตหรือการฉ้อโกงจากการใช้งานระบบอย่างน้อยดังนี้

7.1 มีกลไกในการตรวจจับเหตุการณ์การทุจริตหรือการฉ้อโกงหรือเหตุการณ์ที่น่าสงสัยว่าจะเกิดการทุจริตหรือการฉ้อโกง รวมถึงจัดให้มีช่องทางที่เป็นการรักษาความลับสำหรับบุคลากรและผู้ใช้งานในการแจ้งเหตุการณ์ดังกล่าว

7.2 ต้องจัดให้มีกลไกในการเฝ้าระวังเหตุการณ์การทุจริตหรือการฉ้อโกงที่มีลักษณะคล้ายกับเหตุการณ์ที่ตรวจพบ หรือที่เกี่ยวข้องกับเหตุการณ์ที่ตรวจพบ และนำกลไกในการเฝ้าระวังดังกล่าวมาตรวจสอบกับการลงทะเบียนใหม่และการปรับปรุงข้อมูลของผู้ใช้งานเดิม และระบบจะต้องไม่อนุญาตให้มีการลงทะเบียนใหม่หรือมีการปรับปรุงข้อมูล หากพบว่าการลงทะเบียนหรือการปรับปรุงสุ่มเสี่ยงจะก่อให้เกิดเหตุการณ์ทุจริตหรือฉ้อโกง

8. ผู้รับใบอนุญาตต้องจัดให้มีกลไกในการจัดการเหตุการณ์การทุจริตหรือการฉ้อโกง หรือเหตุการณ์ที่น่าสงสัยว่าจะเกิดการทุจริตหรือการฉ้อโกงอย่างเหมาะสมและทันท่วงที โดยมีกระบวนการอย่างน้อยดังนี้

8.1 มีกลไกในการตรวจสอบเหตุการณ์การทุจริตหรือการฉ้อโกง หรือเหตุการณ์ที่น่าสงสัยว่าจะเกิดการทุจริตหรือการฉ้อโกง

8.2 ในกรณีที่เกิดเหตุการณ์การทุจริตหรือการฉ้อโกง ต้องมีการบรรเทาผลกระทบจากเหตุการณ์ดังกล่าวอย่างเหมาะสม และพิจารณาจัดการความเสี่ยงที่อาจทำให้เกิดเหตุการณ์การทุจริตหรือการฉ้อโกงในลักษณะเดียวกันเพื่อไม่ให้เกิดซ้ำ

8.3 มีขั้นตอนการปฏิบัติงานที่กำหนดหลักเกณฑ์การตัดสินใจในช่วงที่สำคัญ (Critical stage) เพื่อจัดการเหตุการณ์การทุจริตหรือการฉ้อโกง หรือเหตุการณ์ที่น่าสงสัยว่าจะเกิดการทุจริตหรือการฉ้อโกง

8.4 มีการบันทึกการตัดสินใจเกี่ยวกับการตอบสนอง การดำเนินการ หรือกรณีที่ไม่มีการดำเนินการกับเหตุการณ์ที่น่าสงสัยว่าจะเกิดการทุจริตหรือการฉ้อโกง

8.5 ผู้รับใบอนุญาตต้องมีการรายงานเหตุการณ์การทุจริตหรือการฉ้อโกง หรือเหตุการณ์ที่น่าจะสงสัยว่าจะเกิดการทุจริตหรือการฉ้อโกง โดยนำส่งพร้อมสรุปผลการดำเนินงานเกี่ยวกับการให้บริการประจำปี ซึ่งควรประกอบด้วยข้อมูลอย่างน้อย ดังนี้

(1) จำนวนเหตุการณ์

(2) ประเภทและระดับความรุนแรงของเหตุการณ์

(3) การตัดสินใจเกี่ยวกับการตอบสนอง การดำเนินการ หรือกรณีที่ไม่มีการดำเนินการกับเหตุการณ์ที่น่าสงสัยว่าจะเกิดการทุจริตหรือการฉ้อโกง

