ประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
ที่ สธ. 44/2565
เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับระบบการบริหารจัดการ
กระเป๋าสินทรัพย์ดิจิทัลและกุญแจ

อาศัยอำนาจตามความในข้อ 3(1) แห่งประกาศคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ กธ. 19/2561 เรื่อง หลักเกณฑ์ เงื่อนไข และวิธีการประกอบธุรกิจสินทรัพย์ดิจิทัล ลงวันที่ 3 กรกฎาคม พ.ศ. 2561 ประกอบกับข้อ 9(6) (ค) แห่งประกาศคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ กธ. 19/2561 เรื่อง หลักเกณฑ์ เงื่อนไข และวิธีการประกอบธุรกิจสินทรัพย์ดิจิทัล ลงวันที่ 3 กรกฎาคม พ.ศ. 2561 ซึ่งแก้ไขเพิ่มเติมโดยประกาศคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ กธ. 34/2565 เรื่อง หลักเกณฑ์ เงื่อนไข และวิธีการประกอบธุรกิจสินทรัพย์ดิจิทัล (ฉบับที่ 19) ลงวันที่ 15 ธันวาคม พ.ศ. 2565 สำนักงาน ก.ล.ต. ออกประกาศไว้ดังต่อไปนี้

ข้อ 1 ประกาศนี้ให้ใช้บังคับตั้งแต่วันที่ 16 มกราคม พ.ศ. 2566 เป็นต้นไป

ข้อ 2 ในประกาศนี้

“ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล” หมายความว่า ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลที่ได้รับใบอนุญาตประกอบธุรกิจสินทรัพย์ดิจิทัล และมีการเก็บรักษาสินทรัพย์ดิจิทัลของลูกค้า

“ระบบที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัล” หมายความว่า

(1) ระบบการบริหารจัดการกระเป๋าสินทรัพย์ดิจิทัล (wallet management)

(2) ระบบการบริหารจัดการกุญแจ (key management)

“นโยบาย” หมายความว่า นโยบายการกำกับดูแลและบริหารจัดการระบบที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัล

“ข้อมูลต้นกำเนิด” (seed) หมายความว่า ชุดตัวเลขที่ได้จากการประมวลค่าวลีช่วยจำที่ผ่านกระบวนการทางคอมพิวเตอร์ตามที่มาตรฐานกำหนด

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

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

ข้อ 3 ข้อกำหนดในรายละเอียดตามประกาศนี้ กำหนดขึ้นเพื่อให้ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลที่มีการเก็บรักษาสินทรัพย์ดิจิทัลของลูกค้า ปฏิบัติตามประกาศคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ว่าด้วยหลักเกณฑ์ เงื่อนไข และวิธีการประกอบธุรกิจสินทรัพย์ดิจิทัล ในส่วนที่เกี่ยวกับระบบที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัลที่มีประสิทธิภาพในเรื่องดังต่อไปนี้ ให้เป็นไปในแนวทางเดียวกัน

(1) นโยบายและวิธีปฏิบัติในการกำกับดูแลและบริหารจัดการระบบที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัล ให้เป็นไปตามหมวด 1

(2) การบริหารจัดการระบบที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัล ให้เป็นไปตามหมวด 2

(3) การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อระบบที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัล (incident management) ให้เป็นไปตามหมวด 3

หมวด 1
นโยบายและวิธีปฏิบัติในการกำกับดูแลและบริหารจัดการระบบที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัล

ข้อ 4 ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลต้องจัดให้มีนโยบายเป็นลายลักษณ์อักษรอย่างน้อยในเรื่องดังต่อไปนี้ ทั้งนี้ นโยบายดังกล่าวต้องได้รับความเห็นชอบจากคณะกรรมการของผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล หรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

(1) การบริหารจัดการความเสี่ยงเกี่ยวกับระบบที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัลที่สอดคล้องกับนโยบายและการบริหารความเสี่ยงองค์กร (enterprise risk) ซึ่งครอบคลุมถึงการระบุความเสี่ยง การประเมินความเสี่ยง และการควบคุมความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้

