

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

The Securities and Exchange Commission, Thailand

มาตรฐานสำหรับการออกและให้บริการหลักทรัพย์โทเคน

Standards for Securities Tokenization

Draft Version

ข้อสงวนสิทธิ (Disclaimer)

มาตรฐานการออกและให้บริการหลักทรัพย์โทเคนฉบับนี้จัดทำขึ้นเพื่อเป็นกรอบแนวทางสำหรับผู้เกี่ยวข้องในการออกแบบและดำเนินการเกี่ยวกับหลักทรัพย์โทเคน โดยครอบคลุมหลักการและแนวปฏิบัติที่เกี่ยวข้องกับการออกและให้บริการหลักทรัพย์โทเคน ตลอดจนการนำเทคโนโลยีมาใช้โดยคำนึงถึงสิทธิ หน้าที่ และผลทางกฎหมายที่เกี่ยวข้อง

สถานะและวัตถุประสงค์ของเอกสาร

เอกสารฉบับนี้จัดทำขึ้นเพื่อใช้เป็นมาตรฐานอ้างอิงและแนวทางประกอบการพิจารณาสำหรับผู้ที่เกี่ยวข้องกับการออกและให้บริการหลักทรัพย์โทเคน ทั้งนี้ การนำมาตรฐานไปใช้ควรพิจารณาตามลักษณะของกิจกรรม โครงสร้างการดำเนินงาน เทคโนโลยีที่เกี่ยวข้อง และบริบทของผู้ใช้งานแต่ละราย ภายใต้กฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง

ความสัมพันธ์กับกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง

เอกสารฉบับนี้ไม่เป็นการทดแทนกฎหมาย กฎเกณฑ์ ประกาศ ข้อกำหนด หรือคำสั่งของหน่วยงานที่มีอำนาจตามกฎหมาย ผู้เกี่ยวข้องยังคงมีหน้าที่ต้องปฏิบัติตามกฎหมายและหลักเกณฑ์ที่ใช้บังคับกับกิจกรรมของตน การนำมาตรฐานไปใช้ไม่ทำให้ผู้เกี่ยวข้องพ้นจากหน้าที่หรือความรับผิดตามกฎหมายที่เกี่ยวข้อง ทั้งนี้ ต้องพิจารณาควบคู่กับข้อกำหนดตามสัญญาและเอกสารที่มีผลผูกพันตามกฎหมายในแต่ละกรณี

การนำมาตรฐานไปใช้และการตีความ

ผู้นำมาตรฐานไปใช้ควรพิจารณาความเหมาะสมของหลักการและแนวปฏิบัติในเอกสารฉบับนี้ให้สอดคล้องกับลักษณะการดำเนินงานและบริบทของตน รวมถึงประเมินความเสี่ยงและผลกระทบทางกฎหมายและการดำเนินงานที่เกี่ยวข้อง ทั้งนี้ การกล่าวถึงเทคโนโลยี รูปแบบการดำเนินงาน ผลิตภัณฑ์ หรือผู้ให้บริการใดในเอกสารฉบับนี้ ไม่ถือเป็นการรับรองหรือแนะนำให้เลือกใช้สิ่งดังกล่าวเป็นการเฉพาะ

การควบคุมเอกสาร (Document Control)

ส่วนนี้ระบุข้อมูลสำคัญสำหรับการควบคุมและอ้างอิงเอกสารมาตรฐานฉบับนี้ รวมถึงรายละเอียดเกี่ยวกับหน่วยงานที่เกี่ยวข้อง สถานะของเอกสาร และประวัติการเผยแพร่และปรับปรุงเอกสาร

ข้อมูลเกี่ยวกับเอกสาร

รายการ	รายละเอียด
ชื่อเอกสาร	มาตรฐานสำหรับการออกและให้บริการหลักทรัพย์โทเคน Standards for Securities Tokenization
เวอร์ชันเอกสาร	0.5
วันที่เผยแพร่	XX พฤศจิกายน 2569
สถานะเอกสาร	ร่างเพื่อรับฟังความเห็น
หน่วยงานที่ออกเอกสาร	สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

ประวัติการปรับปรุง

เวอร์ชัน	เดือนและปีที่เผยแพร่	สาระสำคัญ
0.5	XX พฤศจิกายน 2569	ร่างรับฟังความคิดเห็น

คำนำ (Foreword)

การพัฒนาตลาดทุนไทยให้ก้าวทันความเปลี่ยนแปลงทางเทคโนโลยีเป็นหนึ่งในแนวทางสำคัญในการเพิ่มประสิทธิภาพและพัฒนารูปแบบการให้บริการในตลาดทุน โดยเฉพาะการออกและให้บริการหลักทรัพย์ในรูปแบบใหม่ เช่น หลักทรัพย์โทเคน (Securities Token) ซึ่งมีศักยภาพในการเพิ่มประสิทธิภาพของกระบวนการดำเนินงาน และส่งเสริมการเชื่อมโยงระหว่างผู้เกี่ยวข้องในระบบนิเวศหลักทรัพย์อิเล็กทรอนิกส์ (Digital Securities Ecosystem: DSE) เพื่อสนับสนุนการพัฒนาตลาดทุนดิจิทัลของไทย

อย่างไรก็ตาม การนำหลักทรัพย์โทเคนมาใช้จำเป็นต้องมีกรอบการดำเนินงานและมาตรฐานที่เหมาะสม เพื่อให้สามารถรองรับสิทธิและหน้าที่ของผู้เกี่ยวข้องได้อย่างชัดเจน ตลอดจนส่งเสริมความมั่นคงปลอดภัย ความน่าเชื่อถือ และการทำงานร่วมกันของระบบที่เกี่ยวข้อง อันเป็นปัจจัยสำคัญต่อการพัฒนาระบบนิเวศหลักทรัพย์อิเล็กทรอนิกส์อย่างมีประสิทธิภาพ

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) จึงได้จัดทำมาตรฐานการออกและให้บริการหลักทรัพย์โทเคนฉบับนี้ขึ้น เพื่อใช้เป็นแนวทางสำหรับผู้เกี่ยวข้องในการดำเนินงานและพัฒนาระบบที่เกี่ยวข้อง โดยมุ่งส่งเสริมให้การดำเนินงานระหว่างผู้เกี่ยวข้องมีความสอดคล้องกัน สนับสนุนการพัฒนาระบบนิเวศหลักทรัพย์อิเล็กทรอนิกส์ของไทย และคำนึงถึงการคุ้มครองผู้ลงทุน

บทสรุปผู้บริหาร (Executive Summary)

มาตรฐานสำหรับการออกและให้บริการหลักทรัพย์โทเคน (Standards for Securities Tokenization) จัดทำขึ้นเพื่อเป็นแนวปฏิบัติและข้อเสนอแนะขั้นต่ำสำหรับผู้ออกหลักทรัพย์โทเคน ผู้ให้บริการสนับสนุนการออกและเสนอขายหลักทรัพย์โทเคน และผู้ประกอบธุรกิจตัวกลางที่เกี่ยวข้อง โดยมีเป้าหมายเพื่อส่งเสริมการนำเทคโนโลยีบล็อกเชนหรือเทคโนโลยีบัญชีแบบกระจายศูนย์ (Distributed Ledger Technology : DLT) มาใช้ในตลาดทุนอย่างมีมาตรฐาน สอดคล้องกับกฎหมาย และรองรับการเชื่อมโยงการทำงานระหว่างระบบและโครงสร้างพื้นฐานตลาดทุน (Capital Market Interoperability)

มาตรฐานฉบับนี้เป็นส่วนหนึ่งของการพัฒนาระบบนิเวศหลักทรัพย์อิเล็กทรอนิกส์ (Digital Securities Ecosystem : DSE) ซึ่งมุ่งสนับสนุนให้ผู้เกี่ยวข้องสามารถพัฒนาระบบและบริการของตนเองได้ภายใต้กรอบมาตรฐานร่วมที่เอื้อต่อการเชื่อมโยงและทำงานร่วมกัน โดยไม่จำเป็นต้องพึ่งพาระบบกลางเพียงระบบเดียว ทั้งนี้ การนำหลักทรัพย์มาออกในรูปแบบโทเคนเป็นการเปลี่ยนรูปแบบการบันทึกและบริหารจัดการสิทธิด้วยเทคโนโลยี โดยต้องคำนึงถึงการคงไว้ซึ่งสิทธิ หน้าที่ และผลทางกฎหมายของหลักทรัพย์ ตลอดจนความมั่นคงปลอดภัยและความน่าเชื่อถือของระบบที่เกี่ยวข้อง

มาตรฐานประกอบด้วย 4 ส่วนสำคัญ ดังนี้

ส่วนที่ 1 มาตรฐานด้านกฎหมายสำหรับการให้บริการหลักทรัพย์โทเคน

กำหนดหลักการและแนวปฏิบัติเพื่อให้การออกและให้บริการหลักทรัพย์โทเคนสอดคล้องกับกฎหมายที่เกี่ยวข้อง ครอบคลุมการออกและเสนอขาย การเชื่อมโยงระหว่างหลักทรัพย์กับโทเคน การรองรับสิทธิและผลทางกฎหมาย การเปิดเผยข้อมูล การดำเนินการภายหลังการเสนอขาย และการจัดการกรณีพิเศษที่เกี่ยวข้องกับหลักทรัพย์โทเคน

ส่วนที่ 2 มาตรฐานด้านเทคนิคสำหรับหลักทรัพย์โทเคน

กำหนดหลักการออกแบบและสถาปัตยกรรมของโทเคน ฟังก์ชันการทำงาน ข้อกำหนดด้านข้อมูล และการเชื่อมโยงการทำงานระหว่างระบบ เพื่อให้โทเคนสามารถรองรับวงจรชีวิตของหลักทรัพย์ได้อย่างเหมาะสม มีข้อมูลที่ตรวจสอบย้อนหลังได้ และสนับสนุนการทำงานร่วมกันระหว่างระบบและเครือข่ายที่เกี่ยวข้อง

ส่วนที่ 3 มาตรฐานของผู้ให้บริการสนับสนุนการออกและเสนอขายหลักทรัพย์โทเคน

กำหนดแนวปฏิบัติเกี่ยวกับบทบาทและขอบเขตการให้บริการ คุณสมบัติและความพร้อมของผู้ให้บริการ ตลอดจนมาตรฐานการปฏิบัติหน้าที่และการให้บริการ เพื่อให้การดำเนินงานของผู้เกี่ยวข้องมีความชัดเจน เหมาะสมกับขอบเขตบริการ และคำนึงถึงการคุ้มครองผู้ลงทุน

ส่วนที่ 4 มาตรฐานด้านความมั่นคงปลอดภัยทางไซเบอร์ ความเสี่ยงด้านเทคโนโลยีและความพร้อมในการดำเนินงาน

กำหนดแนวปฏิบัติด้านการกำกับดูแลและบริหารความเสี่ยงด้านเทคโนโลยี การรักษาความมั่นคงปลอดภัยของระบบและโครงสร้างพื้นฐาน DLT การควบคุมสิทธิการเข้าถึง การบริหารจัดการกุญแจเข้ารหัส การตรวจสอบย้อนหลัง การจัดการช่องโหว่ ตลอดจนการตอบสนองต่อเหตุการณ์และการรักษาความต่อเนื่องในการดำเนินงาน

มาตรฐานทั้ง 4 ส่วนมีความเชื่อมโยงกัน โดยมุ่งให้การออกและให้บริการหลักทรัพย์โทเคนมีกรอบทางกฎหมายที่ชัดเจน มีมาตรฐานทางเทคนิคและการให้บริการที่เหมาะสม และมีการบริหารจัดการความเสี่ยงอย่างเพียงพอ เพื่อสนับสนุนการพัฒนาระบบนิเวศหลักทรัพย์อิเล็กทรอนิกส์ของไทยให้สามารถรองรับนวัตกรรม การเชื่อมโยงระบบ และการพัฒนาบริการในตลาดทุนดิจิทัลได้อย่างมีประสิทธิภาพควบคู่กับความมั่นคงปลอดภัย ความโปร่งใส และการคุ้มครองผู้ลงทุน

สารบัญ

1. ขอบเขตการใช้งานมาตรฐาน 1

2. อภิธานศัพท์ 1

3. มาตรฐานด้านกฎหมายสำหรับการให้บริการหลักทรัพย์โทเคน 5

3.1 หลักการสำหรับการออกหลักทรัพย์โทเคน

3.2 การออกและเสนอขายหลักทรัพย์โทเคน

3.3 การออกแบบเทคโนโลยีเพื่อรองรับผลทางกฎหมายของหลักทรัพย์โทเคน

3.4 การเปิดเผยข้อมูลเกี่ยวกับหลักทรัพย์โทเคน

3.5 การดำเนินการภายหลังเสนอขายหลักทรัพย์โทเคน

3.6 การจัดการกรณีพิเศษที่เกี่ยวข้องกับหลักทรัพย์โทเคน

4. มาตรฐานด้านเทคนิคสำหรับหลักทรัพย์โทเคน 27

4.1 หลักการออกแบบและสถาปัตยกรรมของโทเคน

4.2 ฟังก์ชันการทำงานของโทเคน

4.3 ข้อกำหนดด้านข้อมูลของโทเคน

4.4 ข้อกำหนดด้านการทำงานร่วมกันระหว่างระบบ

5. มาตรฐานของผู้ให้บริการสนับสนุนการออกและเสนอขายหลักทรัพย์โทเคน 59

5.1 บทบาทและขอบเขตการให้บริการ

5.2 คุณสมบัติและความพร้อมของผู้ให้บริการ

5.3 มาตรฐานการปฏิบัติหน้าที่และการให้บริการ

5.4 แนวทางการดำเนินงานตามขอบเขตของผู้ให้บริการสนับสนุนการออกและการเสนอขายหลักทรัพย์โทเคน

6. ความมั่นคงปลอดภัยทางไซเบอร์ ความเสี่ยงด้านเทคโนโลยีและความพร้อมในการดำเนินงาน 104

6.1 การกำกับดูแลและความเสี่ยงด้านเทคโนโลยี

6.2 ระบบ แอปพลิเคชันและโครงสร้างพื้นฐาน DLT

6.3 การพิสูจน์ตัวตนและการควบคุมสิทธิการเข้าถึง

6.4 การบริหารจัดการกุญแจเข้ารหัสและการดำเนินการที่มีสิทธิพิเศษ

6.5 ความปลอดภัย ความถูกต้องครบถ้วน และการรับรองข้อมูล

6.6 การติดตามเหตุการณ์ การบันทึกข้อมูล และการตรวจสอบย้อนหลัง
6.7 การบริหารจัดการช่องโหว่และการทดสอบด้านความมั่นคงปลอดภัย
6.8 การตอบสนองต่อเหตุการณ์และความพร้อมด้านการดำเนินงาน
7. ภาคผนวก **155**
ตัวอย่าง Tokenization Terms
8. บรรณานุกรม **158**

1. ขอบเขตการใช้งานมาตรฐาน (Scope)

มาตรฐานฉบับนี้จัดทำขึ้นสำหรับผู้เกี่ยวข้องกับการออกและให้บริการหลักทรัพย์โทเคน โดยมีกลุ่มเป้าหมายหลัก 3 กลุ่ม ได้แก่

(1) ผู้ออกหลักทรัพย์โทเคน (Issuer) ซึ่งมีหน้าที่รับผิดชอบการออกและเสนอขายหลักทรัพย์โทเคน

(2) ผู้ให้บริการสนับสนุนการออกและเสนอขายหลักทรัพย์โทเคน (Securities Tokenizer) ซึ่งให้บริการหรือดำเนินการสนับสนุนการออกและเสนอขายหลักทรัพย์โทเคน รวมถึงการดำเนินงานที่เกี่ยวข้องตามขอบเขตบริการของตน

(3) ผู้ประกอบธุรกิจตัวกลางที่เกี่ยวข้อง (Intermediaries) ซึ่งให้บริการเกี่ยวกับกระเป๋าอิเล็กทรอนิกส์หรือการเก็บรักษาหลักทรัพย์โทเคน หรือดำเนินธุรกรรมที่เกี่ยวข้องกับหลักทรัพย์โทเคน

นอกจากนี้ มาตรฐานฉบับนี้ยังสามารถใช้เป็นกรอบอ้างอิงสำหรับผู้ให้บริการด้านเทคโนโลยีและผู้ให้บริการอื่นที่เกี่ยวข้องกับการออกหรือให้บริการหลักทรัพย์โทเคน รวมถึงบุคคลหรือองค์กรที่สนใจศึกษาแนวทางและมาตรฐานที่เกี่ยวข้อง ทั้งนี้ ผู้เกี่ยวข้องควรพิจารณานำเนื้อหาในส่วนที่เกี่ยวข้องไปใช้ให้เหมาะสมกับบทบาท หน้าที่ และขอบเขตการดำเนินงานของตน โดยคำนึงถึงกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง

