สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

ประกาศแนวปฏิบัติ

ที่ นป. 8 /2565

เรื่อง แนวปฏิบัติในการบริหารจัดการกระเป๋าสินทรัพย์ดิจิทัล (wallet management) และการบริหารจัดการกุญแจ (key management)

ตามที่ประกาศคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ กธ. 19/2561 เรื่อง หลักเกณฑ์ เงื่อนไข และวิธีการประกอบธุรกิจสินทรัพย์ดิจิทัล ลงวันที่ 3 กรกฎาคม พ.ศ. 2561 ("ประกาศ ที่ กธ. 19/2561") และประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ สธ. 44 /2565 เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับระบบการบริหารจัดการกระเป๋าสินทรัพย์ดิจิทัลและกุญแจ ลงวันที่ 19 ธันวาคม พ.ศ. 2565 ("ประกาศ ที่ สธ. 44 /2565") กำหนดให้ผู้ประกอบธุรกิจต้องมีระบบการบริหารจัดการกระเป๋าสินทรัพย์ดิจิทัลที่ใช้ในการเก็บรักษาสินทรัพย์ดิจิทัล (wallet management) และกุญแจ (key management) ที่มีประสิทธิภาพ โดยต้องจัดให้มีนโยบายและวิธีปฏิบัติในการกำกับดูแลและบริหารจัดการระบบดังกล่าว และมีการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อระบบดังกล่าว นั้น

เพื่อประโยชน์ในการปฏิบัติตามข้อกำหนดข้างต้นของผู้ประกอบธุรกิจ สำนักงาน ก.ล.ต. โดยอาศัยอำนาจตามข้อ 3(2) ประกอบกับข้อ 9(6)(ค) แห่งประกาศที่ กธ. 19/2561 ซึ่งแก้ไขเพิ่มเติมโดยประกาศคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ กธ. 34 /2565 เรื่อง หลักเกณฑ์ เงื่อนไข และวิธีการประกอบธุรกิจสินทรัพย์ดิจิทัล (ฉบับที่ 19) ลงวันที่ 15 ธันวาคม พ.ศ. 2565 สำนักงาน ก.ล.ต. กำหนดแนวปฏิบัติไว้ดังต่อไปนี้

ข้อ 1 แนวปฏิบัตินี้เป็นแนวทางเกี่ยวกับเรื่องดังต่อไปนี้

(1) การจัดให้มีนโยบาย วิธีปฏิบัติ และระบบงานเกี่ยวกับการบริหารจัดการกระเป๋าสินทรัพย์ดิจิทัลที่ใช้ในการเก็บรักษาสินทรัพย์ดิจิทัล (wallet management) และกุญแจ (key management)

(2) การควบคุมดูแล ติดตาม และตรวจสอบให้มีการปฏิบัติตามนโยบาย มาตรการ และระบบงานตาม (1)

(3) การทบทวนความเหมาะสมของ (1)

ในกรณีที่ผู้ประกอบธุรกิจได้ปฏิบัติตามแนวทางตามวรรคหนึ่งจนครบถ้วน สำนักงาน ก.ล.ต. จะพิจารณาว่าผู้ประกอบธุรกิจได้ปฏิบัติตามประกาศ ที่ กธ. 19/2561 และประกาศ ที่ สธ. 44 /2565 แล้ว ทั้งนี้ หากผู้ประกอบธุรกิจดำเนินการต่างจากแนวปฏิบัตินี้ ผู้ประกอบธุรกิจมีภาระที่จะต้องพิสูจน์

ให้เห็นได้ว่าการดำเนินการนั้นยังคงอยู่ภายใต้หลักการและข้อกำหนดของประกาศ ที่ กธ. 19/2561 ในส่วนที่เกี่ยวกับระบบการบริหารจัดการกระเป๋าสินทรัพย์ดิจิทัลที่ใช้ในการเก็บรักษาสินทรัพย์ดิจิทัล (wallet management) และกุญแจ (key management) และประกาศ ที่ สธ. 44 /2565

ข้อ 2 แนวทางปฏิบัติตามข้อ 1 วรรคหนึ่งมีรายละเอียดตามที่กำหนดในภาคผนวกที่แนบท้ายประกาศแนวปฏิบัตินี้ ทั้งนี้ รายละเอียดดังกล่าวได้แก่เรื่องดังต่อไปนี้

(1) หมวดที่ 1 การกำกับดูแลและบริหารจัดการความเสี่ยงของระบบการบริหารจัดการกระเป๋าสินทรัพย์ดิจิทัล (wallet management) และการบริหารจัดการกุญแจ (key management) (governance of wallet and key management)

(2) หมวดที่ 2 การบริหารจัดการระบบการบริหารจัดการกระเป๋าสินทรัพย์ดิจิทัล (wallet management) และการบริหารจัดการกุญแจ (key management)

(3) หมวดที่ 3 การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อระบบการบริหารจัดการกระเป๋าสินทรัพย์ดิจิทัล (wallet management) และการบริหารจัดการกุญแจ (key management) (incident management)

ประกาศ ณ วันที่ 19 ธันวาคม พ.ศ. 2565

(นางสาวรื่นวดี สุวรรณมงคล)

