(ร่าง) ประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
เรื่อง มาตรการควบคุมและดูแลการทุจริตหรือการฉ้อโกงเกี่ยวกับกระบวนการพิสูจน์และยืนยันตัวตนทางดิจิทัล
พ.ศ. ....

.....
.....
.....
.....
.....
.....
.....
.....

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรการควบคุมและดูแลการทุจริตหรือการฉ้อโกงเกี่ยวกับกระบวนการพิสูจน์และยืนยันตัวตนทางดิจิทัล พ.ศ. ๒๕๖๔”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๓ ในประกาศนี้
“สำนักงาน” หมายความว่า สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ข้อ ๔ คณะกรรมการหรือคณะผู้บริหารของผู้ประกอบธุรกิจมีบทบาทหน้าที่และความรับผิดชอบในการกำกับดูแลนโยบายความเสี่ยงด้านการฉ้อโกงหรือทุจริตในระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล และกำหนดให้มีผู้บริหารระดับสูงอย่างน้อยหนึ่งคน (เช่น ไม่ต่ำกว่า ๓ ระดับจากผู้บริหารสูงสุด) รับผิดชอบในการบริหารความเสี่ยงด้านการฉ้อโกงหรือทุจริตในระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

ข้อ ๕ ผู้บริหารระดับสูงตามข้อ ๔ มีหน้าที่ดังต่อไปนี้

(๑) จัดให้มีการบริหารความเสี่ยงด้านการฉ้อโกงหรือทุจริตในระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

(๒) จัดให้มีนโยบายการป้องกันและจัดการการฉ้อโกงหรือทุจริตในระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล รวมทั้งเสนอต่อคณะกรรมการหรือคณะผู้บริหารของประกอบธุรกิจเพื่ออนุมัตินโยบายดังกล่าว

(๓) ดูแลให้มีการติดตาม ตรวจสอบ และรายงานต่อคณะกรรมการหรือคณะผู้บริหารของผู้ประกอบธุรกิจ ในเรื่องที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านการฉ้อโกงหรือทุจริตในระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

(๔) จัดไห้มีการรายงานการดำเนินงานเกี่ยวกับการทุจริตหรือการฉ้อโกงในระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล ต่อสำนักงาน ตามที่สำนักงานกำหนด

ข้อ ๖ นโยบายการป้องกันและจัดการการฉ้อโกงหรือทุจริตในระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล ต้องสอดคล้องกับลักษณะการดำเนินธุรกิจ ความเสี่ยงที่เกี่ยวข้อง รวมถึงปริมาณธุรกรรม และความซับซ้อนของเทคโนโลยีตามเกณฑ์ที่สำนักงานกำหนด โดยต้องประกอบด้วยข้อมูลอย่างน้อยดังนี้

(๑) แผนการดำเนินงานด้านการบริหารจัดการความเสี่ยงด้านการฉ้อโกงหรือทุจริตในระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

(๒) โครงสร้างการกำกับดูแลความเสี่ยงด้านการฉ้อโกงหรือทุจริตในระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล ที่กำหนดบทบาท หน้าที่ และความรับผิดชอบของบุคลากร พร้อมแนวทางการบริหารจัดการบุคลากรและส่งเสริมการสร้างความตระหนักเกี่ยวกับความเสี่ยงด้านการฉ้อโกงหรือทุจริต

(๓) มาตรการในการป้องกันและจัดการการฉ้อโกงหรือทุจริตในระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล ซึ่งรวมถึงการบริหารจัดการเหตุการณ์ฉ้อโกงหรือทุจริต การตรวจสอบเหตุการณ์ และการรายงานเหตุการณ์ที่เกิดขึ้น