2. อภิธานศัพท์ (Glossary)

ความหมายของคำที่ใช้ในมาตรฐานฉบับนี้ มีดังนี้

(1) “หลักทรัพย์โทเคน” (Securities Token) หมายถึง หลักทรัพย์ที่ออก บันทึก หรือแสดงสิทธิในรูปแบบโทเคนบนระบบหรือเครือข่ายอิเล็กทรอนิกส์ โดยอาศัยเทคโนโลยีบล็อกเชนหรือเทคโนโลยีบัญชีแบบกระจายศูนย์ (Distributed Ledger Technology: DLT) หรือเทคโนโลยีอื่นที่มีคุณลักษณะเทียบเท่า โดยโทเคนดังกล่าวมีความเชื่อมโยงกับหลักทรัพย์หรือสิทธิในหลักทรัพย์นั้นตามโครงสร้างทางกฎหมายที่เกี่ยวข้อง

(2) “ผู้ออกหลักทรัพย์โทเคน” (Issuer) หมายถึง บริษัท บริษัทจำกัด หรือ บริษัทมหาชนจำกัด รวมถึงหน่วยงาน องค์กร นิติบุคคล หรือผู้ออกหลักทรัพย์อื่น ซึ่งมีความประสงค์ที่จะระดมทุนจากผู้ลงทุนที่เป็นประชาชนทั่วไปผ่านการออกหลักทรัพย์โทเคนตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง

(3) “ผู้ให้บริการสนับสนุนการออกและเสนอขายหลักทรัพย์โทเคน” (Securities Tokenizer) หมายถึง บุคคลที่ให้บริการหรือดำเนินการเกี่ยวกับหลักทรัพย์โทเคน ซึ่งอาจครอบคลุมการออก การจัดทำและบันทึกข้อมูล การจัดสรรและส่งมอบ การโอน การใช้หลักทรัพย์

โทเคนเป็นหลักประกัน การชำระราคาและส่งมอบหลักทรัพย์ การให้บริการด้านกระเป๋าอิเล็กทรอนิกส์ ตลอดจนการรับฝากหรือเก็บรักษาหลักทรัพย์โทเคนและการดำเนินการที่เกี่ยวข้องกับสิทธิของผู้ถือหลักทรัพย์ ทั้งนี้ ขอบเขตหน้าที่ของบุคคลดังกล่าวขึ้นอยู่กับรูปแบบการให้บริการและการแบ่งหน้าที่กับผู้ออกหลักทรัพย์ นายทะเบียน ผู้รับฝากทรัพย์สิน หรือผู้ให้บริการโครงสร้างพื้นฐานรายอื่น โดยไม่จำเป็นต้องให้บริการหรือดำเนินการในทุกด้าน

(4) “ผู้ประกอบธุรกิจหลักทรัพย์ที่เป็นตัวกลาง” (Intermediaries) หมายถึง ผู้ประกอบธุรกิจหลักทรัพย์ที่ได้รับอนุญาตจากสำนักงาน ก.ล.ต. ให้ประกอบธุรกิจ หลักทรัพย์ และให้บริการหรือแสดงต่อบุคคลทั่วไปว่าพร้อมจะให้บริการเก็บรักษาทรัพย์สินลูกค้าที่เป็นหลักทรัพย์โทเคน (Custodial Service) ตามหลักเกณฑ์ที่สำนักงาน ก.ล.ต. กำหนด

(5) “การให้บริการเก็บรักษาหลักทรัพย์โทเคน” (Custodial Service) หมายถึง การให้บริการหรือแสดงต่อบุคคลทั่วไปว่าพร้อมจะให้บริการอย่างใดอย่างหนึ่งหรือหลายอย่างดังต่อไปนี้

- รับฝากหรือเก็บรักษาหลักทรัพย์โทเคน
- บริหารจัดการกุญแจเข้ารหัส (Cryptographic Key) หรือสิ่งอื่นใดที่ต้องเก็บรักษาเป็นความลับ เพื่อใช้อนุมัติการโอนหรือการทำธุรกรรมเกี่ยวกับหลักทรัพย์ทรัพย์โทเคน โดยมีอำนาจเบ็ดเสร็จหรือบางส่วน

(6) “กระเป๋าอิเล็กทรอนิกส์” (Wallet) หมายถึง อุปกรณ์ ระบบ หรือกลไกทางอิเล็กทรอนิกส์ที่ใช้ในการเข้าถึง ควบคุม หรือดำเนินธุรกรรมเกี่ยวกับหลักทรัพย์โทเคน โดยอาศัยกุญแจเข้ารหัส (Cryptographic Key) ข้อมูลรับรอง หรือกลไกอื่นที่ใช้ในการยืนยันตัวตนหรืออนุมัติการดำเนินการที่เกี่ยวข้อง

(7) “กระเป๋าอิเล็กทรอนิกส์ที่ผู้ใช้เก็บรักษาด้วยตนเอง” (Non-Custodial Wallet) หมายถึง กระเป๋าอิเล็กทรอนิกส์ที่ผู้ใช้งานเป็นผู้เก็บรักษาและควบคุมกุญแจเข้ารหัส (Cryptographic Key) หรือชุดคำสำหรับกู้คืนกระเป๋า (Seed Phrase) ด้วยตนเอง และเป็นผู้อนุมัติธุรกรรมเกี่ยวกับหลักทรัพย์โทเคน โดยไม่มีผู้ให้บริการหรือบุคคลภายนอกเก็บรักษาหรือควบคุมกุญแจดังกล่าวแทนผู้ใช้งาน

(8) “เทคโนโลยีบัญชีแบบกระจายศูนย์” (Distributed Ledger Technology: DLT) หมายถึง เทคโนโลยีที่ใช้ในการบันทึก จัดเก็บ และปรับปรุงข้อมูลหรือรายการธุรกรรมในบัญชีที่มีการกระจายข้อมูลไปยังผู้เข้าร่วมในระบบหรือเครือข่ายหลายแห่ง โดยมีกระบวนการการตรวจสอบและกลไกเพื่อให้ผู้เข้าร่วมในระบบหรือเครือข่ายบรรลุฉันทามติ (Consensus) เกี่ยวกับข้อมูลหรือธุรกรรมที่บันทึกไว้

(9) “บล็อกเชน” (Blockchain) หมายถึง เทคโนโลยีบัญชีแบบกระจายศูนย์ที่มีการจัดเก็บข้อมูลหรือรายการธุรกรรมเป็นชุดข้อมูล (Block) ซึ่งเชื่อมโยงกันตามลำดับโดยใช้วิธีการทางวิทยาการเข้ารหัส (Cryptography) และมีกลไกในการตรวจสอบและยืนยันความถูกต้องของข้อมูลตามหลักเกณฑ์ของระบบหรือเครือข่าย ทั้งนี้ เครือข่ายบล็อกเชนอาจมีรูปแบบการกำหนดสิทธิในการเข้าร่วมและดำเนินการแตกต่างกัน เช่น

- เครือข่ายที่จำกัดสิทธิในการเข้าร่วม หรือการดำเนินการบางประการไว้สำหรับบุคคลที่ได้รับอนุญาต (Permissioned Blockchain)
- เครือข่ายที่เปิดให้เข้าร่วมหรือการดำเนินการได้โดยไม่ต้องได้รับอนุญาตจากผู้มีอำนาจ (Permissionless Blockchain)

(10) “กลไกฉันทามติ” (Consensus Mechanism) หมายถึง กลไกหรือหลักเกณฑ์ที่ใช้เพื่อให้ผู้เข้าร่วมในระบบหรือเครือข่ายที่ใช้เทคโนโลยีบัญชีแบบกระจายศูนย์ได้ข้อยุติร่วมกันเกี่ยวกับความถูกต้องและสถานะของข้อมูลหรือรายการธุรกรรม เช่น กลไก Proof of Work (PoW) : ใช้การแข่งขันในการคำนวณเพื่อให้ได้สิทธิในการเพิ่มบล็อก หรือกลไก Proof of Stake (PoS) : ใช้กลไกที่เกี่ยวข้องกับการวางสินทรัพย์ค้ำประกัน (Stake) และการเลือกหรือกำหนดผู้ตรวจสอบธุรกรรม เป็นต้น

(11) “สัญญาอัจฉริยะ” (Smart Contract) หมายถึง ชุดคำสั่งหรือโปรแกรมคอมพิวเตอร์ที่ทำงานบนเทคโนโลยีบัญชีแบบกระจายศูนย์หรือบล็อกเชน และใช้ในการตรวจสอบประมวลผล หรือดำเนินการตามเงื่อนไขหรือหลักเกณฑ์ที่กำหนดไว้ในชุดคำสั่งนั้น

(12) “ตราสารเปลี่ยนมืออิเล็กทรอนิกส์” (Electronic Transferable Record: ETR) หมายถึง ข้อมูลหรือชุดข้อมูลในรูปแบบอิเล็กทรอนิกส์ที่มีคุณสมบัติเทียบเท่าเอกสารหรือตราสารที่เปลี่ยนมือได้ โดยสามารถระบุบันทึกดังกล่าวได้อย่างเฉพาะเจาะจง อยู่ภายใต้การควบคุมตั้งแต่เวลาที่จัดทำขึ้นจนสิ้นผลหรือสิ้นความสมบูรณ์ และสามารถรักษาความครบถ้วนถูกต้องของบันทึกดังกล่าวได้

(13) “การมีหนึ่งเดียว” (Singularity) หมายถึง คุณลักษณะที่ทำให้หลักทรัพย์โทเคนหรือข้อมูลที่ใช้แสดงสิทธิในหลักทรัพย์สามารถระบุได้อย่างเฉพาะเจาะจงว่าเป็นรายการที่ใช้แสดงสิทธินั้น โดยมีกลไกป้องกันมิให้มีการสร้างหรือใช้รายการอื่นเพื่อแสดงหรือเรียกร้องสิทธิเดียวกันซ้ำซ้อนโดยมิชอบ

(14) “การควบคุม” (Control) หมายถึง ความสามารถของบุคคลในการดำเนินการ หรือกำหนดให้มีการดำเนินการเกี่ยวกับหลักทรัพย์โทเคนตามสิทธิหรืออำนาจที่บุคคลนั้นมี

เช่น การโอน การใช้สิทธิ หรือการดำเนินการอื่นที่เกี่ยวข้อง โดยมีกลไกที่สามารถระบุบุคคลดังกล่าว และป้องกันการดำเนินการโดยบุคคลที่ไม่มีสิทธิหรืออำนาจได้

(15) “การควบคุมแต่เพียงผู้เดียว” (Exclusive Control) หมายถึง สภาวะที่บุคคลหนึ่งหรือกลุ่มบุคคลหนึ่งมีอำนาจควบคุมเหนือหลักทรัพย์โทเคนนั้น โดยสามารถระบุตัวบุคคลหรือกลุ่มบุคคลดังกล่าวได้ว่าเป็นผู้มีอำนาจควบคุม และสามารถป้องกันมิให้บุคคลอื่นที่ไม่มีอำนาจดำเนินการเกี่ยวกับหลักทรัพย์โทเคนได้ ทั้งนี้ การควบคุมอาจดำเนินการแทนผู้มีสิทธิควบคุมหรือมีขึ้นเป็นการชั่วคราวตามกฎหมาย หรือคำสั่งของผู้มีอำนาจ โดยการควบคุมดังกล่าวไม่ทำให้สิทธิหรือกรรมสิทธิ์ในหลักทรัพย์โทเคนเปลี่ยนแปลงไปเพียงเพราะมีการเปลี่ยนแปลงผู้ควบคุม

(16) “ข้อมูลรับรอง” (Credential) หมายถึง ข้อมูลหรือชุดข้อมูลที่ใช้ในการยืนยันตัวตน คุณลักษณะ หรือสิทธิของบุคคล ระบบ หรือสิ่งอื่นใด เพื่อประกอบการตรวจสอบหรืออนุญาตให้เข้าถึงข้อมูล ระบบ หรือดำเนินการตามที่กำหนด

(17) “แหล่งข้อมูลอ้างอิงหลัก” (Authoritative Source) หมายถึง แหล่งข้อมูลหรือระบบที่กำหนดให้ใช้เป็นแหล่งอ้างอิงหลักสำหรับข้อมูลประเภทหนึ่ง เมื่อข้อมูลเดียวกันถูกบันทึกหรือปรากฏอยู่ในหลายระบบหรือหลายแหล่ง

(18) “ความสมบูรณ์ของธุรกรรมการโอน” (Transfer Finality) หมายถึง จุดเวลาที่การโอนหลักทรัพย์โทเคนมีผลสมบูรณ์และไม่อาจเพิกถอนหรือย้อนกลับได้ตามกฎหมายและหลักเกณฑ์ของระบบที่เกี่ยวข้อง โดยสิทธิในหลักทรัพย์ของผู้โอนได้ถูกโอนไปยังผู้รับโอนอย่างมีผลสมบูรณ์

(19) “ความสมบูรณ์ของการชำระราคาและส่งมอบ” (Settlement Finality) หมายถึง จุดเวลาที่การชำระราคาและการส่งมอบที่เกี่ยวข้องกับธุรกรรมหลักทรัพย์โทเคนถือว่าเสร็จสมบูรณ์และเป็นที่สุดตามกฎหมาย หลักเกณฑ์ และเงื่อนไขของระบบที่เกี่ยวข้อง โดยไม่อาจเพิกถอนหรือย้อนกลับได้

(20) “การเชื่อมโยงการทำงานข้ามกันระหว่างเครือข่าย” (Interoperability) หมายถึง ความสามารถของระบบหรือเครือข่ายที่เกี่ยวข้องกับหลักทรัพย์โทเคนในการเชื่อมต่อแลกเปลี่ยนข้อมูล หรือดำเนินธุรกรรมระหว่างกันได้อย่างสอดคล้อง โดยไม่จำเป็นต้องใช้ระบบหรือเทคโนโลยีเดียวกัน

3. มาตรฐานด้านกฎหมายสำหรับหลักทรัพย์โทเคน (Legal Standard)

หลักทรัพย์โทเคนเป็นการนำเทคโนโลยีดิจิทัล เช่น บล็อกเชน หรือ Distributed Ledger Technology (“DLT”) มาใช้ในการบันทึกและบริหารจัดการข้อมูล สิทธิ และธุรกรรมที่เกี่ยวข้องกับหลักทรัพย์ ซึ่งการนำเทคโนโลยีดังกล่าวมาใช้ จำเป็นต้องคำนึงถึงความสอดคล้องระหว่างการดำเนินการทางเทคโนโลยีกับสิทธิ หน้าที่ และผลทางกฎหมายของหลักทรัพย์ตลอดอายุของหลักทรัพย์

มาตรฐานในบทนี้มุ่งกำหนดหลักการพื้นฐาน และแนวทางปฏิบัติที่เกี่ยวข้องกับสิทธิ หน้าที่ และผลทางกฎหมายของหลักทรัพย์โทเคน ตั้งแต่การออกและเสนอขาย การเชื่อมโยงระหว่างหลักทรัพย์กับโทเคน การออกแบบเทคโนโลยีเพื่อรองรับสิทธิและการดำเนินการตามกฎหมาย การเปิดเผยข้อมูลการดำเนินการภายหลังการออกและเสนอขาย ตลอดจนการจัดการกรณีพิเศษที่เกี่ยวข้องกับหลักทรัพย์โทเคน เพื่อให้การดำเนินการเกี่ยวกับหลักทรัพย์โทเคนเป็นไปอย่างถูกต้องและสอดคล้องกับกฎหมายที่เกี่ยวข้อง

ทั้งนี้ มาตรฐานฉบับนี้ไม่ครอบคลุมข้อกำหนดด้านฟังก์ชันและคุณลักษณะทางเทคนิคของโทเคน ข้อกำหนดด้านความมั่นคงปลอดภัยและความเสี่ยงด้านเทคโนโลยี ตลอดจนข้อกำหนดด้านการกำกับดูแลและการดำเนินงานของผู้ประกอบธุรกิจ ซึ่งให้เป็นไปตามมาตรฐานและหลักเกณฑ์ที่เกี่ยวข้อง

3.1 หลักการสำหรับการออกหลักทรัพย์โทเคน (Principles of Securities Token)

การนำหลักทรัพย์มาออกในรูปแบบโทเคนเป็นเพียงการเปลี่ยนแปลงรูปแบบการบันทึกและการบริหารจัดการหลักทรัพย์โดยอาศัยเทคโนโลยีเป็นเครื่องมือ ทั้งนี้ การใช้เทคโนโลยีดังกล่าวจะต้องไม่ก่อให้เกิดการเปลี่ยนแปลงสถานะ สิทธิ หน้าที่ หรือผลทางกฎหมายของหลักทรัพย์ เว้นแต่กฎหมายกำหนดไว้เป็นอย่างอื่น