เลขาธิการ

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

ภาคผนวก

บทนิยาม

“กระเป๋าสินทรัพย์ดิจิทัล (wallet)”	หมายถึง	ระบบที่ใช้ในการจัดเก็บสินทรัพย์ดิจิทัล
“กุญแจ (key)”	หมายถึง	กุญแจเข้ารหัส (cryptographic key) หรือสิ่งอื่นใดที่ต้องเก็บรักษาเป็นความลับ เพื่อใช้อนุมัติการโอนหรือการทำธุรกรรมเกี่ยวกับสินทรัพย์ดิจิทัลในกระเป๋าสินทรัพย์ดิจิทัล
“ข้อมูลต้นกำเนิด (seed)”	หมายถึง	ชุดตัวเลขที่ได้จากการประมวลค่าวลีช่วยจำที่ผ่านกระบวนการทางคอมพิวเตอร์ตามที่มาตรฐานกำหนด เช่น ในกรณีของ BIP32 BIP39 และ BIP44 เป็นต้น
“ผู้ประกอบธุรกิจ (business operator)”	หมายถึง	ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลที่ได้รับใบอนุญาตและมีการเก็บรักษาสินทรัพย์ดิจิทัลของลูกค้า ซึ่งรวมถึงผู้ให้บริการรับฝากสินทรัพย์ดิจิทัล
“วลีช่วยจำ (mnemonic phrase)”	หมายถึง	ชุดคำ (word lists) ที่ได้จากการประมวลค่าเอนโทรปีที่ผ่านกระบวนการทางคอมพิวเตอร์ โดยชุดคำจะเป็นไปตามที่มาตรฐานกำหนด เช่น ในกรณีของ Bitcoin ใช้ BIP32 BIP39 และ BIP44 เป็นต้น
“เอนโทรปี (entropy)”	หมายถึง	การใช้กระบวนการทางคอมพิวเตอร์เพื่อสร้างชุดตัวเลขที่เป็นคำสุ่ม (randomness) ประกอบด้วย bit 0 หรือ bit 1 โดยมีความยาวเป็นไปตามที่มาตรฐานกำหนด เพื่อนำไปใช้ประกอบการสร้างกุญแจเข้ารหัส
“ข้อมูลต้นกำเนิดสำรอง (backup seed)”	หมายถึง	การสำรองข้อมูลต้นกำเนิด
“ผู้จัดการ”	หมายถึง	บุคคลที่ได้รับมอบหมายจากคณะกรรมการบริษัทให้เป็นผู้ดูแลรับผิดชอบสูงสุดในการบริหารงานของบริษัท

“เวลาราชการ”	หมายถึง	ช่วงเวลาตั้งแต่เวลา 08.30 น. ถึง 16.30 น.
“นอกเวลาราชการ”	หมายถึง	ช่วงเวลาตั้งแต่เวลา 16.31 น. ถึง 08.29 น. ของวันถัดไป

หมวดที่ 1 : การกำกับดูแลและบริหารจัดการความเสี่ยงของระบบการบริหารจัดการกระเป๋าสินทรัพย์ดิจิทัล (wallet management) และการบริหารจัดการกุญแจ (key management) (governance of wallet and key management)

วัตถุประสงค์

เนื่องจากระบบการบริหารจัดการกระเป๋าสินทรัพย์ดิจิทัล (wallet management) และการบริหารจัดการกุญแจ (key management) ถือเป็นหนึ่งในระบบงานหลักในการเก็บรักษาสินทรัพย์ดิจิทัลของลูกค้า ซึ่งหากเกิดเหตุการณ์ที่ส่งผลต่อความมั่นคงปลอดภัย เช่น การสูญหาย ถูกทำลาย หรือเกิดการทุจริต จะส่งผลกระทบต่อการดำเนินงานของผู้ประกอบธุรกิจ สินทรัพย์ดิจิทัลของลูกค้าที่ฝากไว้ และความเชื่อมั่นต่อตลาดสินทรัพย์ดิจิทัลโดยรวมได้ ผู้บริหารระดับสูงจึงควรมีบทบาทสำคัญในการบริหารจัดการระบบการบริหารจัดการกระเป๋าสินทรัพย์ดิจิทัล (wallet management) และการบริหารจัดการกุญแจ (key management) ภายใต้การกำกับดูแลของคณะกรรมการบริษัท เพื่อให้สอดคล้องกับการกำกับดูแลกิจการที่ดี (corporate governance)

ข้อกำหนดในประกาศ ที่ สธ. 44/2565

"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”

แนวปฏิบัติ

1. นโยบายการบริหารจัดการความเสี่ยงเกี่ยวกับระบบการจัดการกระเป๋าสินทรัพย์ดิจิทัล (wallet management) และการบริหารจัดการกุญแจ (key management) ตามข้อกำหนด 4(1) ควรสอดคล้องกับนโยบายและการบริหารความเสี่ยงองค์กร (enterprise risk) และควรมีเนื้อหาขั้นต่ำดังนี้
   1.1 การระบุความเสี่ยงที่เกี่ยวข้องกับระบบการบริหารจัดการกระเป๋าสินทรัพย์ดิจิทัล (wallet management) และการบริหารจัดการกุญแจ (key management)
   1.2 การประเมินความเสี่ยง ซึ่งครอบคลุมถึงโอกาสหรือความถี่ที่จะเกิดความเสี่ยง และความมีนัยสำคัญหรือผลกระทบที่จะเกิดขึ้น เพื่อจัดลำดับความสำคัญในการบริหารจัดการความเสี่ยง
   1.3 การกำหนดเครื่องมือและมาตรการในการบริหารจัดการความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้ (risk appetite)
   1.4 การกำหนดตัวชี้วัดระดับความเสี่ยง (risk indicator) สำหรับความเสี่ยงสำคัญที่สอดคล้องกับความเสี่ยงที่ระบุตาม 1.1 รวมถึงจัดให้มีการติดตามและรายงานผลตัวชี้วัดดังกล่าว เพื่อให้สามารถบริหารจัดการความเสี่ยงด้านกุญแจได้อย่างเหมาะสมและทันต่อเหตุการณ์
   1.5 การกำหนดหน้าที่และความรับผิดชอบของผู้รับผิดชอบ (accountable person) และผู้ทำหน้าที่บริหารจัดการ (responsible person) ระบบการบริหารจัดการกระเป๋าสินทรัพย์ดิจิทัล (wallet management) และการบริหารจัดการกุญแจ (key management) ตามข้อกำหนด 4(1)
2. ในการปฏิบัติตามข้อกำหนด 5(1) ผู้ประกอบธุรกิจควรสื่อสารนโยบายให้แก่บุคลากรเฉพาะที่เกี่ยวข้องสอดคล้องกับบทบาทหน้าที่ของผู้ปฏิบัติงาน (หลัก need-to-know) โดยเฉพาะในส่วนของนโยบายที่เกี่ยวข้องกับ cold wallet ให้สื่อสารเฉพาะกับผู้ที่มีหน้าที่เท่านั้น