ข้อ ๗ ผู้บริหารระดับสูงตามข้อ ๔ ต้องจัดให้มีการทบทวนนโยบายการป้องกันและจัดการการฉ้อโกงหรือทุจริตในระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล อย่างน้อยทุก ๆ ๑ ปี หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ โดยการทบทวนให้พิจารณาถึงความเพียงพอของมาตรการในการป้องกันและจัดการการฉ้อโกงหรือทุจริตที่ใช้งาน ณ ปัจจุบัน และความเสี่ยงหรือสภาพแวดล้อมการให้บริการที่เปลี่ยนแปลงไป และมีการรายงานต่อคณะกรรมการหรือคณะผู้บริหารของผู้ประกอบธุรกิจ

ข้อ ๘ การบริหารความเสี่ยงด้านการฉ้อโกงหรือทุจริตในระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล ต้องครอบคลุมการดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

(๑) การระบุความเสี่ยง ซึ่งรวมถึงภัยคุกคามและช่องโหว่ต่าง ๆ โดยความเสี่ยงอาจมีสาเหตุมาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก

(๒) การวิเคราะห์ความเสี่ยง เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม

(๓) การประเมินค่าความเสี่ยง โดยประเมินถึงโอกาสที่ความเสี่ยงจะเกิดขึ้นและผลกระทบต่อการปฏิบัติงานและการประกอบธุรกิจ รวมถึงกำหนดระดับความเสี่ยงที่ยอมรับได้

(๔) การจัดการความเสี่ยง โดยมีแนวทางและมาตรการในการจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมและสอดคล้องกับผลการประเมินความเสี่ยง เพื่อให้ความเสี่ยงอยู่ในระดับที่ยอมรับได้

(๕) การติดตามและทบทวนความเสี่ยง ด้วยกระบวนการที่มีประสิทธิภาพ

(๖) การรายงานผลการบริหารความเสี่ยง และแนวโน้มของความเสี่ยงที่อาจเกิดขึ้น ต่อคณะกรรมการหรือคณะผู้บริหารของผู้ประกอบธุรกิจตามระยะเวลาที่เหมาะสม

ข้อ ๙ ผู้บริหารระดับสูงตามข้อ ๔ ต้องส่งเสริมการป้องกันการฉ้อโกงหรือทุจริตในระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล โดยการให้ความรู้ และสร้างความตระหนักเกี่ยวกับความเสี่ยงด้านการฉ้อโกงหรือทุจริตแก่บุคลากรและผู้ใช้บริการ อย่างน้อยดังนี้

(๑) จัดให้มีบุคลากรที่ทำหน้าที่ปฏิบัติงานด้านระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล ที่มีคุณสมบัติเหมาะสม มีความรู้หรือประสบการณ์เพียงพอในการปฏิบัติหน้าที่ตามที่ได้รับมอบหมาย และมีปริมาณบุคลากรที่เพียงพอกับลักษณะการดำเนินธุรกิจ

(๒) จัดให้มีการอบรมให้ความรู้ที่จำเป็นสำหรับการป้องกันการฉ้อโกงหรือทุจริตในระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล แก่บุคลากรที่ทำหน้าที่ปฏิบัติงานด้านระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล อย่างเพียงพอทั้งก่อนการปฏิบัติงานและอย่างน้อยหนึ่งครั้งต่อปี เพื่อให้บุคลากรมีความรู้และทักษะที่เพียงพอต่อการปฏิบัติงานในส่วนที่เกี่ยวข้อง

(๓) จัดให้มีมาตรการในการสร้างและส่งเสริมความตระหนักถึงความสำคัญของความเสี่ยงด้านการฉ้อโกงหรือทุจริต เพื่อให้บุคลากรมีการตระหนักถึงบทบาทหน้าที่และความรับผิดชอบตามที่กำหนดไว้

(๔) จัดให้มีการให้คำแนะนำแก่ผู้ใช้บริการ ถึงวิธีการดูแลข้อมูลเกี่ยวกับ Digital ID และสิ่งที่ใช้ยืนยันตัวตนของผู้ใช้บริการ ซึ่งรวมถึงคำแนะนำในการป้องกันการฉ้อโกงหรือทุจริตในระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล พร้อมทั้งการสร้างความตระหนักในการระมัดระวังต่อเหตุการณ์การฉ้อโกงหรือทุจริตที่ตรวจพบ