(2) การบริหารจัดการระบบที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัลตามข้อ 6

ข้อ 5 ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลต้องจัดให้มีการกำกับดูแลและบริหารจัดการระบบที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัลตามหลักเกณฑ์ดังต่อไปนี้ เพื่อให้เป็นไปตามนโยบายตามข้อ 4

(1) สื่อสารนโยบายให้แก่บุคลากรของผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลที่เกี่ยวข้องอย่างทั่วถึงในลักษณะที่สามารถเข้าถึงได้ง่าย เพื่อให้บุคลากรดังกล่าวเข้าใจและสามารถปฏิบัติตามนโยบายดังกล่าวได้ถูกต้อง

(2) กำหนดขั้นตอนและวิธีปฏิบัติงานให้เป็นไปตามนโยบาย

(3) ทบทวนหรือปรับปรุงนโยบาย อย่างน้อยปีละ 1 ครั้ง และทบทวนโดยไม่ชักช้าเมื่อมีเหตุการณ์ใด ๆ ซึ่งอาจส่งผลกระทบต่อการกำกับดูแลและบริหารจัดการระบบที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัลอย่างมีนัยสำคัญ ทั้งนี้ ต้องปรับปรุงขั้นตอนและวิธีปฏิบัติงานตาม (2) ให้สอดคล้องกับนโยบายที่มีการเปลี่ยนแปลงด้วย

(4) จัดให้มีการกำกับดูแลการปฏิบัติตามนโยบาย โดยหน่วยงานซึ่งเป็นอิสระจากการบริหารจัดการระบบที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัล และหน่วยงานดังกล่าวมีหน้าที่รายงานผลการปฏิบัติตามนโยบายดังกล่าวให้คณะกรรมการของผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลทราบอย่างน้อยปีละ 1 ครั้ง และในกรณีที่มีเหตุการณ์ใด ๆ ซึ่งอาจส่งผลกระทบต่อการปฏิบัติตามนโยบายดังกล่าวอย่างมีนัยสำคัญ ต้องรายงานให้คณะกรรมการของผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลทราบโดยไม่ชักช้า

(5) จัดให้มีระบบควบคุมภายในสำหรับการปฏิบัติงานให้เป็นไปตามนโยบายอย่างน้อยดังนี้

(ก) มีการตรวจสอบภายในและสอบทานการปฏิบัติงานให้เป็นไปตามนโยบายดังกล่าวอย่างเป็นระบบ

(ข) มีการปรับปรุงแก้ไขข้อบกพร่อง และติดตามการปรับปรุงแก้ไขดังกล่าวอย่างเป็นระบบและทันต่อเหตุการณ์ เพื่อลดผลกระทบต่อทรัพย์สินลูกค้า

หมวด 2
การบริหารจัดการระบบที่เกี่ยวข้องกับ
การเก็บรักษาสินทรัพย์ดิจิทัล

ข้อ 6 ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลต้องจัดให้มีนโยบายและกำหนดกระบวนการในการบริหารจัดการระบบที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัล ในเรื่องของการออกแบบ พัฒนา และบริหารจัดการกระเป๋าสินทรัพย์ดิจิทัล อย่างเหมาะสมและมั่นคงปลอดภัย

ในกรณีที่ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลมีการสร้าง จัดเก็บ หรือเข้าถึงกุญแจข้อมูลต้นกำเนิด หรือข้อมูลอื่น ๆ ที่เกี่ยวข้อง ให้ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลจัดให้มีนโยบายและกำหนดกระบวนการในการบริหารจัดการระบบที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัลในเรื่องดังกล่าวด้วย

หมวด 3
การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อระบบ
ที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัล

ข้อ 7 ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลต้องจัดให้มีการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อระบบที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัลตามหลักเกณฑ์ดังต่อไปนี้