(4) การให้ความช่วยเหลือเยียวยาแก่ที่ได้รับผลกระทบหรืออาจได้รับผลกระทบจากการทุจริตหรือการฉ้อโกง

9. ในกรณีที่เกิดหรือคาดว่าจะเกิดปัญหาหรือเหตุการณ์ที่มีนัยสำคัญที่เกี่ยวกับการทุจริตหรือการฉ้อโกงในระบบให้บริการและเป็นปัญหาสำคัญที่ผู้รับใบอนุญาตต้องรายงานต่อผู้บริหารทราบ ให้ผู้รับใบอนุญาตรายงานมายังสำนักงานทันทีเมื่อเกิดหรือรับทราบปัญหาหรือเหตุการณ์ดังกล่าว และให้แจ้งสาเหตุและการแก้ไขปัญหาเพิ่มเติมภายหลัง

10. ผู้รับใบอนุญาตต้องจัดให้มีมาตรการ ช่องทาง และการให้ความช่วยเหลือ เยียวยาแก่ผู้ที่ได้รับผลกระทบหรืออาจได้รับผลกระทบจากการทุจริตหรือการฉ้อโกง อย่างน้อยดังนี้

(1) มีช่องทางในการแจ้งเหตุในกรณีที่มีข้อสงสัยว่าอัตลักษณ์ หรือสิ่งที่ใช้ยืนยันตัวตน ของผู้ใช้บริการถูกนำไปใช้งานโดยไม่ชอบ

(2) ให้ความช่วยเหลือผู้ใช้บริการในกรณีที่อัตลักษณ์ หรือสิ่งที่ใช้ยืนยันตัวตนของผู้ใช้บริการรั่วไหล หรือถูกล่วงรู้โดยบุคคลอื่น

(3) มีมาตรการป้องกันการใช้งานอัตลักษณ์ และ/หรือสิ่งที่ใช้ยืนยันตัวตนของผู้ใช้บริการ เมื่อผู้รับใบอนุญาตมีเหตุสงสัยว่าอาจเกิดการทุจริตหรือการฉ้อโกง

(4) ในกรณีที่ผู้รับใบอนุญาตตรวจพบหรือผู้เสียหายแจ้งต่อผู้รับใบอนุญาต ว่าบุคคลดังกล่าวเป็นเหยื่อของการทุจริตหรือการฉ้อโกง ผู้รับใบอนุญาตต้องจัดให้มีการพิสูจน์ตัวตนของบุคคลนั้นใหม่ โดยอย่างน้อยต้องใช้ระดับความน่าเชื่อถือในการพิสูจน์ตัวตนที่เทียบเท่าหรือสูงกว่ากระบวนการที่เคยทำไว้

11. ในกรณีที่เกิดเหตุการณ์ซึ่งส่งผลกระทบหรือขัดขวางความสามารถของผู้รับใบอนุญาตในการปฏิบัติตามหลักเกณฑ์ที่กำหนด ผู้รับใบอนุญาตต้องพิจารณาดำเนินการดังต่อไปนี้

(1) แจ้งให้สำนักงานทราบถึงเหตุการณ์ซึ่งส่งผลให้ไม่สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดโดยเร็ว

(2) บันทึกการตัดสินใจเกี่ยวกับการบริหารจัดการการทุจริตหรือฉ้อโกงจากการใช้งานระบบ และการแก้ไขหรือเยียวยา (ถ้ามี) โดยนำส่งพร้อมสรุปผลการดำเนินงานเกี่ยวกับการให้บริการประจำปี

(3) ผู้รับใบอนุญาตอาจเปลี่ยนแปลงการบริหารจัดการการทุจริตหรือฉ้อโกงจากการใช้งานระบบได้ภายในระยะเวลาจำกัดเพื่อรับมือเหตุการณ์ที่เกิดขึ้น ทั้งนี้ การเปลี่ยนแปลงดังกล่าวต้องไม่ทำให้ระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศสูงกว่าระดับความเสี่ยงที่ยอมรับได้