3. ในการปฏิบัติตามข้อกำหนด 5(4) ผู้ประกอบธุรกิจควรจัดให้มีขั้นตอนการจัดทำการติดตามและการควบคุมดูแลการจัดทำรายงานเพื่อให้มั่นใจได้ว่าสามารถจัดทำรายงานได้อย่างครบถ้วน ถูกต้องและทันเวลา โดยให้ผู้บริหารระดับสูงเป็นผู้รับผิดชอบในการปฏิบัติให้เป็นไปตามข้อกำหนด 5(4) และมีหน่วยงานที่เป็นอิสระจากผู้มีหน้าที่ปฏิบัติงานและรายงานผลการปฏิบัติตามนโยบายดังกล่าว เช่น หน่วยงานกำกับดูแลการปฏิบัติงาน และหน่วยงานตรวจสอบภายใน เป็นต้น

4. ในการปฏิบัติให้เป็นไปตามข้อกำหนด 5(5) ผู้ประกอบธุรกิจควรจัดให้มีการติดตาม ประเมินและปรับปรุงแก้ไขข้อบกพร่องของระบบควบคุมภายใน ดังต่อไปนี้

   4.1 จัดให้มีการติดตาม ตรวจสอบ และประเมินประสิทธิภาพของขั้นตอนการปฏิบัติงานของหน่วยงานที่ทำหน้าที่บริหารและจัดการในเรื่องดังต่อไปนี้ โดยผู้ตรวจสอบที่เป็นอิสระจากหน่วยงานดังกล่าว

   (ก) การปฏิบัติงานให้เป็นไปตามนโยบายในข้อกำหนด 4(1) และ (2)

   (ข) การรายงานการปฏิบัติงานในข้อกำหนด 5(4)

   4.2 จัดให้มีการประเมินตนเองในด้านประสิทธิภาพของขั้นตอนการปฏิบัติงาน (control self-assessment : CSA)

   4.3 จัดให้ผู้ตรวจสอบที่เป็นอิสระเป็นผู้ประมวลและรายงานผลที่ได้จากการดำเนินการตาม 4.1 และ 4.2 พร้อมทั้งรายงานข้อบกพร่องที่ตรวจพบและผลการปรับปรุงแก้ไขให้คณะกรรมการบริษัทหรือคณะกรรมการตรวจสอบและผู้บริหารระดับสูงทราบตามรอบการประเมินและตามรอบการติดตามการปรับปรุงแก้ไขข้อบกพร่อง หรือโดยไม่ชักช้าเมื่อพบข้อบกพร่องที่มีนัยสำคัญ

หมวดที่ 2 : การบริหารจัดการระบบการบริหารจัดการกระเป๋าสินทรัพย์ดิจิทัล (wallet management) และการบริหารจัดการกุญแจ (key management)

วัตถุประสงค์
เพื่อให้ผู้ประกอบธุรกิจมีมาตรการควบคุมดูแลความปลอดภัยขั้นสูงสุด ตั้งแต่กระบวนการสร้าง การจัดเก็บ การเข้าถึง การใช้งาน และการกู้คืนกุญแจ รวมทั้งเพื่อให้ผู้ประกอบธุรกิจมีการควบคุมการเข้าถึงสินทรัพย์ดิจิทัลในกระเป๋าสินทรัพย์ดิจิทัลของลูกค้า โดยกำหนดกระบวนการการออกแบบ การพัฒนา และบริหารจัดการระบบกระเป๋าสินทรัพย์ดิจิทัล รวมถึงการจัดเก็บ log ขั้นตอนและกิจกรรมต่าง ๆ ที่เกี่ยวข้อง เพื่อให้สามารถตรวจสอบย้อนหลังได้

ข้อกำหนดในประกาศ ที่ สธ. 44/2565

"ข้อ 6 ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลต้องจัดให้มีนโยบายและกำหนดกระบวนการในการบริหารจัดการระบบที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัล ในเรื่องของการออกแบบ พัฒนา และบริหารจัดการกระเป๋าสินทรัพย์ดิจิทัล อย่างเหมาะสมและมั่นคงปลอดภัย

ในกรณีที่ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลมีการสร้าง จัดเก็บ หรือเข้าถึงกุญแจ ข้อมูลต้นกำเนิด หรือข้อมูลอื่น ๆ ที่เกี่ยวข้อง ให้ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลจัดให้มีนโยบายและกำหนดกระบวนการในการบริหารจัดการระบบที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัลในเรื่องดังกล่าวด้วย"

แนวปฏิบัติ

1. เพื่อให้มีการดำเนินการเป็นไปตามข้อกำหนด 6 วรรคสองข้างต้น ผู้ประกอบธุรกิจควรจัดให้มีนโยบายและกระบวนการในการสร้าง และจัดเก็บ key รวมถึงการควบคุมการเข้าถึง key และข้อมูลอื่น ๆ ที่เกี่ยวข้องที่ครอบคลุมเนื้อหาขั้นต่ำดังนี้

   1.1 กรณี cryptographic key

      1.1.1 กระบวนการสร้าง cryptographic key และ seed

         (1) ผู้ประกอบธุรกิจควรทำให้มั่นใจได้ว่า key และ seed ถูกคาดเดาได้ยาก โดยครอบคลุมการดำเนินการดังนี้

            (ก) ปฏิบัติตามแนวปฏิบัติที่ดีและมาตรฐานสากลที่ได้รับการยอมรับสำหรับ entropy ที่ใช้ในการสร้าง key

            (ข) มีระบบการป้องกันในกระบวนการสร้าง key และ seed เพื่อให้มั่นใจได้ว่า key และ seed จะถูกคาดเดาได้ยาก เพื่อความปลอดภัยของทรัพย์สินลูกค้า

         (2) ผู้ประกอบธุรกิจควรจัดให้มีการแบ่งแยกหน้าที่ในกระบวนการสร้าง key และ seed โดยครอบคลุมการดำเนินการดังนี้

(ก) มีพนักงานอย่างน้อย 3 คนที่มีส่วนร่วมในกระบวนการสร้าง key และ seed ซึ่งแต่งตั้งโดยคณะกรรมการของผู้ประกอบธุรกิจ รวมถึงมีมาตรการที่เหมาะสมเพื่อให้มั่นใจได้ว่า ไม่มีพนักงานคนใดคนหนึ่งได้รับรู้ข้อมูลที่ใช้ในการสร้าง key และ seed ทั้งหมดได้