มาตรฐานในข้อนี้ จึงมุ่งเน้นไปที่การวางกรอบสำหรับการออกหลักทรัพย์โทเคนเพื่อให้เข้าใจในหลักการพื้นฐานสำคัญ ก่อนที่มาตรฐานในข้ออื่นจะกำหนดแนวทางเพื่อให้ผู้ออกหลักทรัพย์โทเคนและผู้ให้บริการที่เกี่ยวข้องปฏิบัติตามได้อย่างถูกต้องต่อไป โดยหลักการดังกล่าวจะครอบคลุมการพิจารณาหลักทรัพย์ที่สามารถออกในรูปแบบโทเคน การคงไว้ซึ่งสิทธิ หน้าที่ และผลทางกฎหมายของหลักทรัพย์ ซึ่งรวมถึงกรณีที่ผู้ลงทุนถือครองหลักทรัพย์โทเคนผ่านผู้ให้บริการตัวกลางด้วย โดยมีรายละเอียดต่อไปนี้

3.1.1 หลักทรัพย์ที่สามารถออกในรูปแบบโทเคน (Eligible Securities)

หลักทรัพย์โทเคน (Securities Token) เป็นการนำหลักทรัพย์ที่มีอยู่ตามกฎหมายมาออกและบันทึกในรูปแบบโทเคน โดยใช้เทคโนโลยีเป็นเครื่องมือในการบริหารจัดการสิทธิและธุรกรรมที่เกี่ยวข้องกับหลักทรัพย์ ดังนั้น การออกหลักทรัพย์ในรูปแบบโทเคนจึงไม่ได้ก่อให้เกิด

หลักทรัพย์ประเภทใหม่ แต่เป็นการเปลี่ยนแปลงรูปแบบการบันทึกและการแสดงสิทธิของหลักทรัพย์เดิม โดยสิทธิ หน้าที่ และผลทางกฎหมายของหลักทรัพย์ยังคงเป็นไปตามกฎหมายที่เกี่ยวข้อง

ดังนั้น หลักทรัพย์ที่จะออกในรูปแบบโทเคนต้องเป็นหลักทรัพย์ที่สามารถออกได้โดยชอบด้วยกฎหมาย และอยู่ภายใต้ประเภทและหลักเกณฑ์ที่กฎหมายกำหนด โดยหลักทรัพย์ที่สามารถออก ในรูปแบบโทเคน เช่น หุ้นกู้ หรือหน่วยลงทุนอันได้แก่ ตราสารหรือหลักฐานแสดงสิทธิในทรัพย์สินของกองทุนรวม เป็นต้น

3.1.2 การคงไว้ซึ่งสิทธิและผลทางกฎหมายของหลักทรัพย์ (Preservation of Legal Rights and Legal Effects)

การออกหลักทรัพย์ในรูปแบบโทเคนไม่ทำให้สิทธิ หน้าที่ และผลทางกฎหมายที่เกี่ยวข้องกับหลักทรัพย์เปลี่ยนแปลงไป ผู้ถือหลักทรัพย์โทเคนจึงยังคงมีสิทธิและหน้าที่เช่นเดียวกับผู้ถือหลักทรัพย์ในรูปแบบอื่นตามประเภทของหลักทรัพย์ เช่น สิทธิในฐานะเจ้าหนี้กรณีหุ้นกู้ สิทธิในฐานะผู้ถือหน่วยลงทุนกรณีกองทุนรวม หรือสิทธิในฐานะผู้ถือหุ้นกรณีหุ้น

ผู้ถือโทเคนสามารถใช้สิทธิในหลักทรัพย์โทเคน ได้เช่นเดียวกับหลักทรัพย์แบบไร้ใบหลักทรัพย์ (Scripless) หรือหลักทรัพย์แบบมีใบหลักทรัพย์ เช่น การโอน การรับผลประโยชน์ หรือการใช้สิทธิในฐานะผู้ถือหลักทรัพย์ และมีผลทางกฎหมายสอดคล้องกับการดำเนินการกับหลักทรัพย์ในรูปแบบอื่น โดยการเปลี่ยนแปลงหรือการโอนสิทธิในหลักทรัพย์ต้องสามารถระบุผู้มีสิทธิในหลักทรัพย์และหลักฐานที่ใช้ยืนยันสิทธิดังกล่าวได้อย่างชัดเจน รวมถึงต้องมีการกำหนดหลักเกณฑ์และขั้นตอนในการระบุจุดที่ธุรกรรมการโอนมีผลสมบูรณ์อย่างชัดเจน (Transfer Finality)

3.1.3 การถือครองหลักทรัพย์โทเคนผ่านผู้ประกอบธุรกิจตัวกลาง (Intermediated Holding of Tokenized Securities)

การถือครองหลักทรัพย์โทเคนจะดำเนินการจัดเก็บผ่านกระเป๋าอิเล็กทรอนิกส์ (Wallet) โดยสามารถดำเนินการได้ทั้งในลักษณะที่ผู้ถือหลักทรัพย์ถือครองและควบคุมโทเคนด้วยตนเอง (Non-Custodial Wallet) หรือผ่านผู้ประกอบธุรกิจตัวกลางที่ทำหน้าที่ถือครองหรือบริหารจัดการหลักทรัพย์โทเคนแทนผู้ถือหลักทรัพย์ (Custodial service) ทั้งนี้ รูปแบบการถือครองดังกล่าวไม่ทำให้สิทธิ หน้าที่ หรือผลทางกฎหมายของผู้ถือหลักทรัพย์เปลี่ยนแปลงไป

ในกรณีที่หลักทรัพย์โทเคนถูกถือครองผ่านผู้ประกอบธุรกิจตัวกลาง ต้องสามารถระบุและพิสูจน์ผู้ถือหลักทรัพย์หรือผู้มีสิทธิในหลักทรัพย์โทเคนได้อย่างชัดเจน และการบันทึกหรือบริหารจัดการสิทธิของผู้ถือหลักทรัพย์อาจดำเนินการผ่านระบบของผู้ให้บริการตัวกลางได้ โดยไม่จำเป็นต้องมีการโอนหลักทรัพย์โทเคนบนบล็อกเชน / DLT ทุกครั้ง ทั้งนี้ การดำเนินการดังกล่าวต้องไม่กระทบต่อสิทธิและผลทางกฎหมายของผู้ถือหลักทรัพย์

3.2 การออกและการเสนอขายหลักทรัพย์โทเคน (Issuance and Offering of Tokenized Securities)

การออกและเสนอขายหลักทรัพย์โทเคน นอกจากต้องดำเนินการให้เป็นไปตามกฎหมายและหลักเกณฑ์ที่ใช้บังคับกับหลักทรัพย์แต่ละประเภทแล้ว ผู้ออกหลักทรัพย์ต้องสามารถระบุและเชื่อมโยงหลักทรัพย์กับโทเคนได้อย่างชัดเจนตลอดกระบวนการ ตั้งแต่การออกและเสนอขาย การจัดสรร การชำระราคาและส่งมอบ ตลอดจนการเริ่มต้นการถือครองหลักทรัพย์โทเคน เพื่อให้หลักทรัพย์โทเคนที่ออกสามารถแสดงและรองรับสิทธิและผลทางกฎหมายของหลักทรัพย์ที่เกี่ยวข้องได้อย่างถูกต้อง

ในการดำเนินการดังกล่าว ควรมีกลไกและเอกสารที่ทำให้ความสัมพันธ์ระหว่างหลักทรัพย์กับโทเคนมีความชัดเจนและสามารถตรวจสอบได้ รวมถึงข้อมูลหรือหลักฐานที่ใช้ยืนยันการเชื่อมโยงดังกล่าว ตลอดจนข้อกำหนดและเงื่อนไขที่เกี่ยวข้องกับการออกหลักทรัพย์โทเคน การกำหนดสิทธิและเงื่อนไขของผู้ถือหลักทรัพย์ และการสร้างและจัดสรรหลักทรัพย์โทเคน โดยรายละเอียดของการดำเนินการในแต่ละเรื่องให้เป็นไปตามแนวทางปฏิบัติที่กำหนดในข้อย่อยต่อไปนี้

3.2.1 การออกหลักทรัพย์โดยชอบด้วยกฎหมาย (Valid Issuance of Securities)

ผู้ออกหลักทรัพย์ยังคงต้องปฏิบัติตามกฎหมายว่าด้วยหลักทรัพย์และตลาดหลักทรัพย์ รวมถึงหลักเกณฑ์ที่ใช้บังคับกับหลักทรัพย์แต่ละประเภทก่อนดำเนินการออกหลักทรัพย์โทเคน ดังนั้น ผู้ออกหลักทรัพย์ควรดำเนินการให้มั่นใจว่าหลักทรัพย์ดังกล่าวได้ออกและเสนอขายโดยชอบด้วยกฎหมาย และไม่ส่งผลกระทบต่อสถานะ สิทธิ หรือผลทางกฎหมายของหลักทรัพย์นั้น

แนวทางปฏิบัติ : ผู้ออกหลักทรัพย์ควรดำเนินการอย่างน้อยดังต่อไปนี้

(1) **การออกและเสนอขายหลักทรัพย์โทเคน :** ผู้ออกหลักทรัพย์ที่ประสงค์จะออกและเสนอขายหลักทรัพย์โทเคน ต้องดำเนินการให้เป็นไปตามพระราชบัญญัติหลักทรัพย์และตลาดหลักทรัพย์ รวมถึงประกาศ หลักเกณฑ์และเงื่อนไขที่เกี่ยวข้องกับการออกและเสนอขายหลักทรัพย์ประเภทนั้น

(2) **การปฏิบัติตามหลักเกณฑ์เฉพาะของหลักทรัพย์แต่ละประเภท :** ผู้ออกหลักทรัพย์ต้องปฏิบัติตามหลักเกณฑ์เฉพาะที่ใช้กับหลักทรัพย์แต่ละประเภท เช่น หลักเกณฑ์การเสนอขายตราสารหนี้ หลักเกณฑ์เกี่ยวกับการจัดตั้งกองทุน การแบ่งชนิดหน่วยลงทุน (Share Class) หรือข้อกำหนดเฉพาะอื่นที่เกี่ยวข้อง (ถ้ามี)

3.2.2 การจัดให้มีการเชื่อมโยงระหว่างหลักทรัพย์กับโทเคน (Establishing Legal Linkage between Securities and Tokens)

ผู้ออกหลักทรัพย์ต้องจัดให้มีการเชื่อมโยงระหว่างหลักทรัพย์กับโทเคนที่ทำหน้าที่เป็นตัวแทนในการแสดงสิทธิในหลักทรัพย์ประเภทนั้นอย่างชัดเจนและสามารถพิสูจน์ได้ โดยความเชื่อมโยง

ดังกล่าวควรสามารถตรวจสอบและติดตามได้ตลอดอายุของหลักทรัพย์ รวมถึงรองรับการดำเนินการเมื่อหลักทรัพย์ถูกยกเลิก สิ้นสุด หรือมีการเปลี่ยนแปลงที่ส่งผลต่อความเชื่อมโยงระหว่างหลักทรัพย์กับโทเคน

แนวทางปฏิบัติ : ผู้ออกหลักทรัพย์ควรจัดให้มีกลไกในการระบุและตรวจสอบความเชื่อมโยงระหว่างหลักทรัพย์กับโทเคน เพื่อให้สามารถพิสูจน์ได้ว่าโทเคนดังกล่าวเกี่ยวข้องกับหลักทรัพย์ใด โดยมีแนวทางปฏิบัติอย่างน้อยดังต่อไปนี้

(1) **การระบุความเชื่อมโยงระหว่างหลักทรัพย์กับโทเคน (Identification of Legal Linkage) :** ผู้ออกหลักทรัพย์ควรจัดให้มีข้อมูลหรือกลไกเชื่อมโยงระหว่างหลักทรัพย์กับโทเคน เช่น สิ่งที่ใช้ระบุเอกลักษณ์ (Unique Identifier) รหัสหลักทรัพย์สากล (International Securities Identification Number) หรือข้อมูลอ้างอิงอื่นที่พิสูจน์ความสัมพันธ์ระหว่างหลักทรัพย์กับโทเคน

(2) **การตรวจสอบความเชื่อมโยงระหว่างหลักทรัพย์กับโทเคน (Verification of Legal Linkage) :** ผู้ออกหลักทรัพย์ควรจัดให้มีช่องทางที่ผู้ถือหลักทรัพย์โทเคนสามารถตรวจสอบความเชื่อมโยงระหว่างหลักทรัพย์กับโทเคนได้ด้วยตนเอง โดยข้อมูลหรือหลักฐานที่แสดงผ่านช่องทางดังกล่าวต้องสามารถระบุความสัมพันธ์ระหว่างหลักทรัพย์กับโทเคนได้อย่างชัดเจน ทั้งนี้ ผู้ออกหลักทรัพย์อาจดำเนินการผ่านช่องทางหรือกลไกที่เหมาะสม เช่น การจัดให้ข้อมูลที่เกี่ยวข้องสามารถเข้าถึงและตรวจสอบได้ผ่าน Smart Contract หรือบนบล็อกเชน / DLT การอ้างอิงเอกสารที่เกี่ยวข้องด้วย Unique Identifier หรือ Envelope Number[1] หรือการเผยแพร่ข้อมูลผ่านช่องทางของผู้ออกหลักทรัพย์ เป็นต้น

(3) **กรณีมีการเปลี่ยนแปลงความเชื่อมโยงระหว่างหลักทรัพย์กับโทเคน (Changes to Legal Linkage) :** ผู้ออกหลักทรัพย์ต้องมีกลไกและกระบวนการที่เหมาะสมสำหรับรองรับการเปลี่ยนแปลงหรือยกเลิกความเชื่อมโยงระหว่างหลักทรัพย์กับโทเคน เพื่อให้ความเชื่อมโยงดังกล่าวยังคงถูกต้อง สอดคล้องกับหลักทรัพย์ที่เกี่ยวข้อง และไม่กระทบต่อสิทธิของผู้ถือหลักทรัพย์โทเคนหรือผลทางกฎหมายของหลักทรัพย์ การดำเนินการดังกล่าวอาจครอบคลุมกรณีที่มีการเปลี่ยนแปลงข้อมูลสำคัญของหลักทรัพย์ การแตก รวม หรือแปลงสภาพหลักทรัพย์ หรือการดำเนินการอื่นที่ส่งผลต่อสิทธิของผู้ถือหลักทรัพย์ (Corporate Actions) การเปลี่ยนหรือย้าย DLT / Smart Contract ที่ใช้ในการบริหารจัดการโทเคน การออกโทเคนใหม่

[1] รหัสหรือหมายเลขเฉพาะที่ใช้ระบุตัวตนและติดตามเอกสารอิเล็กทรอนิกส์

เพื่อทดแทนโทเคนเดิม (Reissuance) ตลอดจนการดำเนินการกับโทเคนเมื่อหลักทรัพย์ครบกำหนดหรือสิ้นสุดลง เป็นต้น

3.2.3 ข้อกำหนดการออกหลักทรัพย์รูปแบบโทเคน ("Tokenization Terms")

ผู้ออกหลักทรัพย์ควรจัดให้มีและเปิดเผยข้อกำหนดและเงื่อนไขเกี่ยวกับการออกหลักทรัพย์ในรูปแบบโทเคน (Tokenization Terms) เพื่อกำหนดความสัมพันธ์ระหว่างผู้ออกหลักทรัพย์กับผู้ถือโทเคน ตลอดจนสิทธิ หน้าที่ และเงื่อนไขที่เกี่ยวข้องกับการออกและการถือครองหลักทรัพย์โทเคน โดยอาจจัดทำเป็นเอกสารเฉพาะในรูปแบบ Tokenization Terms หรือรวมเป็นส่วนหนึ่งของข้อกำหนดสิทธิ หนังสือชี้ชวน หรือเอกสารทางกฎหมายอื่นของหลักทรัพย์ก็ได้

แนวทางปฏิบัติ : ผู้ออกหลักทรัพย์ควรจัดทำและเปิดเผย Tokenization Terms ให้ผู้ลงทุนและผู้ถือหลักทรัพย์โทเคนสามารถรับทราบและเข้าใจเงื่อนไขที่เกี่ยวข้องกับการออก และการถือครองหลักทรัพย์โทเคน โดย Tokenization Terms ควรครอบคลุมสาระสำคัญที่เกี่ยวข้องกับการออกหลักทรัพย์โทเคน และมีผลผูกพันต่อผู้ถือหลักทรัพย์โทเคนตามเงื่อนไขที่กำหนด อย่างน้อยดังต่อไปนี้

- ขอบเขตและวัตถุประสงค์ (Scope and Objectives)
- การเชื่อมโยงหลักทรัพย์กับโทเคน (Legal Linkage)
- ธุรกรรมและผลทางกฎหมายของหลักทรัพย์โทเคน (Transactions and Legal Effects)
- การดำเนินการในกรณีพิเศษ (Special Events)
- การแก้ไขเพิ่มเติมข้อกำหนดและเงื่อนไข (Amendments to Tokenization Terms)