ข้อ ๑๐ ผู้บริหารระดับสูงตามข้อ ๔ ต้องจัดให้มีกระบวนการติดตามและเฝ้าระวังเหตุการณ์การฉ้อโกงหรือทุจริตในระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล อย่างน้อยดังนี้

(๑) มีกระบวนการในการเฝ้าระวังเหตุการณ์การฉ้อโกงหรือทุจริตในระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล ที่เกิดหรือคาดว่าจะเกิดขึ้น

(๒) มีกระบวนการในการระบุหรือบ่งชี้ถึงเหตุการณ์การฉ้อโกงหรือทุจริตในระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล ที่เกิดหรือคาดว่าจะเกิดขึ้น โดยผู้ประกอบธุรกิจต้องนำข้อมูลเกี่ยวกับเหตุการณ์ที่พบนี้ไปพัฒนาหรือปรับปรุงวิธีการลงทะเบียนผู้ใช้งานใหม่ และอาจรวมถึงการปรับปรุงหรือการไม่ให้ปรับปรุงข้อมูลของผู้ใช้งานเดิมด้วย

(๓) มีกระบวนการรองรับการแจ้งเหตุหรือการรายงานเหตุการณ์การฉ้อโกงหรือทุจริตที่เกิดหรือคาดว่าจะเกิดขึ้น จากทั้งบุคลากรและผู้ใช้บริการ

ข้อ ๑๑ ผู้บริหารระดับสูงตามข้อ ๔ ต้องจัดให้มีการบริหารจัดการเหตุการณ์การฉ้อโกงหรือทุจริตที่เกิดหรือคาดว่าจะเกิดขึ้น อย่างเหมาะสมและทันท่วงที โดยมีกระบวนการอย่างน้อยดังนี้

(๑) มีกระบวนการในการตรวจสอบเหตุการณ์การฉ้อโกงหรือทุจริตที่เกิดหรือคาดว่าจะเกิดขึ้น โดยผู้ทำการตรวจสอบต้องมีคุณสมบัติเหมาะสม มีความรู้หรือประสบการณ์เพียงพอในการปฏิบัติหน้าที่ตามที่ได้รับมอบหมาย

(๒) มีการกำหนดเกณฑ์การประเมินเหตุการณ์การฉ้อโกงหรือทุจริต

(๓) มีการบันทึกการวิเคราะห์ การตัดสินใจและการดำเนินการแก้ไขเหตุการณ์การฉ้อโกงหรือทุจริตที่เกิดหรือคาดว่าจะเกิดขึ้น พร้อมวิเคราะห์สาเหตุที่แท้จริงของปัญหา เพื่อหาแนวทางแก้ไขจากสาเหตุที่แท้จริง และป้องกันไม่ให้เกิดเหตุการณ์ผิดปกติซ้ำในอนาคต

(๔) มีการรายงานเหตุการณ์การฉ้อโกงหรือทุจริตที่เกิดหรือคาดว่าจะเกิดขึ้น สาเหตุของปัญหา และวิธีดำเนินการแก้ไข ต่อคณะกรรมการหรือคณะผู้บริหารของผู้ประกอบธุรกิจโดยไม่ชักช้า

(๕) มีการรายงานสรุปเหตุการณ์การฉ้อโกงหรือทุจริตตามหลักเกณฑ์ที่สำนักงานกำหนดต่อสำนักงานทันทีเมื่อเกิดหรือทราบถึงเหตุการณ์ และให้ผู้ประกอบธุรกิจจัดเก็บรายละเอียดเกี่ยวกับเหตุการณ์ไว้อย่างน้อยดังนี้

