

ประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

ที่ สธ. ๔๔/๒๕๖๕

เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับระบบการบริหารจัดการ

กระเป๋าสินทรัพย์ดิจิทัลและกุญแจ

อาศัยอำนาจตามความในข้อ ๓ (๑) แห่งประกาศคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ กธ. ๑๙/๒๕๖๑ เรื่อง หลักเกณฑ์ เงื่อนไข และวิธีการประกอบธุรกิจสินทรัพย์ดิจิทัล ลงวันที่ ๓ กรกฎาคม พ.ศ. ๒๕๖๑ ประกอบกับข้อ ๙ (๖) (ค) แห่งประกาศคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ กธ. ๑๙/๒๕๖๑ เรื่อง หลักเกณฑ์ เงื่อนไข และวิธีการประกอบธุรกิจสินทรัพย์ดิจิทัล ลงวันที่ ๓ กรกฎาคม พ.ศ. ๒๕๖๑ ซึ่งแก้ไขเพิ่มเติมโดยประกาศคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ กธ. ๓๔/๒๕๖๕ เรื่อง หลักเกณฑ์ เงื่อนไข และวิธีการประกอบธุรกิจสินทรัพย์ดิจิทัล (ฉบับที่ ๑๙) ลงวันที่ ๑๕ ธันวาคม พ.ศ. ๒๕๖๕ สำนักงาน ก.ล.ต. ออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้ให้ใช้บังคับตั้งแต่วันที่ ๑๖ มกราคม พ.ศ. ๒๕๖๖ เป็นต้นไป

ข้อ ๒ ในประกาศนี้

“ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล” หมายความว่า ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลที่ได้รับใบอนุญาตประกอบธุรกิจสินทรัพย์ดิจิทัล และมีการเก็บรักษาสินทรัพย์ดิจิทัลของลูกค้า

“ระบบที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัล” หมายความว่า

(๑) ระบบการบริหารจัดการกระเป๋าสินทรัพย์ดิจิทัล (wallet management)

(๒) ระบบการบริหารจัดการกุญแจ (key management)

“นโยบาย” หมายความว่า นโยบายการกำกับดูแลและบริหารจัดการระบบที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัล

“ข้อมูลต้นกำเนิด” (seed) หมายความว่า ชุดตัวเลขที่ได้จากการประมวลค่าวลีช่วยจำที่ผ่านกระบวนการทางคอมพิวเตอร์ตามที่มาตรฐานกำหนด

“วลีช่วยจำ” (mnemonic phrase) หมายความว่า ชุดคำ (word lists) ที่ได้จากการประมวลค่าเอนโทรปีที่ผ่านกระบวนการทางคอมพิวเตอร์ โดยชุดคำจะเป็นไปตามที่มาตรฐานกำหนด

“เอนโทรปี” (entropy) หมายความว่า การใช้กระบวนการทางคอมพิวเตอร์ เพื่อสร้างชุดตัวเลขที่เป็นค่าสุ่ม (randomness) ประกอบด้วย bit 0 หรือ bit 1 โดยมีความยาวเป็นไปตามที่มาตรฐานกำหนด เพื่อนำไปใช้ประกอบการสร้างกุญแจเข้ารหัส

ข้อ ๓ ข้อกำหนดในรายละเอียดตามประกาศนี้ กำหนดขึ้นเพื่อให้ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลที่มีการเก็บรักษาสินทรัพย์ดิจิทัลของลูกค้า ปฏิบัติตามประกาศคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ว่าด้วยหลักเกณฑ์ เงื่อนไข และวิธีการประกอบธุรกิจสินทรัพย์ดิจิทัลในส่วน

ที่เกี่ยวกับระบบที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัลที่มีประสิทธิภาพในเรื่องดังต่อไปนี้ให้เป็นไปในแนวทางเดียวกัน

- (๑) นโยบายและวิธีปฏิบัติในการกำกับดูแลและบริหารจัดการระบบที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัล ให้เป็นไปตามหมวด ๑
- (๒) การบริหารจัดการระบบที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัล ให้เป็นไปตามหมวด ๒
- (๓) การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อระบบที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัล (incident management) ให้เป็นไปตามหมวด ๓

หมวด ๑

นโยบายและวิธีปฏิบัติในการกำกับดูแลและบริหารจัดการระบบ ที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัล

ข้อ ๔ ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลต้องจัดให้มีนโยบายเป็นลายลักษณ์อักษรอย่างน้อยในเรื่องดังต่อไปนี้ ทั้งนี้ นโยบายดังกล่าวต้องได้รับความเห็นชอบจากคณะกรรมการของผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล หรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

(๑) การบริหารจัดการความเสี่ยงเกี่ยวกับระบบที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัลที่สอดคล้องกับนโยบายและการบริหารความเสี่ยงองค์กร (enterprise risk) ซึ่งครอบคลุมถึงการระบุความเสี่ยง การประเมินความเสี่ยง และการควบคุมความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้