(ข) จัดให้มีบุคคลที่มีความเป็นอิสระจากหน่วยงานที่รับผิดชอบในกระบวนการสร้าง key และ seed เช่น หน่วยงานกำกับดูแลการปฏิบัติงาน และหน่วยงานตรวจสอบภายใน เป็นต้น เข้าร่วมสังเกตการณ์ในขั้นตอนการสร้าง key และ seed ว่าเป็นไปตามขั้นตอนที่กำหนดไว้ ทั้งนี้ ผู้สังเกตการณ์ต้องไม่สามารถรู้ข้อมูลที่ใช้ในการสร้าง key และ seed ทั้งหมดได้

(ค) พนักงานที่เกี่ยวข้องกับกระบวนการสร้าง key และ seed ไม่มีส่วนร่วมในระบบหรือขั้นตอนการปฏิบัติสำหรับการสร้างธุรกรรมให้ลูกค้า

(3) ผู้ประกอบธุรกิจควรจัดให้มีขั้นตอนการกู้คืน key โดยครอบคลุมการดำเนินการดังนี้

(ก) จัดให้มี mnemonic phrase หรือข้อมูลอื่นใดที่สร้างขึ้นในกระบวนการสร้าง key ซึ่งยังคงสามารถรักษาความลับในการได้มาซึ่ง key เพื่อใช้ในการกู้คืน key (regenerate) เมื่อมีเหตุจำเป็น

(ข) กำหนดขั้นตอนและการควบคุมการกู้คืน key เพื่อให้มั่นใจได้ว่า ผู้ประกอบธุรกิจจะกู้คืน key ได้ก็ต่อเมื่อได้รับอนุมัติโดยผู้มีอำนาจและเจ้าของ wallet รวมถึงมีการจัดเก็บ log หลักฐานในกระบวนการที่เกี่ยวข้อง

(4) ผู้ประกอบธุรกิจควรมีกระบวนการทดสอบการใช้งาน key seed และข้อมูลอื่น ๆ ที่เกี่ยวข้อง โดยครอบคลุมการดำเนินการดังนี้

(ก) มีกระบวนการทดสอบเพื่อให้มั่นใจได้ว่า key ที่สร้างขึ้นสามารถใช้งานเพื่อทำธุรกรรมสำหรับ wallet นั้น ๆ ได้

(ข) มีกระบวนการทดสอบเพื่อให้มั่นใจได้ว่า ข้อมูลและเครื่องมือที่ใช้ในการกู้คืน key สามารถใช้ในการกู้คืน key ได้

(5) ผู้ประกอบธุรกิจควรทำให้มั่นใจได้ว่า มีความมั่นคงปลอดภัยในการสร้าง key และ seed รวมถึงการทำลายข้อมูลที่หลงเหลือ โดยครอบคลุมการดำเนินการดังนี้

(ก) ทำให้มั่นใจได้ว่า การสร้าง key seed และข้อมูลที่เกี่ยวข้องถูกจัดทำในสภาพแวดล้อมที่มีการควบคุมที่เหมาะสมอย่างมั่นคงปลอดภัย และควรใช้อุปกรณ์ที่ปลอดภัย โดยให้การสร้าง key ทำงานแบบไม่เชื่อมต่อกับเครือข่าย แต่ถ้าเป็นการทำงานแบบมีการเชื่อมต่อกับเครือข่ายควรมีการควบคุมการเข้าถึงหรือมีการควบคุมอื่น ๆ ที่เหมาะสมทดแทน โดยให้

มีการใช้งาน ตั้งค่า ตามข้อแนะนำเพื่อความปลอดภัยที่แนะนำโดยเจ้าของผลิตภัณฑ์ หรือตามมาตรฐานสากล

(ข) มีกระบวนการและมาตรฐานการดำเนินงานที่เหมาะสม ในการทำลายข้อมูลที่สำคัญที่อาจหลงเหลืออยู่จากขั้นตอนการสร้าง key เพื่อป้องกันการเข้าถึงข้อมูลดังกล่าวโดยไม่ได้รับอนุญาต เช่น ข้อมูลบน RAM หรือ memory ของเครื่องคอมพิวเตอร์ที่ใช้ในขั้นตอนการสร้าง key เป็นต้น รวมทั้งการดำเนินการในกระบวนการดังกล่าวในแต่ละครั้ง ได้รับการสอบทานความเหมาะสมจากบุคคลที่มีความเป็นอิสระจากจากหน่วยงานที่รับผิดชอบในกระบวนการสร้าง key และ seed

(ค) จัดเก็บบันทึกเหตุการณ์ที่เกี่ยวข้องกับกระบวนการสร้าง key และ seed รวมถึงการลบหรือทำลายข้อมูลที่เกี่ยวข้อง เพื่อการสอบทานในอนาคต

1.1.2 <u>กระบวนการจัดเก็บ cryptographic key และ seed</u>

(1) ผู้ประกอบธุรกิจควรทำให้มั่นใจได้ว่า key สำหรับระบบเก็บรักษาสินทรัพย์ดิจิทัลที่เชื่อมต่อกับเครือข่ายเมื่อทำธุรกรรมเท่านั้น (cold wallet) ซึ่งไม่ได้อยู่ระหว่างการใช้งานถูกจัดเก็บอยู่ในอุปกรณ์ที่เข้ารหัสหรือตู้นิรภัย และมีการควบคุมการเข้าถึงอย่างปลอดภัย และควรมีระบบและวิธีการปฏิบัติงานที่เหมาะสม

(2) ผู้ประกอบธุรกิจควรมีการจำกัดการเข้าถึง key ข้อมูล และอุปกรณ์ที่ใช้ในการทำธุรกรรม สำหรับระบบเก็บรักษาสินทรัพย์ดิจิทัลที่เชื่อมต่อกับเครือข่ายเมื่อทำธุรกรรมเท่านั้น (cold wallet) เฉพาะกับผู้บริหารระดับสูงที่ได้รับอนุญาต โดยไม่มีผู้บริหารระดับสูงรายใดรายหนึ่งสามารถทำธุรกรรมได้โดยบุคคลเดียว