ทั้งนี้ ตัวอย่างรายละเอียดของ Tokenization Terms ในแต่ละหัวข้อแสดงไว้ในเอกสารแนบท้าย ซึ่งผู้ออกหลักทรัพย์สามารถเพิ่มเติมรายละเอียดได้ตามลักษณะของหลักทรัพย์และเงื่อนไขที่เกี่ยวข้อง

3.2.4 การสร้าง การจัดสรร และการส่งมอบหลักทรัพย์โทเคน (Creation, Allocation and Delivery of Tokenized Securities)

ผู้ออกหลักทรัพย์ควรดำเนินการสร้าง จัดสรร และส่งมอบหลักทรัพย์โทเคนให้แก่ผู้ลงทุนที่มีสิทธิได้รับจัดสรรตามผลการเสนอขาย โดยการดำเนินการดังกล่าวต้องเป็นไปตามจำนวนและประเภทของหลักทรัพย์ที่ผู้ลงทุนมีสิทธิได้รับ รวมทั้งสอดคล้องกับกฎหมาย เงื่อนไขการเสนอขาย และข้อกำหนดที่เกี่ยวข้อง

การสร้าง การจัดสรร และการส่งมอบหลักทรัพย์โทเคนควรมีความถูกต้อง สามารถพิสูจน์และตรวจสอบได้ว่าเป็นไปตามสิทธิของผู้ลงทุน โดยผู้ออกหลักทรัพย์ควร จัดให้มีกลไกหรือมาตรการที่เหมาะสมเพื่อให้มั่นใจว่าหลักทรัพย์โทเคนถูกสร้างและจัดสรรในจำนวนที่ถูกต้อง และส่งมอบ

ให้แก่ผู้ลงทุนที่มีสิทธิได้รับจัดสรร รวมถึงจัดเก็บข้อมูลหรือหลักฐานที่เกี่ยวข้องเพื่อให้สามารถตรวจสอบย้อนหลังได้

แนวทางปฏิบัติ : ผู้ออกหลักทรัพย์ควรมีกลไกหรือมาตรการในการสร้าง จัดสรร และส่งมอบหลักทรัพย์โทเคน อย่างน้อยดังต่อไปนี้

(1) **การสร้างและจัดสรรหลักทรัพย์โทเคน :** ผู้ออกหลักทรัพย์ควรดำเนินการสร้าง (mint) และจัดสรรหลักทรัพย์โทเคนให้สอดคล้องกับจำนวนและประเภทของหลักทรัพย์ที่ผู้ลงทุนมีสิทธิได้รับจัดสรรตามผลการเสนอขาย โดยต้องมีกระบวนการหรือกลไกในการตรวจสอบความถูกต้องของการสร้างและการจัดสรรหลักทรัพย์โทเคน เพื่อให้เป็นไปตามจำนวนและสิทธิที่ผู้ลงทุนแต่ละรายได้รับจัดสรร

(2) **การส่งมอบหลักทรัพย์โทเคน :** ผู้ออกหลักทรัพย์ควรดำเนินการส่งมอบหลักทรัพย์โทเคนให้แก่ผู้ลงทุนที่ได้รับจัดสรร หรือผู้ให้บริการตัวกลางที่ผู้ลงทุนใช้บริการเพื่อการถือครองหลักทรัพย์โทเคน โดยควรมีกระบวนการหรือกลไกในการตรวจสอบและยืนยันความถูกต้องของผู้รับหลักทรัพย์โทเคนก่อนดำเนินการส่งมอบ เพื่อให้มั่นใจว่าหลักทรัพย์โทเคนถูกส่งมอบให้แก่ผู้ลงทุนที่มีสิทธิได้รับจัดสรรตามผลการเสนอขายอย่างถูกต้อง

ทั้งนี้ การส่งมอบอาจดำเนินการโดยอัตโนมัติผ่าน Smart Contract หรือดำเนินการตามกระบวนการอื่นที่เหมาะสมก็ได้ โดยไม่ว่าจะใช้วิธีการใด การส่งมอบควรดำเนินการไปยัง Wallet หรือบัญชีที่สามารถระบุได้ว่าเป็นของผู้ลงทุนที่ได้รับจัดสรร หรืออยู่ภายใต้การให้บริการของผู้ให้บริการตัวกลางที่ผู้ลงทุนดังกล่าวใช้บริการ และควรสามารถตรวจสอบย้อนหลังได้

(3) **การตรวจสอบความถูกต้องของข้อมูลโดยผู้ถือหลักทรัพย์โทเคน :** ผู้ออกหลักทรัพย์ควรจัดให้ผู้ลงทุนสามารถตรวจสอบข้อมูลเกี่ยวกับหลักทรัพย์โทเคนที่ได้รับจัดสรรและส่งมอบแก่ตนได้ตามความเหมาะสม เพื่อให้ผู้ลงทุนมั่นใจว่าการจัดสรรและการส่งมอบเป็นไปตามสิทธิที่ได้รับตามผลการเสนอขาย

3.3 การออกแบบเทคโนโลยีเพื่อรองรับผลทางกฎหมายของหลักทรัพย์โทเคน (Technology Design Supporting the Legal Characteristics of Tokenized Securities)

การออกหลักทรัพย์ในรูปแบบโทเคนต้องอาศัยระบบและกลไกทางเทคโนโลยีในการรองรับการดำเนินการที่เกี่ยวข้องกับหลักทรัพย์ ดังนั้นการออกแบบเทคโนโลยีควรสามารถรองรับผลทางกฎหมาย สิทธิ หน้าที่ และผลทางกฎหมายของหลักทรัพย์ได้อย่างถูกต้องตลอดอายุของหลักทรัพย์โทเคน

ผู้ออกหลักทรัพย์ควรเลือกใช้และออกแบบเทคโนโลยีที่เหมาะสม โดยอาจใช้บล็อกเชน / DLT สัญญาอัจฉริยะ (Smart Contract) หรือกลไกทางเทคโนโลยีอื่น เพื่อรองรับการดำเนินการที่เกี่ยวข้องกับหลักทรัพย์โทเคน เช่น การระบุหรือพิสูจน์สิทธิของผู้ถือหลักทรัพย์ การโอน การใช้สิทธิ การจัดทำทะเบียนหลักทรัพย์ และการดำเนินการอื่นที่เกี่ยวข้อง โดยคำนึงถึงความถูกต้อง ความน่าเชื่อถือ และความสามารถในการตรวจสอบข้อมูลตามกฎหมาย

3.3.1 การเลือกใช้เทคโนโลยี (Technology Selection)

ผู้ออกหลักทรัพย์ควรเลือกใช้เทคโนโลยีที่มีความเหมาะสมกับลักษณะของหลักทรัพย์โทเคนและรูปแบบการดำเนินการที่เกี่ยวข้อง โดยคำนึงถึงความสามารถของเทคโนโลยีในการรองรับการบันทึกข้อมูล การดำเนินการ และการบริหารจัดการหลักทรัพย์โทเคนตลอดอายุของหลักทรัพย์ รวมถึงการจัดทำหรือเชื่อมโยงกับระบบทะเบียนหลักทรัพย์ การใช้สิทธิของผู้ถือหลักทรัพย์ และการตรวจสอบข้อมูลที่เกี่ยวข้องตามกฎหมาย

แนวทางปฏิบัติ : ผู้ออกหลักทรัพย์ควรเลือกใช้และออกแบบเทคโนโลยีให้สามารถรองรับลักษณะและการดำเนินการที่เกี่ยวข้อง โดยมีรายละเอียดอย่างน้อย ดังต่อไปนี้

(1) การรองรับผลทางกฎหมายของหลักทรัพย์ (Support for Legal Characteristics) : ผู้ออกหลักทรัพย์ควรเลือกใช้บล็อกเชน / DLT ที่เหมาะสม หรือเทคโนโลยีหรือกลไกอื่นที่ให้ผลเทียบเท่า เพื่อให้สามารถรองรับการบันทึกข้อมูลและการดำเนินการที่เกี่ยวข้องกับหลักทรัพย์โทเคนตลอดอายุของหลักทรัพย์ รวมถึงการระบุและพิสูจน์สิทธิของผู้ถือหลักทรัพย์ การโอน การใช้สิทธิ และการดำเนินการอื่นที่เกี่ยวข้องตามกฎหมาย ทั้งนี้ เทคโนโลยีที่เลือกใช้ควรมีคุณลักษณะหรือกลไกที่เหมาะสมเพื่อรองรับอย่างน้อยในเรื่องต่อไปนี้

(ก) การควบคุมโดยผู้มีสิทธิ (Control) เพื่อให้การควบคุมและการดำเนินการเกี่ยวกับหลักทรัพย์โทเคนเป็นไปโดยผู้ถือหลักทรัพย์หรือบุคคลอื่นที่มีสิทธิหรืออำนาจดำเนินการตามกฎหมาย ข้อกำหนดที่เกี่ยวข้อง หรือรูปแบบการถือครองที่กำหนด และเพื่อป้องกันมิให้บุคคลอื่นที่ไม่มีสิทธิหรืออำนาจดำเนินการโดยไม่ได้รับอนุญาต

(ข) ความถูกต้องครบถ้วนของข้อมูล (Integrity) เพื่อให้ข้อมูลและรายการที่เกี่ยวข้องกับหลักทรัพย์โทเคนมีความถูกต้องครบถ้วนและสอดคล้องกัน รวมถึงมีมาตรการหรือกลไกที่เหมาะสม

เพื่อป้องกันการแก้ไข เปลี่ยนแปลง หรือดำเนินการกับข้อมูลโดยไม่ได้รับอนุญาต

(ค) ความโปร่งใส (Transparency) เพื่อให้ข้อมูลและการดำเนินการที่เกี่ยวข้องกับหลักทรัพย์โทเคนมีความชัดเจน และสามารถเปิดเผยหรือเข้าถึงได้อย่างเหมาะสม โดยคำนึงถึงลักษณะของข้อมูล สิทธิในการเข้าถึง และข้อกำหนดเกี่ยวกับการเปิดเผยข้อมูลต่อสาธารณะที่เกี่ยวข้อง

(ง) ความสามารถในการตรวจสอบ (Verifiability) เพื่อให้ข้อมูลและรายการที่เกี่ยวข้องกับหลักทรัพย์โทเคนสามารถตรวจสอบและพิสูจน์ความถูกต้องได้ รวมถึงสามารถติดตามการดำเนินการหรือการเปลี่ยนแปลงที่มีผลต่อสิทธิของผู้ถือหลักทรัพย์ได้ตามความเหมาะสม

(2) การรองรับการจัดทำทะเบียนหลักทรัพย์ (Support for Securities Register) : ผู้ออกหลักทรัพย์ควรเลือกใช้บล็อกเชน / DLT หรือเทคโนโลยีหรือกลไกอื่นที่เหมาะสม ให้สามารถรองรับการจัดทำทะเบียนหลักทรัพย์หรือเชื่อมโยงกับระบบทะเบียนหลักทรัพย์ตามที่กฎหมายหรือหลักเกณฑ์ที่เกี่ยวข้องกำหนด ทั้งนี้ ในกรณีที่มีการใช้มากกว่าหนึ่งระบบ ควรมีการกำหนดบทบาทของแต่ละระบบและกลไกในการเชื่อมโยงข้อมูลระหว่างกันอย่างชัดเจน ทั้งนี้ การออกแบบระบบควรคำนึงถึงการบันทึกและปรับปรุงข้อมูลทะเบียนหลักทรัพย์ การกำหนดระบบหรือข้อมูลที่ใช้เป็นข้อมูลอ้างอิงสำหรับทะเบียนหลักทรัพย์ และการเชื่อมโยงข้อมูลระหว่างระบบ โดยมีแนวทางดังต่อไปนี้

(ก) การบันทึกและปรับปรุงข้อมูลทะเบียนหลักทรัพย์ ระบบควรรองรับการบันทึกและปรับปรุงข้อมูลทะเบียนหลักทรัพย์ที่เกี่ยวกับผู้ถือหลักทรัพย์และการถือครองหลักทรัพย์ รวมถึงการเปลี่ยนแปลงข้อมูลอันเกิดจากการโอน การใช้สิทธิ หรือการดำเนินการอื่นที่มีผลต่อสิทธิหรือสถานะของหลักทรัพย์โทเคน เพื่อให้ข้อมูลทะเบียนสะท้อนสถานะการถือครองหลักทรัพย์ที่เกี่ยวข้องได้อย่างเหมาะสม

(ข) การกำหนดระบบทะเบียนหลักทรัพย์ที่ใช้เป็นหลัก ในกรณีที่มีการบันทึกข้อมูลเกี่ยวกับผู้ถือหลักทรัพย์หรือการถือครองหลักทรัพย์ไว้ในมากกว่าหนึ่งระบบ ผู้ออกหลักทรัพย์ควรกำหนด

และระบุให้ชัดเจนว่าระบบใดเป็นระบบทะเบียนหลักทรัพย์ที่ใช้เป็นแหล่งข้อมูลอ้างอิงหลัก (Authoritative Source) ในการระบุสถานะและสิทธิของผู้ถือหลักทรัพย์ตามกฎหมาย รวมถึงกำหนดบทบาทของข้อมูลที่บันทึกอยู่ในแต่ละระบบให้ชัดเจน

ทั้งนี้ ผู้ออกหลักทรัพย์ควรจัดให้มีกลไกในการเชื่อมโยงและอ้างอิงข้อมูลระหว่างระบบ เพื่อให้สามารถระบุความสัมพันธ์ของข้อมูลที่เกี่ยวข้องกับหลักทรัพย์และข้อมูลทะเบียนหลักทรัพย์ในแต่ละระบบได้อย่างชัดเจน โดยอาจกำหนดข้อมูลหรือรหัสอ้างอิงที่ใช้ร่วมกันระหว่างระบบ เช่น Unique Identifier, Reference Identifier หรือข้อมูลอ้างอิงอื่นที่มีลักษณะเฉพาะ รวมทั้งควรมีกลไกที่เหมาะสมในการตรวจสอบและรักษาความสอดคล้องของข้อมูลระหว่างระบบการกำหนดระบบทะเบียนหลักทรัพย์ที่ใช้เป็นหลักและการเชื่อมโยงข้อมูลระหว่างระบบควรมีความชัดเจนและต่อเนื่องตลอดอายุของหลักทรัพย์ และในกรณีที่มีการเปลี่ยนแปลงระบบทะเบียนหลักทรัพย์ ควรมีกระบวนการที่เหมาะสมเพื่อไม่ให้กระทบต่อความต่อเนื่องและความสามารถในการอ้างอิงสถานะและสิทธิของผู้ถือหลักทรัพย์

3.3.2 การออกแบบสัญญาอัจฉริยะ (Smart Contract Design)

สัญญาอัจฉริยะ (Smart Contract) หรือกลไกทางเทคโนโลยีอื่นที่ให้ผลเทียบเท่าเป็นองค์ประกอบสำคัญในการรองรับการดำเนินการเกี่ยวกับหลักทรัพย์โทเคนบนบล็อกเชน / DLT ดังนั้น ผู้ออกหลักทรัพย์ควรออกแบบสัญญาอัจฉริยะหรือกลไกทางเทคโนโลยีดังกล่าว ให้สามารถรองรับสิทธิ หน้าที่ และผลทางกฎหมายของหลักทรัพย์ รวมถึงการดำเนินการตามข้อกำหนดและเงื่อนไขของหลักทรัพย์ได้อย่างถูกต้อง ตลอดอายุของหลักทรัพย์

แนวทางปฏิบัติ : ผู้ออกหลักทรัพย์ควรออกแบบสัญญาอัจฉริยะ (Smart Contract) หรือกลไกทางเทคโนโลยีอื่นที่ใช้ในการดำเนินการเกี่ยวกับหลักทรัพย์โทเคน ให้สอดคล้องกับสิทธิ หน้าที่ ข้อจำกัด และเงื่อนไขของหลักทรัพย์ตามกฎหมาย รวมถึงข้อกำหนดและเงื่อนไขของการออกหลักทรัพย์โทเคน (Tokenization Terms) โดยควรพิจารณาและกำหนดให้ชัดเจนว่า **สิทธิ หน้าที่ ข้อจำกัดหรือเงื่อนไขใดที่ต้องรองรับหรือดำเนินการผ่านระบบเทคโนโลยี และออกแบบกลไกให้การดำเนินการและผลของการดำเนินการเป็นไปตามข้อกำหนดดังกล่าว**

ในกรณีที่สิทธิ หน้าที่ ข้อจำกัด หรือเงื่อนไขบางประการไม่สามารถหรือไม่จำเป็นต้องดำเนินการผ่านสัญญาอัจฉริยะหรือกลไกทางเทคโนโลยีดังกล่าว ผู้ออกหลักทรัพย์ควรกำหนดวิธีการหรือกลไกอื่นที่เหมาะสมในการรองรับการดำเนินการดังกล่าว