(ก) วันและเวลาที่เกิดเหตุ

(ข) ปริมาณและความรุนแรง

(ค) เวลาตอบสนองต่อเหตุการณ์ที่เกิดขึ้น

(ง) วิธีการที่ใช้ในการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น

(จ) ประเภทของเหตุการณ์ที่เกิดขึ้น

(ฉ) ระดับการพิสูจน์ตัวตน (IAL) และระดับของการยืนยันตัวตน (AAL) ที่เกี่ยวข้อง

(ช) ข้อมูลประกอบอื่น ๆ

ทั้งนี้ สำนักงานอาจขอข้อมูลรายละเอียดเหตุการณ์ และแจ้งผลการตรวจสอบรวมถึงคำแนะนำในการป้องกันเหตุการณ์ดังกล่าวกับผู้ที่ได้รับผลกระทบ

ข้อ ๑๒ ผู้บริหารระดับสูงตามข้อ ๔ ต้องจัดให้มีการช่วยเหลือ ลดความเสียหาย และเยียวยาต่อผู้ใช้บริการที่ได้รับผลกระทบจากเหตุการณ์ฉ้อโกงหรือทุจริตที่เกิดขึ้น อย่างน้อยดังนี้

(๑) มีกระบวนการหรือช่องทางที่ผู้ใช้บริการสามารถแจ้งเหตุอันควรสงสัยว่ามีการฉ้อโกงหรือทุจริตของข้อมูลเกี่ยวกับ Digital ID หรือสิ่งที่ใช้ยืนยันตัวตน

(๒) มีบริการให้ความช่วยเหลือผู้ใช้งาน ในกรณีที่ข้อมูลเกี่ยวกับ Digital ID หรือสิ่งที่ใช้ยืนยันตัวตนของผู้ใช้บริการรั่วไหล

(๓) มีมาตรการในการป้องกันการใช้งานข้อมูลเกี่ยวกับ Digital ID หรือสิ่งที่ใช้ยืนยันตัวตนของผู้ใช้บริการที่มีเหตุอันควรสงสัยว่ามีการฉ้อโกงหรือทุจริต

(๔) ในกรณีที่ตรวจพบเหตุการณ์การฉ้อโกงหรือทุจริต ไม่ว่าโดยผู้ประกอบธุรกิจตรวจพบเองหรือได้รับแจ้งจากผู้ใช้บริการ ผู้ประกอบธุรกิจจะมีกระบวนการทบทวนและตรวจสอบการพิสูจน์ตัวตนอีกครั้งในระดับที่ไม่ต่ำกว่าระดับการพิสูจน์ตัวตน (IAL) เดิม

(๕) มีกระบวนการที่เหมาะสมในการเยียวยาความเสียหายแก่ผู้ใช้บริการ ซึ่งเกิดขึ้นจากการที่ผู้ประกอบธุรกิจฝ่าฝืนหลักเกณฑ์

ข้อ ๑๓ ในกรณีที่ผู้ประกอบธุรกิจรายใดไม่สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดตามประกาศฉบับนี้ได้ ให้ผู้ประกอบธุรกิจยื่นขออนุญาตผ่อนผันการปฏิบัติตามหลักเกณฑ์ดังกล่าวมายังสำนักงานภายใน ๓๐ วันนับแต่รู้เหตุดังกล่าว พร้อมแสดงเหตุผลและความจำเป็น รวมถึงแผนในการดำเนินการเพื่อให้สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดได้ต่อไป ทั้งนี้ สำนักงานจะพิจารณาให้แล้วเสร็จภายใน ๓๐ วันทำการนับแต่วันที่ได้รับคำขอและเอกสารถูกต้องครบถ้วน โดยสำนักงานอาจกำหนดเงื่อนไขให้ผู้ประกอบธุรกิจดำเนินการในระหว่างที่มีการผ่อนผันได้ อนึ่ง การผ่อนผันให้มีผลเมื่อสำนักงานแจ้งผลอนุญาตให้ดำเนินการได้แล้วเท่านั้น (ในระหว่างที่ผู้ประกอบธุรกิจยื่นขออนุญาตผ่อนผัน แต่ก่อนสำนักงานแจ้งผลอนุญาต ให้ถือว่าผู้ประกอบธุรกิจมีหน้าที่ต้องปฏิบัติตามหลักเกณฑ์อยู่)

ประกาศ ณ วันที่ .. .. พ.ศ. ๒๕๖๔

(.....)
ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์