(3) ผู้ประกอบธุรกิจควรทำให้มั่นใจได้ว่า key สำหรับเก็บรักษาสินทรัพย์ดิจิทัลที่ไม่ได้เชื่อมต่อกับเครือข่ายเมื่อทำธุรกรรมเท่านั้น (hot wallet) ถูกจัดเก็บอยู่ในรูปแบบที่มีการเข้ารหัส (encryption) ที่มีความมั่นคงปลอดภัย

(4) ผู้ประกอบธุรกิจควรแบ่งข้อมูล seed หรือข้อมูลที่ใช้ในการกู้คืน key ออกเป็นอย่างน้อย 3 ส่วน โดยแบ่งผู้ที่สามารถเข้าถึงข้อมูลดังกล่าวต้องไม่ใช่บุคคลเดียวกัน และแต่ละส่วนจะต้องเก็บไว้แยกจากกันในภาชนะที่สามารถป้องกันการงัดแงะได้ รวมทั้งจัดเก็บอย่างปลอดภัย

(5) ผู้ประกอบธุรกิจควรทำให้มั่นใจได้ว่า สถานที่จัดเก็บ backup seed

(ก) ไม่ใช่สถานที่เดียวกันกับสถานที่จัดเก็บ seed และสถานที่สำหรับการจัดการธุรกรรมและการปฏิบัติงานรับฝากสินทรัพย์ดิจิทัล

(ข) แบ่งออกเป็นอย่างน้อย 3 ส่วน โดยแบ่งผู้ที่สามารถเข้าถึงข้อมูลดังกล่าวต้องไม่ใช่บุคคลเดียวกัน และแต่ละส่วนจะต้องเก็บไว้แยกจากกันในภาชนะ

ที่สามารถป้องกันการงัดแงะได้ รวมทั้งจัดเก็บอย่างปลอดภัยโดยจัดเก็บไว้ในตู้นิรภัย และมีมาตรการรักษาความปลอดภัยเทียบเท่ากับข้อมูล seed ซึ่งประกอบด้วยระบบบันทึกภาพอย่างต่อเนื่อง และมีการป้องกันการโจมตีทางกายภาพและภัยพิบัติต่าง ๆ เช่น น้ำท่วม ไฟไหม้ พายุ หรือสภาพอากาศต่าง ๆ

(6) ผู้ประกอบธุรกิจควรทำให้มั่นใจได้ว่าพื้นที่จัดเก็บ backup seed ที่อยู่นอกสถานที่ (off-site) ถูกจำกัดการเข้าถึงเฉพาะพนักงานที่ได้รับอนุญาตเท่านั้น และการยืนยันตัวตนพนักงานดังกล่าวอย่างน้อยต้องมีการใช้ multifactor identity verification ก่อนอนุญาตให้มีการเข้าถึงได้

(7) ผู้ประกอบธุรกิจควรจัดให้มีการตรวจสอบภายในสำหรับระบบและกระบวนการทำงานที่เกี่ยวข้องกับ key seed และข้อมูลอื่น ๆ ซึ่งครอบคลุมถึงการสร้างและการจัดเก็บ backup seed โดยผู้บริหารอย่างน้อยปีละ 1 ครั้ง

(8) ผู้ประกอบธุรกิจควรมีการบันทึกรายละเอียดเกี่ยวกับสิ่งที่ตรวจพบจากการตรวจสอบตาม (7) อย่างเหมาะสม รวมถึงสิ่งที่ได้ดำเนินการเพื่อแก้ไขปรับปรุง (ถ้ามี) และควรนำส่งรายละเอียดดังกล่าวให้แก่สำนักงาน ก.ล.ต. เมื่อมีการร้องขอ

(9) ผู้ประกอบธุรกิจควรจัดให้มีกระบวนการย้าย key ระหว่างอุปกรณ์ หรือติดตั้ง key ลงบน server ที่มั่นคงปลอดภัย โดยข้อมูลในอุปกรณ์ที่ใช้ในการย้าย key ควรถูกลบ ทำลายอย่างปลอดภัย

1.1.3 <u>กระบวนการเข้าถึง cryptographic key seed และข้อมูลอื่น ๆ ที่เกี่ยวข้อง</u>

(1) ผู้ประกอบธุรกิจควรมีการจำกัดการเข้าถึง key seed และข้อมูลอื่น ๆ ที่เกี่ยวข้องกับสินทรัพย์ดิจิทัลที่อยู่ภายใต้การรับฝากเฉพาะกับพนักงานที่ได้รับอนุญาต ภายใต้หลักเท่าที่จำเป็นเท่านั้น

(2) ผู้ประกอบธุรกิจควรจัดทำและทบทวนบัญชีรายชื่อพนักงานที่มีสิทธิเข้าถึง key seed และข้อมูลอื่น ๆ ที่เกี่ยวข้อง และมีวิธีการปฏิบัติที่ชัดเจนเกี่ยวกับการให้สิทธิหรือเพิกถอนสิทธิการเข้าถึงข้อมูลดังกล่าว

(3) ผู้ประกอบธุรกิจควรมีการจัดเก็บบันทึกหลักฐานทั้งการเข้าถึง key seed และข้อมูลอื่น ๆ ที่เกี่ยวข้อง (access log) และการดำเนินงาน (activity log / audit log) เพื่อการสอบทานในอนาคต เป็นระยะเวลาอย่างน้อย 2 ปี โดยอย่างน้อยควรมีข้อมูลบัญชีผู้ใช้งาน วันเวลาเข้าใช้งาน เหตุการณ์ เป็นต้น

(4) ผู้ประกอบธุรกิจควรมีการควบคุมการเปลี่ยนแปลงการตั้งค่าบนอุปกรณ์ที่ใช้สร้างและจัดเก็บ key seed และข้อมูลอื่น ๆ ให้สามารถดำเนินการได้โดยผู้มีหน้าที่รับผิดชอบ และไม่สามารถดำเนินการได้โดยบุคคลเดียว