ทั้งนี้ รายละเอียดเกี่ยวกับฟังก์ชันการทำงานของโทเคน (Token Functional Requirements) และคุณลักษณะทางเทคนิคของสัญญาอัจฉริยะ (Smart Contract) หรือกลไกทางเทคโนโลยีอื่นที่ใช้ในการดำเนินการเกี่ยวกับหลักทรัพย์โทเคน ให้เป็นไปตามมาตรฐานด้านโทเคน (Token Standard)

3.4 การเปิดเผยข้อมูลเกี่ยวกับการออกหลักทรัพย์โทเคน (Disclosure relating to Securities Token)

การออกและเสนอขายหลักทรัพย์ในรูปแบบโทเคนยังคงต้องเป็นไปตามหลักเกณฑ์เกี่ยวกับการเปิดเผยข้อมูลที่ใช้บังคับกับหลักทรัพย์แต่ละประเภท รวมถึงการจัดทำและเปิดเผยแบบแสดงรายการข้อมูล หนังสือชี้ชวน หรือเอกสารอื่นตามที่กำหนด

อย่างไรก็ดี การนำหลักทรัพย์มาออกและบริหารจัดการในรูปแบบโทเคนอาจมีลักษณะ กลไก หรือเงื่อนไขเพิ่มเติมที่เกิดจากการใช้เทคโนโลยี ซึ่งอาจมีผลต่อสิทธิ การถือครอง การโอน การใช้สิทธิ หรือผลทางกฎหมายของหลักทรัพย์ ดังนั้น ผู้ออกหลักทรัพย์ควรเปิดเผยข้อมูลที่เกี่ยวข้องกับลักษณะดังกล่าวให้ผู้ลงทุนและผู้ถือหลักทรัพย์สามารถเข้าใจลักษณะและผลของการถือครองหลักทรัพย์ในรูปแบบโทเคนได้อย่างเหมาะสม

การเปิดเผยข้อมูลตามมาตรฐานในข้อนี้ มุ่งเน้นข้อมูลที่มีลักษณะเฉพาะจากการออกหลักทรัพย์โทเคน และไม่เป็นการทดแทนหรือจำกัดหน้าที่ในการเปิดเผยข้อมูลตามหลักเกณฑ์ที่ใช้บังคับกับการออกและเสนอขายหลักทรัพย์แต่ละประเภท ทั้งนี้ ข้อมูลที่เปิดเผยควรมีความเหมาะสมกับลักษณะของหลักทรัพย์และมีนัยสำคัญต่อสิทธิ หน้าที่ หรือผลทางกฎหมายของผู้ถือหลักทรัพย์โทเคน

3.4.1 การเปิดเผยข้อมูลเกี่ยวกับลักษณะของหลักทรัพย์โทเคน (Product-specific disclosures)

ผู้ออกหลักทรัพย์ควรเปิดเผยข้อมูลเกี่ยวกับลักษณะและเงื่อนไขที่มีลักษณะเฉพาะจากการออกหลักทรัพย์ในรูปแบบโทเคน เพื่อให้ผู้ลงทุนสามารถเข้าใจความสัมพันธ์ระหว่างหลักทรัพย์กับโทเคน รวมถึงลักษณะของการถือครองและการใช้สิทธิในหลักทรัพย์ผ่านโทเคนได้อย่างเหมาะสม

แนวทางปฏิบัติ : ผู้ออกหลักทรัพย์ควรเปิดเผยข้อมูลที่สำคัญเกี่ยวกับลักษณะของหลักทรัพย์ที่ออกในรูปแบบโทเคน โดยครอบคลุมประเด็นอย่างน้อยดังต่อไปนี้

(1) ลักษณะและประเภทของหลักทรัพย์โทเคน
(2) สิทธิ หน้าที่ และผลประโยชน์ของผู้ถือหลักทรัพย์โทเคน ทั้งนี้ ให้รวมถึงลักษณะเฉพาะหรือเงื่อนไขที่เกิดจากการถือครองหลักทรัพย์ในรูปแบบโทเคน
(3) ความเชื่อมโยงระหว่างหลักทรัพย์กับโทเคน รวมถึงข้อมูลที่ใช้ระบุหรืออ้างอิงความเชื่อมโยงดังกล่าว โดยให้เป็นไปตามหลักเกณฑ์ในข้อ 3.2.2

(4) จำนวนหรืออัตราส่วนระหว่างหลักทรัพย์และหลักทรัพย์โทเคนที่ใช้แสดงสิทธิในหลักทรัพย์นั้น (ถ้ามี)

(5) ลักษณะของการถือครองและการบันทึกข้อมูลเกี่ยวกับผู้ถือหลักทรัพย์ รวมถึงข้อมูลเกี่ยวกับทะเบียนหลักทรัพย์ที่มีนัยสำคัญต่อการระบุสถานะและสิทธิของผู้ถือหลักทรัพย์ ตามที่กำหนดไว้ในข้อ 3.3.1

(6) ข้อจำกัดหรือเงื่อนไขที่มีนัยสำคัญเกี่ยวกับการถือครองหรือการโอนหลักทรัพย์โทเคน (ถ้ามี)

(7) วิธีการเข้าถึง Tokenization Terms และเอกสารหรือข้อมูลอื่นที่เกี่ยวข้องกับการออกหลักทรัพย์ในรูปแบบโทเคน โดยให้เป็นไปตามหลักในข้อ 3.2.3

3.4.2 การเปิดเผยข้อมูลเกี่ยวกับการดำเนินงานที่เกี่ยวข้องกับหลักทรัพย์โทเคน (Operational-specific disclosures)

ผู้ออกหลักทรัพย์ควรเปิดเผยข้อมูลเกี่ยวกับกระบวนการและกลไกในการดำเนินงานที่เกี่ยวข้องกับหลักทรัพย์โทเคน ซึ่งมีนัยสำคัญต่อการถือครอง การโอน การใช้สิทธิ หรือการได้รับผลประโยชน์จากหลักทรัพย์ เพื่อให้ผู้ลงทุนสามารถเข้าใจวิธีการและเงื่อนไขในการดำเนินการที่เกี่ยวข้องกับหลักทรัพย์โทเคนได้อย่างเหมาะสม

แนวทางปฏิบัติ : ผู้ออกหลักทรัพย์ควรเปิดเผยข้อมูลเกี่ยวกับกระบวนการและกลไกในการดำเนินงานที่มีนัยสำคัญอย่างน้อยในเรื่องดังต่อไปนี้

(1) กระบวนการจองซื้อ การจัดสรร และการส่งมอบหลักทรัพย์โทเคน : ควรเปิดเผยข้อมูลเกี่ยวกับวิธีการและกระบวนการที่ผู้ลงทุนต้องดำเนินการในการจองซื้อหลักทรัพย์ การจัดสรรหลักทรัพย์โทเคน และวิธีการหรือกลไกในการส่งมอบหลักทรัพย์โทเคนให้แก่ผู้ลงทุน รวมถึงเงื่อนไขหรือข้อกำหนดที่มีนัยสำคัญต่อกระบวนการดังกล่าว ทั้งนี้ ในส่วนที่เกี่ยวข้องกับการสร้าง การจัดสรร และการส่งมอบหลักทรัพย์โทเคน ให้เป็นไปตามหลักการในข้อ 3.2.4

(2) การถือครองและการเก็บรักษาหลักทรัพย์โทเคน : ควรเปิดเผยข้อมูลเกี่ยวกับรูปแบบหรือวิธีการในการถือครองและเก็บรักษาหลักทรัพย์โทเคนที่ผู้ลงทุนสามารถใช้ได้ รวมถึงการใช้กระเป๋าอิเล็กทรอนิกส์ (Wallet) และการใช้บริการหรือผู้ให้บริการที่เกี่ยวข้องกับการถือครองหรือการเก็บรักษาหลักทรัพย์โทเคน ตลอดจนบทบาทและความรับผิดชอบของผู้ที่เกี่ยวข้องเท่าที่มีนัยสำคัญต่อผู้ถือหลักทรัพย์ ทั้งนี้ ในกรณีที่มีการถือครองหลักทรัพย์โทเคนผ่านผู้ประกอบธุรกิจตัวกลาง ให้เปิดเผยข้อมูลที่เกี่ยวข้องตามหลักการในข้อ 3.1.3

(3) **วิธีการและกระบวนการโอนหลักทรัพย์โทเคน :** ควรเปิดเผยข้อมูลเกี่ยวกับวิธีการ กระบวนการ และเงื่อนไขสำคัญในการโอนหลักทรัพย์โทเคน รวมถึงข้อกำหนดหรือการดำเนินการที่ผู้โอนหรือผู้รับโอนจำเป็นต้องปฏิบัติเพื่อให้การโอนสามารถดำเนินการได้อย่างถูกต้องและมีผลตามกฎหมาย ทั้งนี้ ให้เป็นไปตามหลักการที่เกี่ยวข้องในข้อ 3.5.1

(4) **การจ่ายหรือการส่งมอบผลประโยชน์ตอบแทนแก่ผู้ถือหลักทรัพย์ :** ควรเปิดเผยข้อมูลเกี่ยวกับวิธีการ กระบวนการ และช่องทางในการจ่ายหรือส่งมอบผลประโยชน์ตอบแทนแก่ผู้ถือหลักทรัพย์โทเคน รวมถึงเงื่อนไขหรือการดำเนินการที่ผู้ถือหลักทรัพย์จำเป็นต้องทราบหรือปฏิบัติ เพื่อให้ได้รับผลประโยชน์ตอบแทนดังกล่าวตามสิทธิในหลักทรัพย์ โดยให้เป็นไปตามหลักการที่เกี่ยวข้องในข้อ 3.5.2 ทั้งนี้ ในกรณีที่การดำเนินการตามสิทธิของผู้ถือหลักทรัพย์หรือ Corporate Actions มีกระบวนการหรือกลไกที่เกี่ยวข้องกับหลักทรัพย์โทเคนโดยเฉพาะ และมีนัยสำคัญต่อผู้ถือหลักทรัพย์ ควรเปิดเผยข้อมูลเกี่ยวกับกระบวนการหรือกลไกดังกล่าวเพิ่มเติมตามความเหมาะสม

(5) **การดำเนินการเมื่อเกิดเหตุการณ์หรือสถานการณ์พิเศษ :** ควรเปิดเผยข้อมูลเกี่ยวกับกระบวนการและมาตรการที่เกี่ยวข้องในกรณีเกิดเหตุการณ์หรือสถานการณ์พิเศษที่อาจส่งผลต่อการถือครอง สิทธิ หรือผลทางกฎหมายของหลักทรัพย์โทเคน รวมถึงการดำเนินการที่ผู้ถือหลักทรัพย์จำเป็นต้องทราบหรือปฏิบัติ เช่น กรณีสูญเสียหรือไม่สามารถเข้าถึงหลักทรัพย์โทเคน หรือกรณีที่มีการออกหลักทรัพย์โทเคนทดแทน ทั้งนี้ ให้เป็นไปตามหลักการที่เกี่ยวข้องในข้อ 3.6

3.4.3 การเปิดเผยข้อมูลเกี่ยวกับเทคโนโลยีที่ใช้ในการให้บริการหลักทรัพย์โทเคน (Technology-specific disclosures)

หลักทรัพย์โทเคนเป็นการนำเทคโนโลยีบล็อกเชน / DLT เข้ามาใช้ในกระบวนการออก การถือครอง การโอน และการดำเนินการอื่นที่เกี่ยวข้องกับหลักทรัพย์ ซึ่งเทคโนโลยีดังกล่าวอาจมีบทบาทต่อการใช้สิทธิและการดำเนินการที่เกี่ยวข้องกับหลักทรัพย์โทเคน ผู้ออกหลักทรัพย์จึงควรเปิดเผยข้อมูลเกี่ยวกับเทคโนโลยีที่ใช้ ในส่วนที่มีนัยสำคัญต่อผู้ถือหลักทรัพย์ เพื่อให้ผู้ลงทุนสามารถเข้าใจบทบาทและลักษณะของเทคโนโลยีดังกล่าวได้อย่างเหมาะสม

แนวทางปฏิบัติ : ผู้ออกหลักทรัพย์ควรเปิดเผยข้อมูลเกี่ยวกับเทคโนโลยีที่ใช้ในการให้บริการหลักทรัพย์โทเคนอย่างน้อยในเรื่องดังต่อไปนี้

(1) **บล็อกเชนหรือ Distributed Ledger Technology (DLT) :** ควรเปิดเผยข้อมูลเกี่ยวกับบล็อกเชนหรือ DLT ที่ใช้ในการออก การบันทึก การถือครอง การโอน หรือการดำเนินการอื่นที่เกี่ยวข้องกับหลักทรัพย์โทเคน รวมถึงข้อมูลที่ช่วยให้ผู้ลงทุนสามารถเข้าใจลักษณะและบทบาทของเครือข่ายหรือระบบดังกล่าวที่มีนัยสำคัญต่อการให้บริการหลักทรัพย์โทเคน

(2) **สัญญาอัจฉริยะ (Smart Contract) :** ควรเปิดเผยข้อมูลเกี่ยวกับสัญญาอัจฉริยะที่ใช้ในการให้บริการหลักทรัพย์โทเคน รวมถึงลักษณะและหน้าที่สำคัญของสัญญาอัจฉริยะดังกล่าวที่มีนัยสำคัญต่อผู้ถือหลักทรัพย์ เช่น การออกหรือการทำลายหลักทรัพย์โทเคน การควบคุมหรือจำกัดการโอน หรือการดำเนินการโดยอัตโนมัติตามเงื่อนไขที่กำหนด เป็นต้น

(3) **ความสมบูรณ์ของธุรกรรมในระบบ (Transaction Finality) :** ควรเปิดเผยข้อมูลเกี่ยวกับกลไกหรือกระบวนการที่ใช้ในการยืนยันความสมบูรณ์ของธุรกรรมบนบล็อกเชนหรือ DLT รวมถึงช่วงเวลาหรือเงื่อนไขที่ธุรกรรมถือว่าได้รับการยืนยันอย่างสมบูรณ์และไม่สามารถเปลี่ยนแปลงหรือย้อนกลับได้ เช่น ในกรณีที่มีการซื้อขายหรือโอนหลักทรัพย์โทเคน ควรเปิดเผยให้ผู้ลงทุนทราบว่า ณ จุดใดหรือเมื่อเกิดเหตุการณ์ใด ธุรกรรมดังกล่าวจะถือว่าเสร็จสิ้นสมบูรณ์แล้วบนบล็อกเชนหรือ DLT

(4) **อำนาจในการควบคุมหรือเปลี่ยนแปลงระบบ :** ควรเปิดเผยข้อมูลเกี่ยวกับบุคคลหรือกลไกที่มีอำนาจในการควบคุม แก้ไข ระงับ หรือเปลี่ยนแปลงการทำงานของสัญญาอัจฉริยะ (Smart Contract) หรือองค์ประกอบทางเทคโนโลยีที่เกี่ยวข้องกับหลักทรัพย์โทเคน รวมถึงลักษณะและขอบเขตของอำนาจดังกล่าวที่อาจมีผลต่อผู้ถือหลักทรัพย์ เช่น อำนาจในการแก้ไขหรือปรับปรุงสัญญาอัจฉริยะ หรือการระงับการทำงานบางส่วน เป็นต้น

3.4.4 การเปิดเผยความเสี่ยงเกี่ยวกับหลักทรัพย์โทเคน (Risk-specific disclosures)

การออกและให้บริการหลักทรัพย์โทเคนอาจมีความเสี่ยงที่เกี่ยวข้องกับลักษณะของหลักทรัพย์ กระบวนการและการให้บริการ รวมถึงการใช้เทคโนโลยีบล็อกเชนหรือ DLT ซึ่งอาจแตกต่างจากหรือเพิ่มเติมจากความเสี่ยงของหลักทรัพย์ในรูปแบบทั่วไป ผู้ออกหลักทรัพย์จึงควรเปิดเผยข้อมูลเกี่ยวกับความเสี่ยงดังกล่าวที่อาจมีนัยสำคัญต่อผู้ลงทุน เพื่อให้ผู้ลงทุนสามารถเข้าใจและประเมินความเสี่ยงที่เกี่ยวข้องกับการลงทุนในหลักทรัพย์โทเคนได้อย่างเหมาะสม

แนวทางปฏิบัติ : ผู้ออกหลักทรัพย์ควรเปิดเผยข้อมูลเกี่ยวกับความเสี่ยงที่เกี่ยวข้องกับหลักทรัพย์โทเคน โดยอย่างน้อยในประเด็นดังต่อไปนี้