(1) กำหนดขั้นตอนและกระบวนการในการบริหารจัดการเหตุการณ์

(2) กำหนดผู้มีหน้าที่รับผิดชอบในการบริหารจัดการเหตุการณ์

(3) ทดสอบขั้นตอนและกระบวนการในการบริหารจัดการเหตุการณ์ตาม (1) อย่างน้อยปีละ 1 ครั้ง

(4) พิจารณาทบทวนขั้นตอนและกระบวนการในการบริหารจัดการเหตุการณ์หลังจากที่ได้มีการทดสอบตาม (3) แล้วอย่างน้อยปีละ 1 ครั้ง

(5) จัดให้มีการประเมินผลการทดสอบตาม (3) และประเมินผลการพิจารณาทบทวนตาม (4) โดยต้องรายงานผลต่อคณะกรรมการของผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลอย่างน้อยปีละ 1 ครั้ง ทั้งนี้ การดำเนินการดังกล่าวต้องกระทำโดยบุคคลที่เป็นอิสระจากผู้มีหน้าที่รับผิดชอบในการบริหารจัดการเหตุการณ์ตาม (2)

(6) รายงานเหตุการณ์ที่อาจส่งผลกระทบต่อระบบที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัลต่อผู้มีหน้าที่รับผิดชอบในการบริหารจัดการเหตุการณ์ตาม (2) และสำนักงาน ก.ล.ต. โดยไม่ชักช้า

(7) ในกรณีที่มีเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัล ซึ่งกระทบต่อทรัพย์สินของลูกค้าอย่างมีนัยสำคัญ ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลต้องดำเนินการดังนี้

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

(ข) จัดส่งรายงานที่จัดทำโดยผู้เชี่ยวชาญตาม (ก) ต่อสำนักงาน ก.ล.ต. ตามหลักเกณฑ์ดังนี้

1. รายงานการตรวจสอบขั้นต้น (interim forensic investigation report) ภายใน 30 วันนับแต่วันที่ลงนามในสัญญาจ้างผู้เชี่ยวชาญภายนอก

2. รายงานการตรวจสอบฉบับสมบูรณ์ (final forensic investigation report) ภายใน 90 วันนับแต่วันที่ลงนามในสัญญาจ้างผู้เชี่ยวชาญภายนอก

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

(8) จัดทำแผนการดำเนินการแก้ไขปัญหาที่พบตาม (7) และมาตรการในการป้องกันไม่ให้เกิดปัญหาดังกล่าวซ้ำ รวมทั้งระยะเวลาในการดำเนินการตามแผนดังกล่าว โดยจัดส่งต่อสำนักงาน ก.ล.ต. ภายใน 10 วันนับแต่วันที่ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลได้รับรายงานจากผู้เชี่ยวชาญตาม (7) วรรคหนึ่ง (ข) 2.

ให้ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลดำเนินการตามแผนดังกล่าว และจัดส่งรายงานความคืบหน้าในการดำเนินการต่อสำนักงาน ก.ล.ต. ทุกวันศุกร์จนกว่าผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลจะดำเนินการตามแผนแล้วเสร็จ

ในกรณีที่มีเหตุอันสมควรทำให้ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลไม่สามารถจัดส่งแผนการดำเนินการตามวรรคหนึ่งหรือรายงานความคืบหน้าตามวรรคสองภายในระยะเวลาที่กำหนด ให้ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลยื่นขอขยายระยะเวลาการจัดส่งแผนหรือรายงาน พร้อมทั้งเหตุผลและเอกสารหลักฐานต่อสำนักงาน ก.ล.ต. ก่อนครบกำหนดระยะเวลาดังกล่าว

(9) จัดเก็บเอกสารหลักฐานที่เกี่ยวข้องกับการดำเนินการในการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อระบบที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัลเป็นระยะเวลาไม่น้อยกว่า 2 ปีนับแต่วันที่จัดทำเอกสารนั้น โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้สำนักงาน ก.ล.ต. สามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า

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

ประกาศ ณ วันที่ 19 ธันวาคม พ.ศ. 2565

(นางสาวรื่นวดี สุวรรณมงคล)
เลขาธิการ
สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์