1.2 **กรณี key ที่ไม่ใช่ cryptographic key**

สำหรับการอนุมัติการโอนหรือการทำธุรกรรมเกี่ยวกับสินทรัพย์ดิจิทัลโดยใช้ key รูปแบบอื่นใดนอกจาก cryptographic key ผู้ประกอบธุรกิจควรจัดให้มีนโยบายและกระบวนการบริหารจัดการ key และข้อมูลอื่น ๆ ที่เกี่ยวข้อง ที่สามารถตรวจสอบและควบคุมได้ มีการแบ่งแยกบุคลากรที่รับผิดชอบเกี่ยวกับการบริหารจัดการ key และมีความปลอดภัยจากการที่ key ถูกโจรกรรม เสียหาย หรือสูญหาย รวมทั้งสามารถกู้คืน key ได้เมื่อได้รับอนุมัติโดยผู้มีอำนาจและเจ้าของ wallet โดยมีการจัดเก็บ log หลักฐานในกระบวนการที่เกี่ยวข้อง

2. เพื่อให้มีการดำเนินการเป็นไปตามข้อกำหนด 6 วรรคหนึ่งข้างต้น ผู้ประกอบธุรกิจควรจัดให้มีนโยบายและกระบวนการสำหรับการออกแบบ การพัฒนา และการบริหารจัดการ wallet โดยครอบคลุมเนื้อหาขั้นต่ำดังต่อไปนี้

2.1 ผู้ประกอบธุรกิจควรจัดให้มีการออกแบบ wallet เพื่อให้สามารถตั้งค่าและกำหนดสิทธิหรือวงเงินในการทำธุรกรรมได้อย่างเหมาะสม และสามารถป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้าถึงได้

2.2 ผู้ประกอบธุรกิจควรจัดให้มีการออกแบบ wallet อย่างเหมาะสม โดยมีการคำนึงถึงการควบคุมที่สำคัญตั้งแต่กระบวนการการพัฒนาและเปลี่ยนแปลงแก้ไข

2.3 ผู้ประกอบธุรกิจควรจัดให้มีกระบวนการจัดหา และคัดเลือกผู้ให้บริการ wallet ก่อนเปิดใช้งานเพื่อให้มั่นใจว่า wallet ที่เลือกใช้มีความเหมาะสมและมีการรักษาความปลอดภัยที่ดี

2.4 ผู้ประกอบธุรกิจควรมีการสอบทานการตั้งค่าและการเปลี่ยนแปลงบน wallet รวมถึงสอบทานการทำธุรกรรมที่มีมูลค่าสูง

2.5 ผู้ประกอบธุรกิจควรมีการจัดเก็บบันทึกหลักฐานการตั้งค่า กำหนดสิทธิ การเข้า wallet (access log) และการดำเนินงาน (activity log / audit log) เพื่อการสอบทานในอนาคต เป็นระยะเวลาอย่างน้อย 2 ปี โดยอย่างน้อยควรมีข้อมูลบัญชีผู้ใช้งาน วันเวลาเข้าใช้งาน เหตุการณ์ เป็นต้น

หมวดที่ 3 : การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อระบบการบริหารจัดการกระเป๋าสินทรัพย์ดิจิทัล (wallet management) และการบริหารจัดการกุญแจ (key management) (incident management)

วัตถุประสงค์
เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบการบริหารจัดการกระเป๋าสินทรัพย์ดิจิทัล (wallet management) และการบริหารจัดการกุญแจ (key management) ได้รับการดำเนินการอย่างถูกต้อง และมีประสิทธิภาพในช่วงระยะเวลาที่เหมาะสม

ข้อกำหนดในประกาศ ที่ สธ. 44/2565

"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.”

แนวปฏิบัติ

1. เพื่อให้มีการดำเนินการเป็นไปตามที่ข้อกำหนด 7(1) และ (2) ผู้ประกอบธุรกิจควรกำหนดขั้นตอนและกระบวนการขั้นต่ำดังต่อไปนี้
   1.1 กำหนดแผนรองรับในกรณีที่เกิดเหตุการณ์อย่างเป็นลายลักษณ์อักษร โดยอย่างน้อยต้องครอบคลุมกรณี (1) cyber attack (2) กุญแจหลักไม่สามารถใช้งานได้ และ (3) การทุจริตโดยบุคคลในองค์กร
   1.2 ประเมินเหตุการณ์หรือจุดอ่อนของระบบการบริหารจัดการกระเป๋าสินทรัพย์ดิจิทัล (wallet management) และการบริหารจัดการกุญแจ (key management) และพิจารณาว่าควรจัดเป็นเหตุการณ์และมีระดับความรุนแรงที่อาจส่งผลกระทบต่อระบบการบริหารจัดการกระเป๋าสินทรัพย์ดิจิทัล (wallet management) และการบริหารจัดการกุญแจ (key management)

1.3 จัดให้มีบุคคลหรือหน่วยงานเพื่อทำหน้าที่รับแจ้งเหตุการณ์ (point of contact) และรายงานเหตุการณ์ต่อคณะผู้บริหารหรือผู้เกี่ยวข้องให้ทราบและดำเนินการต่อไป (escalation)

1.4 ดำเนินการเพื่อตอบสนองต่อเหตุการณ์ที่เกิดขึ้นอย่างมีประสิทธิภาพ เพื่อทำให้เหตุการณ์คลี่คลายหรือกลับสู่ภาวะปกติอย่างรวดเร็ว โดยควรจัดให้มีทีมผู้เชี่ยวชาญ (incident response team) เพื่อตอบสนองต่อเหตุการณ์ที่เกิดขึ้นอย่างมีประสิทธิภาพ

1.5 รวบรวมและจัดเก็บหลักฐานโดยไม่ชักช้า เมื่อเกิดเหตุการณ์ที่ส่งผลกระทบต่อระบบการบริหารจัดการกระเป๋าสินทรัพย์ดิจิทัล (wallet management) และการบริหารจัดการกุญแจ (key management) ที่มีความสำคัญอย่างมีนัยสำคัญ เช่น ก่อให้เกิดความเสียหายกับข้อมูลหรือทรัพย์สินของลูกค้า โดยคำนึงถึงประเด็นสำคัญต่าง ๆ เช่น มีกระบวนการการจัดเก็บอย่างมั่นคงปลอดภัย การกำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้อง การคัดเลือกบุคคลที่มีความรู้ความสามารถหรือมีประสบการณ์ด้านการรวบรวมและจัดเก็บหลักฐาน เพื่อวิเคราะห์ตรวจสอบและจัดทำเอกสารสรุปนำเสนอต่อบุคคลที่มีหน้าที่รับผิดชอบ เป็นต้น ทั้งนี้ การรวบรวม จัดเก็บและนำเสนอหลักฐานควรสอดคล้องกับหลักเกณฑ์ของกฎหมายที่ใช้บังคับ