(1) **ความเสี่ยงที่เกี่ยวข้องกับสัญญาอัจฉริยะ (Smart Contract) :** ควรเปิดเผยความเสี่ยงที่อาจเกิดจากข้อผิดพลาด ช่องโหว่ หรือการทำงานของสัญญาอัจฉริยะที่ไม่เป็นไปตามที่กำหนด ซึ่งอาจส่งผลต่อการออก การโอน การใช้สิทธิ หรือการดำเนินการอื่นที่เกี่ยวข้องกับหลักทรัพย์โทเคน รวมถึงผลกระทบที่อาจเกิดขึ้นต่อผู้ถือหลักทรัพย์ ทั้งนี้ ผู้ออกหลักทรัพย์ควรเปิดเผยข้อมูลเกี่ยวกับมาตรการหรือกลไกสำคัญที่ใช้ในการลดหรือจัดการความเสี่ยงดังกล่าวในระดับที่เหมาะสม

(2) **ความเสี่ยงที่เกี่ยวข้องกับบล็อกเชนหรือ DLT :** ควรเปิดเผยความเสี่ยงที่เกิดจากการพึ่งพาบล็อกเชนหรือ DLT ในการให้บริการหลักทรัพย์โทเคน รวมถึงผลกระทบที่อาจเกิดขึ้นหากเครือข่ายหรือระบบดังกล่าวเกิดการหยุดชะงักขัดข้อง หรือไม่สามารถดำเนินการได้ตามปกติ เช่น การโอนหลักทรัพย์โทเคนไม่สามารถบันทึกหรือยืนยันได้ ความล่าช้าหรือไม่สามารถดำเนินการออกหรือโอนหลักทรัพย์โทเคนได้ตามปกติ หรือการที่ผู้ถือหลักทรัพย์ไม่สามารถดำเนินการใช้สิทธิผ่านระบบที่เกี่ยวข้องกับหลักทรัพย์โทเคนได้ เป็นต้น ทั้งนี้ ผู้ออกหลักทรัพย์ควรเปิดเผยข้อมูลเกี่ยวกับมาตรการหรือกลไกสำคัญที่ใช้ในการลดหรือจัดการความเสี่ยงดังกล่าวในระดับที่เหมาะสม

(3) **ความเสี่ยงที่เกี่ยวข้องกับการถือครองและการเข้าถึงหลักทรัพย์โทเคน :** ควรเปิดเผยความเสี่ยงที่เกี่ยวข้องกับการถือครองหรือการเข้าถึงหลักทรัพย์โทเคน โดยเฉพาะในกรณีที่ผู้ถือหลักทรัพย์เป็นผู้ดูแลหรือควบคุม Private Key หรือข้อมูลที่ใช้ในการเข้าถึงหลักทรัพย์ด้วยตนเอง เช่น ความเสี่ยงจากการสูญหาย การเปิดเผย หรือการถูกเข้าถึงโดยมิชอบ ซึ่งอาจส่งผลให้ผู้ถือหลักทรัพย์สูญเสียการควบคุมหรือไม่สามารถเข้าถึงหลักทรัพย์โทเคนของตนเองได้

(4) **ความเสี่ยงจากการพึ่งพาผู้ให้บริการภายนอก :** ควรเปิดเผยความเสี่ยงที่เกิดจากการพึ่งพาผู้ให้บริการภายนอกที่มีบทบาทสำคัญต่อการออก การถือครอง การโอน หรือการดำเนินการอื่นที่เกี่ยวข้องกับหลักทรัพย์โทเคน รวมถึงผลกระทบที่อาจเกิดขึ้นหากผู้ให้บริการดังกล่าวไม่สามารถให้บริการได้ตามปกติ เช่น ผู้รับฝากทรัพย์สิน ผู้ให้บริการ Wallet ผู้ให้บริการโครงสร้างพื้นฐานที่เกี่ยวข้องกับบล็อกเชนหรือ DLT หรือผู้ให้บริการระบบอื่นที่เกี่ยวข้องกับหลักทรัพย์โทเคน เป็นต้น ทั้งนี้ ผู้ออกหลักทรัพย์ควรเปิดเผยข้อมูลเกี่ยวกับมาตรการหรือกลไกสำคัญที่ใช้ในการลดหรือจัดการความเสี่ยงดังกล่าวในระดับที่เหมาะสม

(5) **ความเสี่ยงจากการเปลี่ยนแปลงหรือเปลี่ยนผ่านระบบและโครงสร้างพื้นฐาน :** ควรเปิดเผยความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากการเปลี่ยนแปลงหรือเปลี่ยนผ่านระบบหรือโครงสร้างพื้นฐานที่ใช้ในการให้บริการหลักทรัพย์โทเคน เช่น การย้ายหลักทรัพย์โทเคนจากบล็อกเชนหรือ DLT ระบบเดิมไปยังอีกระบบใหม่ การเปลี่ยนหรือปรับปรุงสัญญาอัจฉริยะ (Smart Contract) หรือการเปลี่ยนแปลงองค์ประกอบสำคัญของระบบที่เกี่ยวข้องกับการถือครองหรือการดำเนินการเกี่ยวกับหลักทรัพย์โทเคน รวมทั้งมาตรการหรือกลไกสำคัญที่ใช้ในการรองรับหรือจัดการความเสี่ยงดังกล่าว ในระดับที่เหมาะสม

3.5 การดำเนินการภายหลังการออกหลักทรัพย์โทเคน (Post-Issuance Operations of Tokenized Securities)

หลักทรัพย์โทเคนอาจมีการโอนระหว่างผู้ถือหลักทรัพย์ และอาจมีการดำเนินการที่เกี่ยวข้องกับสิทธิและผลประโยชน์ของผู้ถือหลักทรัพย์ตามลักษณะและเงื่อนไขของหลักทรัพย์ตลอดระยะเวลาที่หลักทรัพย์ยังมีผลใช้บังคับ

ผู้ออกหลักทรัพย์จึงควรมีกลไกหรือกระบวนการที่เหมาะสมเพื่อรองรับการดำเนินการดังกล่าวให้เป็นไปตามหลักเกณฑ์ที่เกี่ยวข้อง ข้อกำหนดของหลักทรัพย์และ Tokenization Terms รวมทั้งสามารถตรวจสอบการดำเนินการที่เกี่ยวข้องได้อย่างเหมาะสม

3.5.1 การโอนหลักทรัพย์โทเคน (Transfer of Tokenized Securities)

ผู้ออกหลักทรัพย์ควรมีกลไกในการบริหารจัดการที่เหมาะสม เพื่อรองรับการโอนและการรับโอนหลักทรัพย์โทเคนให้มีความถูกต้องตามเจตนาของผู้โอนและผู้รับโอน รวมถึงสามารถตรวจสอบคุณสมบัติของผู้รับโอนและบังคับใช้เงื่อนไขหรือข้อจำกัดในการโอนที่เกี่ยวข้องได้อย่างเหมาะสม

แนวทางปฏิบัติ : ผู้ออกหลักทรัพย์ควรกำหนดกลไกหรือกระบวนการที่เหมาะสมในการรองรับการโอนและการรับโอนหลักทรัพย์โทเคน โดยอย่างน้อยควรคำนึงถึงเรื่องดังต่อไปนี้

(1) **การตรวจสอบและยืนยันผู้รับโอน :** ผู้ออกหลักทรัพย์ควรมีกลไกหรือกระบวนการในการตรวจสอบและยืนยันตัวตนของผู้รับโอน รวมทั้งตรวจสอบคุณสมบัติหรือสิทธิในการถือครองหลักทรัพย์โทเคนตามเงื่อนไขที่กำหนดก่อนดำเนินการโอนหลักทรัพย์โทเคนให้แก่ผู้รับโอนในกรณีที่ผู้รับโอนใช้กระเป๋าอิเล็กทรอนิกส์ (Wallet) ที่ไม่ได้ให้บริการโดยผู้ออกหลักทรัพย์หรือผู้ประกอบธุรกิจตัวกลาง ผู้ออกหลักทรัพย์ควรมีกระบวนการที่เหมาะสมในการ

ตรวจสอบหรือยืนยันความเชื่อมโยงระหว่างผู้รับโอนกับ Wallet Address ที่จะใช้ในการรับและถือครองหลักทรัพย์โทเคน

ตัวอย่าง : ผู้ออกหลักทรัพย์อาจกำหนดให้ผู้ที่จะรับโอนหลักทรัพย์โทเคนต้องผ่านกระบวนการตรวจสอบและยืนยันตัวตน รวมทั้งตรวจสอบคุณสมบัติในการถือครองหลักทรัพย์โทเคนก่อน โดยเมื่อผ่านการตรวจสอบแล้ว อาจนำ Wallet Address ที่ผู้รับโอนใช้ถือครองหลักทรัพย์โทเคนเข้าสู่บัญชีรายชื่อที่ได้รับอนุญาต (Whitelist) เพื่อใช้ในการรับโอนหลักทรัพย์โทเคน ทั้งนี้ ในกรณีที่เป็น Private Wallet อาจกำหนดให้ผู้รับโอนพิสูจน์ว่าสามารถควบคุม Wallet Address ดังกล่าวได้ก่อนนำ Wallet Address เข้าสู่ Whitelist เช่น การให้ผู้รับโอนลงนามข้อความหรือดำเนินการจาก Wallet Address ดังกล่าว เพื่อพิสูจน์ว่าสามารถควบคุม Wallet Address ที่จะใช้รับและถือครองหลักทรัพย์โทเคนได้ เป็นต้น

(2) **การควบคุมและบังคับใช้เงื่อนไขในการโอน :** ผู้ออกหลักทรัพย์ควรมีกลไกหรือกระบวนการที่เหมาะสมในการตรวจสอบและบังคับใช้เงื่อนไขหรือข้อจำกัดในการโอนหลักทรัพย์โทเคน เพื่อให้การโอนเป็นไปตามเงื่อนไขที่กำหนดสำหรับหลักทรัพย์โทเคนแต่ละประเภท โดยกลไกหรือกระบวนการดังกล่าวควรสามารถป้องกันหรือไม่อนุญาตให้มีการโอนหลักทรัพย์โทเคนในกรณีที่การโอนไม่เป็นไปตามเงื่อนไขหรือข้อจำกัดที่กำหนด

ตัวอย่าง : ผู้ออกหลักทรัพย์อาจกำหนดเงื่อนไขหรือข้อจำกัดในการโอนผ่านสัญญาอัจฉริยะ (Smart Contract) หรือกลไกทางเทคนิคอื่น โดยให้มีการตรวจสอบเงื่อนไขที่กำหนดก่อนดำเนินการโอน เช่น ตรวจสอบว่า Wallet Address ของผู้รับโอนได้รับอนุญาตให้ถือครองหลักทรัพย์โทเคน หรือได้พ้นระยะเวลาห้ามโอนแล้วหรือไม่ ทั้งนี้ หากไม่เป็นไปตามเงื่อนไขที่กำหนด สัญญาอัจฉริยะหรือกลไกดังกล่าวอาจไม่อนุญาตให้ธุรกรรมการโอนดำเนินการ

(3) **การตรวจสอบย้อนหลังธุรกรรมการโอน :** ผู้ออกหลักทรัพย์ควรมีกลไกหรือกระบวนการที่เหมาะสมเพื่อให้สามารถตรวจสอบย้อนหลังธุรกรรมการโอนหลักทรัพย์โทเคนได้ โดยควรมีข้อมูลหรือหลักฐานที่เพียงพอเพื่อให้สามารถตรวจสอบรายละเอียดที่สำคัญของการโอน รวมถึงผู้ที่เกี่ยวข้องกับการโอนและการดำเนินการตามเงื่อนไขหรือข้อจำกัดที่เกี่ยวข้องได้

ตัวอย่าง : ผู้ออกหลักทรัพย์อาจจัดให้มีระบบหรือกลไกที่สามารถเชื่อมโยงข้อมูลธุรกรรมบน DLT หรือ Blockchain เช่น Transaction Hash[2], Block Number หรือข้อมูลที่ระบุ Wallet Address ของผู้โอนและผู้รับโอน เข้ากับข้อมูลหรือหลักฐานที่เกี่ยวข้องกับการตรวจสอบและอนุญาตการโอนที่จัดเก็บไว้ในระบบอื่น เพื่อให้สามารถตรวจสอบย้อนหลังได้ว่าธุรกรรมใดเกิดขึ้นระหว่าง Wallet Address ใด เมื่อใด และผู้รับโอนหรือธุรกรรมดังกล่าวได้ผ่านการตรวจสอบตามเงื่อนไขหรือข้อจำกัดที่กำหนดก่อนการโอนหรือไม่

3.5.2 การดำเนินการตามสิทธิของผู้ถือหลักทรัพย์ (Corporate Actions)

ผู้ออกหลักทรัพย์ควรมีกลไกหรือกระบวนการที่เหมาะสมเพื่อรองรับการดำเนินการตามสิทธิและผลประโยชน์ของผู้ถือหลักทรัพย์โทเคน รวมถึงการดำเนินการอื่นที่มีผลต่อสิทธิหรือสถานะของหลักทรัพย์โทเคนตามเงื่อนไขของหลักทรัพย์ เช่น การจ่ายดอกเบี้ย การจ่ายเงินปันผล การจ่ายผลประโยชน์ตอบแทนการไถ่ถอน การแปลงสภาพ หรือการเปลี่ยนแปลงจำนวนหน่วยของหลักทรัพย์โทเคน เป็นต้น เพื่อให้การดำเนินการดังกล่าวเป็นไปอย่างถูกต้อง สอดคล้องกับหลักเกณฑ์ข้อกำหนดของหลักทรัพย์ และ Tokenization Terms ที่เกี่ยวข้อง

แนวทางปฏิบัติ : ผู้ออกหลักทรัพย์ควรกำหนดกลไกหรือกระบวนการที่เหมาะสมสำหรับการดำเนินการตามสิทธิและผลประโยชน์ของผู้ถือหลักทรัพย์โทเคน โดยอย่างน้อยควรคำนึงถึงเรื่องดังต่อไปนี้

(1) การกำหนดและระบุผู้มีสิทธิ : ผู้ออกหลักทรัพย์ควรมีกลไกหรือกระบวนการที่เหมาะสมในการกำหนดและระบุผู้ถือหลักทรัพย์โทเคนที่มีสิทธิได้รับผลประโยชน์หรือเข้าร่วมในการดำเนินการตามสิทธิแต่ละประเภท โดยควรกำหนดช่วงเวลาหรือหลักเกณฑ์ที่ใช้ในการพิจารณาผู้มีสิทธิให้ชัดเจน และสามารถตรวจสอบข้อมูลผู้ถือหลักทรัพย์ที่ใช้เป็นฐานในการดำเนินการดังกล่าวได้

ตัวอย่าง : ผู้ออกหลักทรัพย์อาจกำหนดวันและเวลาที่ใช้เป็นเกณฑ์ในการระบุผู้มีสิทธิ (Record Date) และใช้ข้อมูลจากทะเบียนผู้ถือหลักทรัพย์โทเคน ณ วันและเวลาดังกล่าวในการพิจารณาผู้มีสิทธิ โดยในกรณีที่ข้อมูลการถือครองหลักทรัพย์โทเคนมีการบันทึกบน DLT หรือ Blockchain อาจใช้ข้อมูลที่เกี่ยวข้องกับการถือครอง ณ Block หรือเวลาที่กำหนดเป็นข้อมูลประกอบในการระบุผู้มีสิทธิ ทั้งนี้ ควรมีกลไกที่สามารถเชื่อมโยงข้อมูลการถือครอง

[2] Hash คือ ค่าที่คำนวณจากข้อมูลและมีความยาวคงที่ ใช้เปรียบเทียบเพื่อตรวจสอบว่าข้อมูลมีการเปลี่ยนแปลงหรือไม่

หลักทรัพย์โทเคนกับข้อมูลของผู้ถือหลักทรัพย์ เพื่อให้สามารถระบุผู้มีสิทธิได้อย่างถูกต้อง

(2) **การดำเนินการตามสิทธิและผลประโยชน์ของผู้ถือหลักทรัพย์ :** ผู้ออกหลักทรัพย์ควรมีกลไกหรือกระบวนการที่เหมาะสมเพื่อให้สามารถดำเนินการตามสิทธิและผลประโยชน์ของผู้ถือหลักทรัพย์โทเคนได้อย่างถูกต้อง ครบถ้วน และเป็นไปตามเงื่อนไขของหลักทรัพย์ หลักเกณฑ์ และ Tokenization Terms ที่เกี่ยวข้อง รวมถึงการจ่ายดอกเบี้ย เงินปันผล หรือผลประโยชน์ตอบแทนอื่น การไถ่ถอน หรือการดำเนินการอื่นตามสิทธิและเงื่อนไขของหลักทรัพย์