(๒) การบริหารจัดการระบบที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัลตามข้อ ๖

ข้อ ๕ ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลต้องจัดให้มีการกำกับดูแลและบริหารจัดการระบบที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัลตามหลักเกณฑ์ดังต่อไปนี้ เพื่อให้เป็นไปตามนโยบายตามข้อ ๔

(๑) สื่อสารนโยบายให้แก่บุคลากรของผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลที่เกี่ยวข้องอย่างทั่วถึงในลักษณะที่สามารถเข้าถึงได้ง่าย เพื่อให้บุคลากรดังกล่าวเข้าใจและสามารถปฏิบัติตามนโยบายดังกล่าวได้ถูกต้อง

(๒) กำหนดขั้นตอนและวิธีปฏิบัติงานให้เป็นไปตามนโยบาย

(๓) ทบทวนหรือปรับปรุงนโยบาย อย่างน้อยปีละ ๑ ครั้ง และทบทวนโดยไม่ชักช้าเมื่อมีเหตุการณ์ใด ๆ ซึ่งอาจส่งผลกระทบต่อการกำกับดูแลและบริหารจัดการระบบที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัลอย่างมีนัยสำคัญ ทั้งนี้ ต้องปรับปรุงขั้นตอนและวิธีปฏิบัติงานตาม (๒) ให้สอดคล้องกับนโยบายที่มีการเปลี่ยนแปลงด้วย

(๔) จัดให้มีการกำกับดูแลการปฏิบัติตามนโยบาย โดยหน่วยงานซึ่งเป็นอิสระจากการบริหารจัดการระบบที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัล และหน่วยงานดังกล่าวมีหน้าที่รายงานผลการปฏิบัติตามนโยบายดังกล่าวให้คณะกรรมการของผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลทราบอย่างน้อยปีละ ๑ ครั้ง

และในกรณีที่มีเหตุการณ์ใด ๆ ซึ่งอาจส่งผลกระทบต่อการปฏิบัติตามนโยบายดังกล่าวอย่างมีนัยสำคัญ ต้องรายงานให้คณะกรรมการของผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลทราบโดยไม่ชักช้า

(๕) จัดให้มีระบบควบคุมภายในสำหรับการปฏิบัติงานให้เป็นไปตามนโยบายอย่างน้อย ดังนี้

(ก) มีการตรวจสอบภายในและสอบทานการปฏิบัติงานให้เป็นไปตามนโยบายดังกล่าวอย่างเป็นระบบ

(ข) มีการปรับปรุงแก้ไขข้อบกพร่อง และติดตามการปรับปรุงแก้ไขดังกล่าวอย่างเป็นระบบ และทันต่อเหตุการณ์ เพื่อลดผลกระทบต่อทรัพย์สินลูกค้า

หมวด ๒

การบริหารจัดการระบบที่เกี่ยวข้องกับ การเก็บรักษาสินทรัพย์ดิจิทัล

ข้อ ๖ ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลต้องจัดให้มีนโยบายและกำหนดกระบวนการในการบริหารจัดการระบบที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัล ในเรื่องของการออกแบบ พัฒนา และบริหารจัดการกระเป๋าสินทรัพย์ดิจิทัล อย่างเหมาะสมและมั่นคงปลอดภัย

ในกรณีที่ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลมีการสร้าง จัดเก็บ หรือเข้าถึงกุญแจ ข้อมูลต้นกำเนิด หรือข้อมูลอื่น ๆ ที่เกี่ยวข้อง ให้ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลจัดให้มีนโยบายและกำหนดกระบวนการในการบริหารจัดการระบบที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัลในเรื่องดังกล่าวด้วย

หมวด ๓

การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อระบบ ที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัล

ข้อ ๗ ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลต้องจัดให้มีการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อระบบที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัลตามหลักเกณฑ์ ดังต่อไปนี้

(๑) กำหนดขั้นตอนและกระบวนการในการบริหารจัดการเหตุการณ์

(๒) กำหนดผู้มีหน้าที่รับผิดชอบในการบริหารจัดการเหตุการณ์

(๓) ทดสอบขั้นตอนและกระบวนการในการบริหารจัดการเหตุการณ์ตาม (๑) อย่างน้อยปีละ ๑ ครั้ง

(๔) พิจารณาทบทวนขั้นตอนและกระบวนการในการบริหารจัดการเหตุการณ์หลังจากที่ได้มีการทดสอบตาม (๓) แล้วอย่างน้อยปีละ ๑ ครั้ง

(๕) จัดให้มีการประเมินผลการทดสอบตาม (๓) และประเมินผลการพิจารณาทบทวนตาม (๔) โดยต้องรายงานผลต่อคณะกรรมการของผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลอย่างน้อยปีละ ๑ ครั้ง ทั้งนี้