1.6 บันทึกและจัดเก็บหลักฐานการบริหารจัดการตามความจำเป็นและความเหมาะสม

1.7 ตรวจหา ติดตาม วิเคราะห์ และรายงานเหตุการณ์ ทั้งนี้ ให้รวมถึงการวิเคราะห์ภายหลังเหตุการณ์ยุติแล้ว เพื่อระบุถึงสาเหตุของเหตุการณ์และเพื่อใช้ประโยชน์จากผลการวิเคราะห์ในการเตรียมความพร้อมรองรับเหตุการณ์ที่อาจเกิดขึ้นได้อีกในอนาคต รวมทั้งรายงานความคืบหน้าให้สำนักงาน ก.ล.ต. ทราบทุกวันถัดไป

1.8 มีหนังสือรายงานสำนักงาน ก.ล.ต. ถึงสถานการณ์และผลการบริหารจัดการทราบภายใน 2 วัน นับแต่วันที่เหตุการณ์ยุติแล้ว

2. เจ้าหน้าที่ปฏิบัติงานที่พบเหตุการณ์ที่ส่งกระทบต่อระบบการบริหารจัดการกระเป๋าสินทรัพย์ดิจิทัล (wallet management) และการบริหารจัดการกุญแจ (key management) ควรต้องรายงานให้ผู้มีหน้าที่รับผิดชอบในการบริหารจัดการเหตุการณ์ที่กำหนดไว้ตามข้อกำหนด 7(2) เพื่อที่จะรายงานให้สำนักงาน ก.ล.ต. ทราบโดยไม่ชักช้าเมื่อเกิดเหตุการณ์ดังกล่าว ทั้งนี้ ผู้มีหน้าที่รับผิดชอบในการบริหารจัดการเหตุการณ์ดังกล่าวควรดำเนินการตามหลักเกณฑ์ดังต่อไปนี้

2.1 จัดทำแบบฟอร์มที่เป็นมาตรฐานเพื่อรองรับการรายงานสถานการณ์ และสร้างความเข้าใจให้กับผู้รายงานเกี่ยวกับการดำเนินการต่าง ๆ ที่จำเป็นกรณีที่เกิดเหตุการณ์ ทั้งนี้ เนื้อหาขั้นต่ำควรประกอบด้วย วันเวลา เหตุการณ์ ผลกระทบที่คาดว่าจะเกิดขึ้น การดำเนินการแก้ไข ผลการแก้ไข ระยะเวลาในการแก้ไข สาเหตุที่เกิดปัญหา และแนวทางการป้องกันในอนาคต

2.2 รายงานคณะผู้บริหารขององค์กรเมื่อทราบเหตุการณ์ที่อาจส่งผลกระทบต่อระบบการบริหารจัดการกระเป๋าสินทรัพย์ดิจิทัล (wallet management) และการบริหารจัดการกุญแจ (key management) เช่น พบช่องโหว่ในการควบคุมความมั่นคงปลอดภัย (ineffective

security control) เกิดเหตุการณ์ที่อาจส่งผลกระทบต่อการรักษาความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) ข้อผิดพลาดจากการปฏิบัติงาน (human errors) การบุกรุกด้านกายภาพ (breaches of physical security arrangements) การปฏิบัติงานที่ไม่เป็นไปตามนโยบาย การทำงานผิดพลาดของโปรแกรมและอุปกรณ์คอมพิวเตอร์ (malfunctions of software or hardware) และการเข้าถึงโดยไม่ได้รับอนุญาต (access violations)

2.3 รายงานสำนักงาน ก.ล.ต. เมื่อมีเหตุการณ์ที่ส่งผลกระทบต่อระบบการบริหารจัดการกระเป๋าสินทรัพย์ดิจิทัล (wallet management) และการบริหารจัดการกุญแจ (key management) ที่มีความสำคัญ

2.4 แจ้งบุคคลที่เกี่ยวข้อง เช่น ลูกค้า รับทราบโดยไม่ชักช้า ในกรณีที่เหตุการณ์ส่งผลกระทบต่อบุคคลดังกล่าว

2.5 จัดให้มีการรายงานความคืบหน้าในการบริหารจัดการสถานการณ์และผลการบริหารจัดการเป็นระยะ และเมื่อเหตุการณ์ยุติแล้ว

3. ในการปฏิบัติให้เป็นไปตามข้อกำหนด 7(3) (4) และ (9) ผู้ประกอบธุรกิจควรดำเนินการดังต่อไปนี้

3.1 จัดให้มีการจำลองสถานการณ์เสี่ยง (risk scenario) เพื่อทดสอบการเตรียมความพร้อมรับมือต่อเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบการบริหารจัดการกระเป๋าสินทรัพย์ดิจิทัล (wallet management) และการบริหารจัดการกุญแจ (key management) โดย risk scenario ดังกล่าวควรมีลักษณะดังต่อไปนี้

(1) เป็นสถานการณ์ที่สอดคล้องกับลักษณะ ขอบเขต และความซับซ้อนในการประกอบธุรกิจของผู้ประกอบธุรกิจ

(2) เป็นสถานการณ์ที่เมื่อเกิดขึ้นแล้ว จะส่งผลกระทบต่อระบบการบริหารจัดการกระเป๋าสินทรัพย์ดิจิทัล (wallet management) และการบริหารจัดการกุญแจ (key management) อย่างมีนัยสำคัญ

(3) เป็นสถานการณ์ที่สามารถวัดผลได้ และนำผลที่ได้ไปใช้ในการทบทวนขั้นตอนและกระบวนการในการบริหารจัดการเหตุการณ์ เพื่อให้เกิดความมั่นคงปลอดภัยของระบบการบริหารจัดการกระเป๋าสินทรัพย์ดิจิทัล (wallet management) และการบริหารจัดการกุญแจ (key management)