ตัวอย่าง : ผู้ออกหลักทรัพย์อาจใช้สัญญาอัจฉริยะ (Smart Contract) หรือระบบงานอื่นในการสนับสนุนการดำเนินการตามสิทธิและผลประโยชน์ของผู้ถือหลักทรัพย์โทเคน เช่น เมื่อถึงวันจ่ายดอกเบี้ยหรือเงินปันผล ระบบอาจอ้างอิงข้อมูลผู้มีสิทธิที่ได้กำหนดไว้ตาม (1) เพื่อคำนวณจำนวนเงินหรือผลประโยชน์ที่ผู้ถือแต่ละรายมีสิทธิได้รับ และดำเนินการจ่ายผลประโยชน์ไปยังบัญชีหรือ Wallet Address ที่กำหนด ทั้งนี้ ผู้ออกหลักทรัพย์ควรมีกลไกในการตรวจสอบความถูกต้องของข้อมูลและผลการดำเนินการดังกล่าวตามความเหมาะสม

(3) **การดำเนินการที่มีผลต่อหลักทรัพย์โทเคน :** ในกรณีที่การดำเนินการตามสิทธิหรือ Corporate Actions มีผลให้เกิดการเปลี่ยนแปลงต่อหลักทรัพย์โทเคน เช่น การไถ่ถอน การแตกหรือรวมหน่วย หรือการแปลงสภาพหลักทรัพย์ เป็นต้น ผู้ออกหลักทรัพย์ควรมีกลไกหรือกระบวนการที่เหมาะสมเพื่อให้การเปลี่ยนแปลงดังกล่าวได้รับการดำเนินการอย่างถูกต้องและสอดคล้องกับผลของ Corporate Actions เงื่อนไขของหลักทรัพย์ หลักเกณฑ์ และ Tokenization Terms ที่เกี่ยวข้อง

ตัวอย่าง : กรณีที่มีการไถ่ถอนหลักทรัพย์เมื่อครบกำหนดอายุ ผู้ออกหลักทรัพย์อาจกำหนดให้สัญญาอัจฉริยะ (Smart Contract) หรือกลไกที่เกี่ยวข้องดำเนินการเปลี่ยนสถานะของหลักทรัพย์โทเคนที่ได้รับการไถ่ถอนเพื่อไม่ให้สามารถโอนหรือทำธุรกรรมต่อได้ หรือในกรณีที่มีการแตกหรือรวมหน่วย ผู้ออกหลักทรัพย์อาจใช้กลไกในการปรับจำนวนหลักทรัพย์โทเคนที่ผู้ถือแต่ละรายถือครองให้สอดคล้องกับผลของ Corporate Actions ดังกล่าว ทั้งนี้ กลไกที่ใช้ควรทำให้การเปลี่ยนแปลงที่เกิดขึ้นกับหลักทรัพย์โทเคนสอดคล้องกับสิทธิและผลของ Corporate Actions ที่เกี่ยวข้อง

(4) การตรวจสอบย้อนหลังการดำเนินการตาม Corporate Actions : ผู้ออกหลักทรัพย์ควรมีกลไกหรือกระบวนการที่เหมาะสมในการจัดเก็บข้อมูลหรือหลักฐานที่เกี่ยวข้องกับการดำเนินการตาม Corporate Actions เพื่อให้สามารถตรวจสอบย้อนหลังถึงรายละเอียดและผลของการดำเนินการดังกล่าวได้ รวมถึงสามารถตรวจสอบความสอดคล้องระหว่างผู้มีสิทธิ การดำเนินการตามสิทธิ และการเปลี่ยนแปลงที่เกิดขึ้นกับหลักทรัพย์โทเคน

ตัวอย่าง : ผู้ออกหลักทรัพย์อาจจัดให้มีระบบหรือกลไกที่สามารถเชื่อมโยงข้อมูลที่เกี่ยวข้องกับ Corporate Actions ตลอดกระบวนการ โดยอาจกำหนดหมายเลขอ้างอิง (Reference ID) สำหรับ Corporate Action แต่ละรายการ และเชื่อมโยงข้อมูลดังกล่าวกับข้อมูลผู้มีสิทธิ หลักเกณฑ์และผลการคำนวณสิทธิ ตลอดจนข้อมูลการดำเนินการที่เกี่ยวข้อง เช่น Transaction Hash, Block Number หรือข้อมูลการเปลี่ยนแปลงสถานะของหลักทรัพย์โทเคนบน DLT หรือ Blockchain เพื่อให้สามารถตรวจสอบและติดตามย้อนหลังได้ว่า Corporate Action แต่ละรายการได้ดำเนินการอย่างไร และมีผลต่อผู้ถือหลักทรัพย์และหลักทรัพย์โทเคนอย่างไร

3.6 การจัดการกรณีพิเศษที่เกี่ยวข้องกับหลักทรัพย์โทเคน (Special Circumstances Management)

หลักทรัพย์โทเคนอาจเกิดกรณีหรือสถานการณ์ที่อยู่นอกเหนือจากการดำเนินงานตามปกติ ซึ่งอาจทำให้ผู้ถือหลักทรัพย์ไม่สามารถใช้หรือเข้าถึงสิทธิของตนได้ หรือทำให้ผู้ออกหลักทรัพย์จำเป็นต้องดำเนินการกับหลักทรัพย์โทเคนเพื่อให้เป็นไปตามกฎหมายหรือคำสั่งของผู้มีอำนาจ ดังนั้น ผู้ออกหลักทรัพย์ควรกำหนดกลไกหรือกระบวนการที่เหมาะสมเพื่อรองรับและจัดการกรณีดังกล่าว

3.6.1 การสูญเสียหรือไม่สามารถเข้าถึงหลักทรัพย์โทเคน (Loss of Access to Tokenized Securities)

ผู้ถือหลักทรัพย์อาจไม่สามารถเข้าถึงหรือควบคุมหลักทรัพย์โทเคนที่ตนถือครองได้จากเหตุการณ์ต่าง ๆ เช่น การสูญหายหรือชำรุดของอุปกรณ์ การสูญเสียหรือไม่สามารถใช้ข้อมูลหรือกลไกที่ใช้ในการเข้าถึง Wallet หรือการสูญเสีย Private Key ซึ่งอาจส่งผลให้ผู้ถือหลักทรัพย์ไม่สามารถใช้หรือดำเนินการเกี่ยวกับหลักทรัพย์โทเคนของตนได้ ดังนั้น ผู้ออกหลักทรัพย์ควรมีกลไกหรือกระบวนการที่เหมาะสมในการตรวจสอบและพิสูจน์สิทธิของผู้ถือหลักทรัพย์ รวมถึงดำเนินการเพื่อให้ผู้ถือหลักทรัพย์สามารถกลับมาใช้สิทธิที่เกี่ยวข้องกับหลักทรัพย์โทเคนได้ตามกระบวนการที่กำหนด

แนวทางปฏิบัติ : ผู้ออกหลักทรัพย์ควรกำหนดกลไกหรือกระบวนการที่เหมาะสมสำหรับรองรับกรณีที่ผู้ถือหลักทรัพย์ไม่สามารถเข้าถึงหรือควบคุมหลักทรัพย์โทเคนของตนได้ โดยอย่างน้อยควรครอบคลุมเรื่องดังต่อไปนี้

(1) **การพิสูจน์ตัวตนและสิทธิของผู้ยื่นคำขอ :** ผู้ออกหลักทรัพย์ควรกำหนดกระบวนการในการตรวจสอบและพิสูจน์ตัวตนของผู้ยื่นคำขอ รวมถึงพิสูจน์สิทธิของผู้ยื่นคำขอในหลักทรัพย์โทเคนที่ไม่สามารถเข้าถึงได้ ก่อนดำเนินการใด ๆ ที่อาจมีผลต่อสิทธิหรือสถานะของหลักทรัพย์โทเคน ทั้งนี้ การพิสูจน์สิทธิดังกล่าวควรพิจารณาข้อมูลและหลักฐานที่เกี่ยวข้องกับความเชื่อมโยงระหว่างผู้ยื่นคำขอกับหลักทรัพย์โทเคนหรือ Wallet Address ที่เกี่ยวข้อง รวมถึงเหตุที่ทำให้ผู้ถือหลักทรัพย์ไม่สามารถเข้าถึงหรือควบคุมหลักทรัพย์โทเคนได้

ตัวอย่าง : ผู้ออกหลักทรัพย์อาจกำหนดให้ผู้ยื่นคำขอผ่านกระบวนการยืนยันและตรวจสอบตัวตนเพิ่มเติม เช่น การดำเนินการ **Re-KYC** และตรวจสอบความสอดคล้องของข้อมูลผู้ยื่นคำขอกับข้อมูลที่ปรากฏในทะเบียนผู้ถือหลักทรัพย์ รวมถึงข้อมูลที่เกี่ยวข้องกับ Wallet Address ที่ใช้ถือครองหลักทรัพย์โทเคน นอกจากนี้ ผู้ออกหลักทรัพย์อาจกำหนดให้ผู้ยื่นคำขอแสดงข้อมูลหรือหลักฐานประกอบเกี่ยวกับเหตุที่ทำให้ไม่สามารถเข้าถึงหลักทรัพย์โทเคน และกำหนดระดับของการตรวจสอบหรือหลักฐานเพิ่มเติมให้เหมาะสมกับลักษณะและผลกระทบของการดำเนินการที่จะเกิดขึ้น ตัวอย่างเช่น หากการดำเนินการมีผลเป็นการ ระงับหรือยกเลิกหลักทรัพย์โทเคนเดิมออกหลักทรัพย์โทเคนทดแทน หรือเปลี่ยนแปลงข้อมูลเกี่ยวกับการถือครองหลักทรัพย์โทเคน ผู้ออกหลักทรัพย์อาจกำหนดให้มีหลักฐานเพิ่มเติมที่เหมาะสมกับกรณี เช่น เอกสารหรือหลักฐานเกี่ยวกับเหตุการณ์ที่เกิดขึ้น หลักฐานการแจ้งความ หรือคำสั่งศาลหรือเอกสารจากหน่วยงานของรัฐที่มีอำนาจ

(2) **การดำเนินการเพื่อให้ผู้ถือหลักทรัพย์สามารถเข้าถึงหลักทรัพย์โทเคนได้ :** เมื่อผู้ออกหลักทรัพย์สามารถพิสูจน์ตัวตนและสิทธิของผู้ยื่นคำขอ รวมถึงเหตุแห่งการไม่สามารถเข้าถึงหลักทรัพย์โทเคนได้แล้ว ผู้ออกหลักทรัพย์ควรมีกระบวนการที่เหมาะสมในการดำเนินการเพื่อให้ผู้ถือหลักทรัพย์สามารถเข้าถึงและควบคุมหลักทรัพย์โทเคนได้อีกครั้ง โดยการดำเนินการดังกล่าวต้องไม่ทำให้เกิดการถือครองหลักทรัพย์โทเคนซ้ำซ้อน และต้องสามารถรักษาความถูกต้องของทะเบียนผู้ถือและสถานะของหลักทรัพย์โทเคนได้

ตัวอย่าง : ผู้ออกหลักทรัพย์อาจกำหนดให้สัญญาอัจฉริยะ (Smart Contract) รองรับฟังก์ชันการกู้คืนหรือโอนย้ายการถือครองโทเคน

(Recovery and Forced Transfer) เพื่อดำเนินการกู้คืนการถือครองหรือเปลี่ยน Wallet Address ที่ใช้ถือครองหลักทรัพย์โทเคนไปยัง Wallet Address ใหม่ของผู้ถือหลักทรัพย์ ภายหลังจากที่ผู้ถือหลักทรัพย์ผ่านกระบวนการตรวจสอบตามที่กำหนดแล้ว

(3) **การจัดเก็บหลักฐานและตรวจสอบย้อนหลัง :** ผู้ออกหลักทรัพย์ควรมีกลไกหรือกระบวนการที่เหมาะสมในการจัดเก็บข้อมูลและหลักฐานที่เกี่ยวข้องกับการดำเนินการกรณีผู้ถือหลักทรัพย์ไม่สามารถเข้าถึงหลักทรัพย์โทเคน เพื่อให้สามารถตรวจสอบย้อนหลังถึงเหตุแห่งการดำเนินการ ผู้ยื่นคำขอกระบวนการตรวจสอบและพิสูจน์สิทธิ ตลอดจนผลของการดำเนินการที่เกี่ยวข้องกับหลักทรัพย์โทเคนได้

ตัวอย่าง : ผู้ออกหลักทรัพย์อาจกำหนดหมายเลขอ้างอิง (Reference ID) สำหรับคำขอแต่ละรายการ และจัดเก็บข้อมูลที่เกี่ยวข้องกับการดำเนินการ เช่น ข้อมูลผู้ยื่นคำขอ ผลการตรวจสอบและพิสูจน์สิทธิ หลักฐานประกอบการดำเนินการ ตลอดจนข้อมูลการดำเนินการบน DLT หรือ Blockchain เช่น Wallet Address เดิมและใหม่ Transaction Hash และ Block Number เพื่อให้สามารถตรวจสอบย้อนหลังได้ว่า การดำเนินการดังกล่าวเป็นไปตามกระบวนการที่กำหนดและมีผลต่อการถือครองหลักทรัพย์โทเคนอย่างไร

3.6.2 การดำเนินการตามคำสั่งของศาลหรือหน่วยงานรัฐที่มีอำนาจสั่งการ (Actions pursuant to Court or Competent Authority Orders)

ในกรณีที่มีคำสั่งของศาลหรือหน่วยงานกำกับดูแลหรือหน่วยงานอื่นที่มีอำนาจตามกฎหมายให้ดำเนินการเกี่ยวกับหลักทรัพย์โทเคน เช่น การอายัด การระงับการโอน การโอน หรือการแก้ไขเปลี่ยนแปลงการถือครองหลักทรัพย์โทเคน ผู้ออกหลักทรัพย์อาจจำเป็นต้องดำเนินการตามคำสั่งดังกล่าวเพื่อให้เป็นไปตามกฎหมาย ดังนั้น ผู้ออกหลักทรัพย์ควรมีกลไกหรือกระบวนการที่เหมาะสมเพื่อรองรับการตรวจสอบและดำเนินการตามคำสั่งดังกล่าว

แนวทางปฏิบัติ : ผู้ออกหลักทรัพย์ควรกำหนดกลไกหรือกระบวนการที่เหมาะสมสำหรับรองรับกรณีที่ต้องดำเนินการตามคำสั่งของศาล หน่วยงานกำกับดูแล หรือหน่วยงานอื่นที่มีอำนาจตามกฎหมาย โดยอย่างน้อยควรครอบคลุมเรื่องดังต่อไปนี้

การดำเนินการตามคำสั่งของศาลหรือหน่วยงานที่มีอำนาจ : ผู้ออกหลักทรัพย์ควรมีกระบวนการสำหรับรับและตรวจสอบคำสั่งของศาล หน่วยงานกำกับดูแล หรือหน่วยงานอื่นที่มีอำนาจตามกฎหมาย รวมถึงตรวจสอบขอบเขตของคำสั่งและหลักทรัพย์โทเคนหรือการถือครองที่เกี่ยวข้อง และดำเนินการกับหลักทรัพย์โทเคนให้เป็นไปตามคำสั่งดังกล่าว

เช่น การระงับการโอนหรือการทำธุรกรรม การยกเลิกหรือเพิกถอนหลักทรัพย์โทเคน หรือการโอนการถือครองไปยังบุคคลหรือ Wallet Address ที่กำหนด เป็นต้น รวมถึงควรจัดเก็บข้อมูลและหลักฐานที่เกี่ยวข้องกับการดำเนินการ เพื่อให้สามารถตรวจสอบย้อนหลังได้ว่าการดำเนินการเป็นไปตามคำสั่งและมีผลต่อหลักทรัพย์โทเคนหรือการถือครองอย่างไร

ตัวอย่าง : หากศาลหรือหน่วยงานที่มีอำนาจมีคำสั่งให้ระงับการโอนหรือการทำธุรกรรมของหลักทรัพย์โทเคน ผู้ออกหลักทรัพย์อาจใช้ฟังก์ชัน **Freeze หรือ Suspend** เพื่อระงับการดำเนินการดังกล่าว ในกรณีที่มีคำสั่งให้ยกเลิกหรือเพิกถอนหลักทรัพย์โทเคน อาจใช้ฟังก์ชัน **Token Recall หรือ Revocation** และในกรณีที่มีคำสั่งให้โอนการถือครองหลักทรัพย์โทเคนจากผู้ถือรายหนึ่งไปยังบุคคลหรือ Wallet Address ที่กำหนด อาจใช้ฟังก์ชัน **Forced Transfer** ทั้งนี้ การเลือกใช้ฟังก์ชันควรสอดคล้องกับลักษณะและผลของคำสั่งที่ได้รับ

4. มาตรฐานด้านเทคนิคสำหรับหลักทรัพย์โทเคน (Token Standard)