การดำเนินการดังกล่าวต้องกระทำโดยบุคคลที่เป็นอิสระจากผู้มีหน้าที่รับผิดชอบในการบริหารจัดการเหตุการณ์ตาม (๒)

(๖) รายงานเหตุการณ์ที่อาจส่งผลกระทบต่อระบบที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัลต่อผู้มีหน้าที่รับผิดชอบในการบริหารจัดการเหตุการณ์ตาม (๒) และสำนักงาน ก.ล.ต. โดยไม่ชักช้า

(๗) ในกรณีที่มีเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัล ซึ่งกระทบต่อทรัพย์สินของลูกค้าอย่างมีนัยสำคัญ ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลต้องดำเนินการ ดังนี้

(ก) จัดให้มีผู้เชี่ยวชาญภายนอกที่มีความเป็นอิสระ มีความชำนาญตามมาตรฐานสากล เป็นที่ยอมรับและน่าเชื่อถือ และได้รับการรับรองหรือได้รับประกาศนียบัตร (accreditations or certifications) ที่เป็นที่ยอมรับในอุตสาหกรรม ทำหน้าที่ตรวจสอบความมั่นคงปลอดภัยของระบบและพิสูจน์พยานหลักฐานทางดิจิทัล (digital forensic investigation) โดยไม่ชักช้า

(ข) จัดส่งรายงานที่จัดทำโดยผู้เชี่ยวชาญตาม (ก) ต่อสำนักงาน ก.ล.ต. ตามหลักเกณฑ์ ดังนี้

๑. รายงานการตรวจสอบขั้นต้น (interim forensic investigation report) ภายใน ๓๐ วันนับแต่วันที่ลงนามในสัญญาจ้างผู้เชี่ยวชาญภายนอก

๒. รายงานการตรวจสอบฉบับสมบูรณ์ (final forensic investigation report) ภายใน ๙๐ วันนับแต่วันที่ลงนามในสัญญาจ้างผู้เชี่ยวชาญภายนอก

ในกรณีที่มีเหตุอันสมควรทำให้ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลไม่สามารถจัดส่งรายงานดังกล่าวภายในระยะเวลาที่กำหนดตามวรรคหนึ่ง (ข) ให้ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลยื่นขอขยายระยะเวลาการจัดส่งรายงาน พร้อมทั้งเหตุผลและเอกสารหลักฐานต่อสำนักงาน ก.ล.ต. ก่อนครบกำหนดระยะดังกล่าว

(๘) จัดทำแผนการดำเนินการแก้ไขปัญหาที่พบตาม (๗) และมาตรการในการป้องกันไม่ให้เกิดปัญหาดังกล่าวซ้ำ รวมทั้งระยะเวลาในการดำเนินการตามแผนดังกล่าว โดยจัดส่งต่อสำนักงาน ก.ล.ต. ภายใน ๑๐ วันนับแต่วันที่ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลได้รับรายงานจากผู้เชี่ยวชาญตาม (๗) วรรคหนึ่ง (ข) ๒.

ให้ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลดำเนินการตามแผนดังกล่าว และจัดส่งรายงานความคืบหน้าในการดำเนินการต่อสำนักงาน ก.ล.ต. ทุกวันศุกร์จนกว่าผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลจะดำเนินการตามแผนแล้วเสร็จ

ในกรณีที่มีเหตุอันสมควรทำให้ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลไม่สามารถจัดส่งแผนการดำเนินการตามวรรคหนึ่งหรือรายงานความคืบหน้าตามวรรคสองภายในระยะเวลาที่กำหนดให้ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลยื่นขอขยายระยะเวลาการจัดส่งแผนหรือรายงาน พร้อมทั้งเหตุผลและเอกสารหลักฐานต่อสำนักงาน ก.ล.ต. ก่อนครบกำหนดระยะเวลาดังกล่าว

(๙) จัดเก็บเอกสารหลักฐานที่เกี่ยวข้องกับการดำเนินการในการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อระบบที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัลเป็นระยะเวลาไม่น้อยกว่า ๒ ปีนับแต่วันที่จัดทำเอกสารนั้น โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้สำนักงาน ก.ล.ต. สามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า

การแจ้ง การส่งแผนการดำเนินการ รายงาน เอกสารหลักฐาน หรือคำขอใด ๆ ต่อสำนักงาน ก.ล.ต. ตามวรรคหนึ่ง ให้เป็นไปตามแบบและวิธีการที่จัดไว้บนเว็บไซต์ของสำนักงาน ก.ล.ต.

ประกาศ ณ วันที่ ๑๙ ธันวาคม พ.ศ. ๒๕๖๕

รื่นวดี สุวรรณมงคล

เลขาธิการ

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์