(4) เป็นสถานการณ์ที่มีความสมเหตุสมผล สามารถปฏิบัติได้จริงโดยไม่ขัดแย้งกัน

(5) เป็นสถานการณ์ที่มีความเป็นไปได้ และสอดคล้องกับสถานการณ์จริงในปัจจุบัน

3.2 จัดเก็บเอกสารที่เกี่ยวข้องกับการทดสอบให้ครบถ้วนและเป็นปัจจุบันดังนี้

(1) สถานการณ์เสี่ยง (risk scenario) ที่ใช้ในการทดสอบ

(2) สรุปผลการทดสอบ ผลการประเมิน และผลการทบทวนแผนรองรับในกรณีที่เกิดเหตุการณ์

4. ในการปฏิบัติให้เป็นไปตามข้อกำหนด 7(6) ผู้ประกอบธุรกิจควรดำเนินการรายงานสำนักงาน ก.ล.ต. เมื่อมีเหตุการณ์ที่ส่งผลกระทบต่อระบบที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัล โดยควรรายงานดังนี้

4.1 หากทราบเหตุการณ์ดังกล่าวในเวลาราชการ

(1) รายงานโดยไม่ชักช้าภายในวันที่ทราบเหตุการณ์นั้น แต่ไม่เกิน 18.00 น. เว้นแต่เป็นเหตุที่กระทบต่อทรัพย์สินของลูกค้า ให้รายงานภายใน 1 ชั่วโมงนับแต่ผู้จัดการหรือบุคคลที่ได้รับมอบหมายให้มีอำนาจทั้งหมดหรือบางส่วนในการจัดการทราบถึงเหตุการณ์ดังกล่าว แต่ไม่เกิน 18.00 น. โดยมีเนื้อหาครอบคลุมถึงวันเวลา เหตุการณ์ และผลกระทบที่คาดว่าจะเกิดขึ้น ทั้งนี้ อาจแจ้งโดยวาจาหรือผ่านระบบรับส่งข้อความผ่านทางอิเล็กทรอนิกส์ (electronic messaging) ตามความเหมาะสม

(2) รายงานความคืบหน้าเป็นลายลักษณ์อักษรอย่างน้อยทุกวัน ภายในเวลา 16.00 น. ตั้งแต่วันถัดไปหลังทราบเหตุการณ์ หรือตามที่สำนักงาน ก.ล.ต. ร้องขอ จนกว่าระบบที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัลจะกลับสู่การให้บริการได้อย่างเป็นปกติ โดยมีเนื้อหาครอบคลุมถึงวันเวลา เหตุการณ์ ผลกระทบที่เกิดขึ้น การดำเนินการแก้ไขปัญหาและความคืบหน้าในการแก้ไขปัญหา ทั้งนี้ ให้รายงานผ่านช่องทางอิเล็กทรอนิกส์ที่สำนักงาน ก.ล.ต. กำหนด

(3) รายงานเมื่อเหตุการณ์ยุติหรือแก้ไขปัญหาแล้วเสร็จ เป็นลายลักษณ์อักษร โดยมีเนื้อหาครอบคลุมถึงวันเวลา เหตุการณ์ ผลกระทบที่เกิดขึ้น การดำเนินการแก้ไขปัญหา ผลการแก้ไขปัญหา ระยะเวลาในการแก้ไข สาเหตุที่เกิดปัญหา และแนวทางป้องกันในอนาคต

4.2 หากทราบเหตุการณ์ดังกล่าวนอกเวลาราชการ

(1) รายงานโดยไม่ชักช้าเมื่อทราบเหตุการณ์นั้น โดยมีเนื้อหาครอบคลุมถึงวันเวลา เหตุการณ์ และผลกระทบที่คาดว่าจะเกิดขึ้น โดยอาจแจ้งโดยวาจาหรือผ่านระบบรับส่งข้อความผ่านทางอิเล็กทรอนิกส์ (electronic messaging) ตามความเหมาะสม

(2) รายงานความคืบหน้าเป็นลายลักษณ์อักษรอย่างน้อยทุกวัน ภายในเวลา 16.00 น. ตั้งแต่วันถัดไปหลังทราบเหตุการณ์หรือตามที่สำนักงาน ก.ล.ต. ร้องขอ จนกว่าระบบที่เกี่ยวข้องกับการเก็บรักษาสินทรัพย์ดิจิทัลจะกลับสู่การให้บริการได้อย่างเป็นปกติ โดยมีเนื้อหาครอบคลุมถึงวันเวลา เหตุการณ์ ผลกระทบที่เกิดขึ้น การดำเนินการแก้ไขปัญหาและความคืบหน้าในการแก้ไขปัญหา ทั้งนี้ ให้รายงานผ่านช่องทางอิเล็กทรอนิกส์ที่สำนักงาน ก.ล.ต. กำหนด

(3) รายงานเมื่อเหตุการณ์ยุติหรือแก้ไขปัญหาแล้วเสร็จ เป็นลายลักษณ์อักษร โดยมีเนื้อหาครอบคลุมถึงวันเวลา เหตุการณ์ ผลกระทบที่เกิดขึ้น การดำเนินการแก้ไขปัญหา ผลการแก้ไขปัญหา ระยะเวลาในการแก้ไข สาเหตุที่เกิดปัญหา และแนวทางป้องกันในอนาคต

5. ในการปฏิบัติให้เป็นไปตามข้อกำหนด 7(7) ผู้ประกอบธุรกิจควรดำเนินการดังนี้

5.1 กำหนดลักษณะเหตุการณ์ที่กระทบต่อทรัพย์สินของลูกค้าอย่างมีนัยสำคัญ โดยอาจพิจารณาจากมูลค่าสินทรัพย์ดิจิทัลที่สูญหายเกินกว่า 100 ล้านบาท หรือจำนวนผู้ใช้บริการที่ได้รับผลกระทบจากการสูญหายของสินทรัพย์ดิจิทัลเกินกว่า 1 พันคน

5.2 จัดจ้างผู้เชี่ยวชาญภายนอกเพื่อดำเนินการตรวจสอบ digital forensic investigation ภายใน 30 วันนับแต่วันที่พบเหตุการณ์ เว้นแต่เป็นเหตุสุดวิสัย ให้แจ้งให้สำนักงาน ก.ล.ต. ทราบเป็นลายลักษณ์อักษร พร้อมแผนดำเนินการดังกล่าว