หลักทรัพย์โทเคนเป็นการแสดงสิทธิในหลักทรัพย์ในรูปแบบดิจิทัลที่อาศัยเทคโนโลยีในการกำหนด บันทึก และบริหารจัดการข้อมูล สิทธิ และธุรกรรมที่เกี่ยวข้อง ดังนั้น การออกแบบหลักทรัพย์โทเคนจึงควรมีมาตรฐานทางเทคนิคที่ชัดเจน เพื่อให้โทเคนสามารถทำหน้าที่เป็นตัวแทนของหลักทรัพย์ได้อย่างถูกต้อง มีความน่าเชื่อถือ สามารถตรวจสอบได้ และรองรับการใช้งานตลอดวงจรชีวิตของหลักทรัพย์ได้อย่างเหมาะสม

มาตรฐานในบทนี้มุ่งกำหนดคุณลักษณะทางเทคนิคและความสามารถขั้นต่ำที่หลักทรัพย์โทเคนและองค์ประกอบที่เกี่ยวข้องควรรองรับ เพื่อสนับสนุนการพัฒนา การเชื่อมโยง และการทำงานร่วมกันของระบบที่เกี่ยวข้องกับหลักทรัพย์โทเคน โดยยึดหลักความเป็นกลางทางเทคโนโลยี (Technology Neutrality) และมุ่งกำหนดผลลัพธ์ที่ควรรองรับ มากกว่าการกำหนดเทคโนโลยี เครือข่าย หรือรูปแบบการพัฒนาเฉพาะ เพื่อให้สามารถนำไปประยุกต์ใช้กับ Distributed Ledger Technology (DLT), Blockchain หรือเทคโนโลยีอื่นที่ให้คุณสมบัติเทียบเท่าได้อย่างเหมาะสม

เนื้อหาในบทนี้ครอบคลุมหลักการออกแบบและสถาปัตยกรรมของระบบ ฟังก์ชันการทำงานของโทเคน ข้อกำหนดด้านข้อมูลของโทเคน และแนวทางการออกแบบเพื่อรองรับการเชื่อมต่อและการทำงานร่วมกันระหว่างระบบและผู้เกี่ยวข้อง เพื่อสนับสนุนการพัฒนาและการใช้งานหลักทรัพย์โทเคนให้มีความสอดคล้อง โปร่งใส สามารถทำงานร่วมกันได้ และรองรับการพัฒนาในระบบนิเวศของตลาดทุนในระยะยาว

ทั้งนี้ มาตรฐานฉบับนี้มุ่งกำหนดคุณลักษณะและความสามารถของหลักทรัพย์โทเคนในเชิงเทคนิค รวมถึงข้อกำหนดที่จำเป็นต่อการเชื่อมโยงและการทำงานร่วมกันของระบบ โดยไม่ครอบคลุมข้อกำหนดเกี่ยวกับสิทธิและผลทางกฎหมายของหลักทรัพย์ มาตรการด้านความมั่นคงปลอดภัยของระบบ หรือข้อกำหนดด้านการกำกับดูแลกิจการและการบริหารจัดการภายในของผู้ให้บริการ ซึ่งให้เป็นไปตามกฎหมายหรือมาตรฐานที่เกี่ยวข้องต่อไป

4.1 หลักการออกแบบและสถาปัตยกรรมของโทเคน (Token Design Principles and Architecture)

การออกแบบหลักทรัพย์โทเคนเป็นปัจจัยสำคัญที่ส่งผลต่อความสามารถในการเป็นตัวแทนของสิทธิในหลักทรัพย์ ความถูกต้องของข้อมูล ความสามารถในการตรวจสอบ และการรองรับการใช้งานของโทเคนตลอดวงจรชีวิตของหลักทรัพย์ การกำหนดหลักการออกแบบและการเลือกโครงสร้างพื้นฐานที่เหมาะสมยังช่วยให้โทเคนสามารถรองรับการเปลี่ยนแปลง การพัฒนาเพิ่มเติม และการเชื่อมต่อกับผู้เกี่ยวข้องหรือโครงสร้างพื้นฐานอื่นได้อย่างมีประสิทธิภาพ

หัวข้อนี้กำหนดหลักการพื้นฐานที่ควรนำมาพิจารณาในการออกแบบหลักทรัพย์โทเคนและการเลือกโครงสร้างพื้นฐานที่ใช้รองรับ โดยมุ่งเน้นการกำหนดกรอบแนวคิดและปัจจัยที่ควรพิจารณา มากกว่าการกำหนดเทคโนโลยี รูปแบบการพัฒนา หรือแพลตฟอร์มเฉพาะ ทั้งนี้ เพื่อเป็นแนวทางในการออกแบบและพัฒนาหลักทรัพย์โทเคนให้สามารถรองรับคุณลักษณะและความสามารถตามมาตรฐานฉบับนี้

4.1.1 หลักการออกแบบโทเคน (Token Design Principles)

การออกแบบหลักทรัพย์โทเคนควรยึดหลักการพื้นฐานที่ส่งเสริมให้โทเคนสามารถเป็นตัวแทนของสิทธิในหลักทรัพย์ได้อย่างถูกต้อง มีโครงสร้างที่เหมาะสม สามารถรองรับการใช้งาน การกำกับดูแล และการพัฒนาในอนาคตได้อย่างมีประสิทธิภาพ ทั้งนี้ หลักการตามหัวข้อนี้มุ่งกำหนดแนวคิดพื้นฐานในการออกแบบหลักทรัพย์โทเคน มากกว่าการกำหนดเทคโนโลยีหรือวิธีการพัฒนาเฉพาะ เพื่อให้สามารถนำไปประยุกต์ใช้กับเทคโนโลยีและรูปแบบสถาปัตยกรรมที่หลากหลายได้

การออกแบบหลักทรัพย์โทเคน ควรคำนึงถึงหลักการสำคัญอย่างน้อย ดังต่อไปนี้

(1) การแยกองค์ประกอบตามหน้าที่ (Separation of Concerns) : การออกแบบหลักทรัพย์โทเคนควรแยกองค์ประกอบที่มีหน้าที่แตกต่างกันออกจากกันอย่างเหมาะสม เพื่อลดความซับซ้อนของระบบ สนับสนุนการพัฒนา การบำรุงรักษา การทดสอบ และการเปลี่ยนแปลงองค์ประกอบแต่ละส่วน โดยไม่ส่งผลกระทบต่อองค์ประกอบอื่นเกินสมควร

ตัวอย่าง : การแยกองค์ประกอบสำหรับจัดเก็บข้อมูลของโทเคน (token state) ออกจากองค์ประกอบที่กำหนดตรรกะหรือฟังก์ชันของโทเคน (business logic) หรือการแยกกลไกด้านการกำกับดูแลและการปฏิบัติตามข้อกำหนด (compliance module) ออกจากฟังก์ชันพื้นฐานของโทเคน (core token functions)

(2) ความสามารถในการขยายและรองรับการพัฒนาในอนาคต (Modularity and Extensibility) : การออกแบบหลักทรัพย์โทเคนควรเอื้อต่อการเพิ่มเติม ปรับปรุง หรือขยายความสามารถในอนาคต โดยไม่กระทบต่อความถูกต้องของข้อมูล สิทธิของผู้ถือหลักทรัพย์ หรือการทำงานขององค์ประกอบเดิมเกินสมควร เพื่อรองรับการเปลี่ยนแปลงของหลักทรัพย์ กฎหมาย หรือความต้องการทางธุรกิจในอนาคต

ตัวอย่าง : การรองรับการปรับปรุง เพิ่ม หรือลดรายการข้อมูล การเพิ่มเติมฟังก์ชัน และการปรับปรุงให้สามารถเชื่อมต่อกับระบบหรือบริการอื่นได้ โดยไม่จำเป็นต้องยกเลิกโทเคนเดิมและย้ายไปใช้งานบนโทเคนที่สร้างขึ้นใหม่ทั้งหมด หรือไม่ทำให้ส่งผลกระทบต่อการทำงานขององค์ประกอบเดิมเกินสมควร

(3) ความสามารถในการตรวจสอบและติดตามย้อนหลัง (Auditability and Traceability) : การออกแบบหลักทรัพย์โทเคนควรเอื้อให้สามารถตรวจสอบข้อมูลสถานะ และการเปลี่ยนแปลงที่เกี่ยวข้องกับโทเคนได้อย่างเหมาะสม เพื่อสนับสนุนการตรวจสอบย้อนหลัง การกำกับดูแล และการพิสูจน์ความถูกต้องของข้อมูลตลอดวงจรชีวิตของโทเคน

ตัวอย่าง : การสามารถตรวจสอบประวัติการออก การโอน การอายัด หรือการเปลี่ยนแปลงข้อมูลสำคัญของโทเคน รวมถึงการเชื่อมโยงไปยังข้อมูลหรือเอกสารอ้างอิงที่เกี่ยวข้อง

(4) การออกแบบเพื่อรองรับการทำงานร่วมกัน (Interoperability by Design) : การออกแบบหลักทรัพย์โทเคนควรคำนึงถึงการเชื่อมต่อและการทำงานร่วมกับผู้เกี่ยวข้อง ระบบ หรือโครงสร้างพื้นฐานอื่นตั้งแต่เริ่มต้น เพื่อสนับสนุนการแลกเปลี่ยนข้อมูล การเชื่อมโยงข้อมูลอ้างอิง และการพัฒนาการทำงานร่วมกันในอนาคต โดยไม่สร้างข้อจำกัดที่ไม่สมเหตุสมผลต่อการเชื่อมต่อหรือการใช้งาน

ตัวอย่าง : การรองรับการใช้ตัวระบุมาตรฐาน (Standard Identifiers) การกำหนดเมตาดาต้าที่สามารถแลกเปลี่ยนกับระบบอื่น หรือการเชื่อมโยงกับระบบทะเบียนผู้ถือหลักทรัพย์ ระบบรับฝากหลักทรัพย์ หรือระบบชำระราคา

4.1.2 หลักการเลือกโครงสร้างพื้นฐาน (Infrastructure Selection Principles)

การเลือกโครงสร้างพื้นฐานสำหรับหลักทรัพย์โทเคนเป็นปัจจัยสำคัญที่ส่งผลต่อความสามารถในการรองรับคุณลักษณะและการทำงานของหลักทรัพย์โทเคน ตลอดจนความสามารถในการเชื่อมต่อ การขยายตัว และการรองรับการเปลี่ยนแปลงในอนาคต โครงสร้างพื้นฐานที่เลือกใช้จึงควรสอดคล้องกับลักษณะของหลักทรัพย์ วัตถุประสงค์ในการใช้งาน รูปแบบการกำกับดูแล และข้อกำหนดที่เกี่ยวข้อง โดยคำนึงถึงคุณลักษณะและความสามารถที่จำเป็น มากกว่าการเลือกใช้เทคโนโลยีหรือเครือข่ายประเภทใดประเภทหนึ่ง

การเลือกโครงสร้างพื้นฐานควรคำนึงถึงหลักการสำคัญอย่างน้อย ดังต่อไปนี้

(1) การเลือกเทคโนโลยีและรูปแบบของโครงสร้างพื้นฐาน (Technology Platform Selection) : การเลือกใช้ Distributed Ledger Technology (DLT), Blockchain หรือเทคโนโลยีอื่นที่มีคุณสมบัติเทียบเท่า รวมถึงรูปแบบของโครงสร้างพื้นฐาน เช่น Public, Private, Consortium, Hybrid หรือรูปแบบอื่นที่เหมาะสม ควรพิจารณาให้สอดคล้องกับลักษณะของหลักทรัพย์ วัตถุประสงค์ในการใช้งาน รูปแบบการกำกับดูแล ข้อกำหนด

ทางกฎหมาย และความเสี่ยงที่เกี่ยวข้อง เพื่อให้สามารถรองรับคุณลักษณะและความสามารถตามมาตรฐานฉบับนี้ได้อย่างเหมาะสม

ตัวอย่าง : หลักทรัพย์โทเคนที่มีผู้เกี่ยวข้องจำนวนจำกัดและต้องการควบคุมการเข้าถึงข้อมูล อาจเลือกใช้ Private หรือ Consortium DLT ขณะที่หลักทรัพย์โทเคนที่มีผู้เกี่ยวข้องจำนวนมาก หรือต้องการให้ข้อมูลหรือธุรกรรมสามารถตรวจสอบได้ในวงกว้าง อาจเลือกใช้ Public Blockchain ที่มีคุณสมบัติเหมาะสม

(2) คุณลักษณะของโครงสร้างพื้นฐาน (Infrastructure Characteristics) : การเลือกโครงสร้างพื้นฐานควรพิจารณาคุณลักษณะที่จำเป็นต่อการรองรับหลักทรัพย์โทเคน เช่น ความถูกต้องครบถ้วนของข้อมูล (Data Integrity) ความสามารถในการตรวจสอบย้อนหลัง (Traceability) ความสมบูรณ์ของธุรกรรม (Transaction Finality) ความสามารถในการรองรับปริมาณการใช้งาน (Scalability) ความพร้อมใช้งาน (Availability) และประสิทธิภาพในการประมวลผลธุรกรรม (Performance) เพื่อให้สามารถรองรับการดำเนินงานได้อย่างเหมาะสมตามลักษณะของผลิตภัณฑ์และปริมาณธุรกรรมที่คาดว่าจะเกิดขึ้น ทั้งนี้ สำหรับโครงสร้างพื้นฐานที่ใช้กลไกฉันทามติ (Consensus) ควรพิจารณาความเหมาะสมของกลไกดังกล่าว จำนวนและการกระจายตัวของโหนดที่ร่วมยืนยันธุรกรรม รวมถึงความสามารถในการรักษาความถูกต้องของข้อมูลและความต่อเนื่องของระบบเมื่อโหนดบางส่วนขัดข้องหรือทำงานไม่ถูกต้อง

(3) การรองรับการกำกับดูแล (Governance Enablement): การเลือกโครงสร้างพื้นฐานควรพิจารณาว่าสามารถรองรับการกำหนดและบังคับใช้กลไกการกำกับดูแลที่เหมาะสมตลอดวงจรชีวิตของหลักทรัพย์โทเคนได้ รวมถึงรองรับการกำหนดบทบาท สิทธิ อำนาจ และกระบวนการอนุมัติที่เกี่ยวข้องกับการดำเนินการที่สำคัญ

ตัวอย่าง : การรองรับการกำหนดสิทธิ์ของผู้มีอำนาจดำเนินการ (Role-based Access Control) การกำหนดให้การดำเนินการสำคัญต้องได้รับการอนุมัติจากหลายฝ่าย (Multi-party Authorization) หรือการรองรับการปรับปรุงองค์ประกอบของระบบตามกระบวนการกำกับดูแลที่กำหนด

(4) การรองรับการทำงานร่วมกันระหว่างโครงสร้างพื้นฐานดิจิทัล (Interoperability Readiness) : การเลือกโครงสร้างพื้นฐานควรพิจารณาความสามารถในการรองรับการเชื่อมต่อและการทำงานร่วมกับโครงสร้างพื้นฐานดิจิทัลอื่น เพื่อรองรับการแลกเปลี่ยนข้อมูล การสื่อสาร การทำธุรกรรม และการชำระราคาและส่งมอบสินทรัพย์ระหว่างเครือข่ายได้อย่างมีประสิทธิภาพ รวมถึงสามารถรองรับการเชื่อมต่อกับโครงสร้างพื้นฐาน

หรือมาตรฐานที่อาจเกิดขึ้นในอนาคต โดยไม่สร้างข้อจำกัดทางเทคนิคที่ไม่จำเป็นต่อการเชื่อมต่อหรือการทำงานร่วมกับเครือข่ายอื่น

ตัวอย่าง : การรองรับการทำธุรกรรมระหว่างเครือข่ายที่แตกต่างกัน (Cross-network Transactions) การเชื่อมต่อกับเครือข่ายที่รองรับหลักทรัพย์โทเคนหรือเงินตราเพื่อการชำระราคา (Tokenized Money) หรือการรองรับกลไกที่เอื้อให้เกิดการชำระราคาและส่งมอบทรัพย์ระหว่างโครงสร้างพื้นฐานที่แตกต่างกัน (Cross-network Settlement)

4.2 ฟังก์ชันการทำงานของโทเคน (Token Functional Requirements)

ฟังก์ชันการทำงานของโทเคนเป็นองค์ประกอบสำคัญที่กำหนดพฤติกรรม (Behavior) และความสามารถในการดำเนินการของหลักทรัพย์โทเคนตลอดวงจรชีวิต ตั้งแต่การออกหลักทรัพย์ การโอน การใช้สิทธิ การกำกับดูแล และการสิ้นสุดสภาพของโทเคน ฟังก์ชันดังกล่าวควรได้รับการออกแบบให้สอดคล้องกับลักษณะ สิทธิ และเงื่อนไขของหลักทรัพย์ที่โทเคนเป็นตัวแทน รวมทั้งสามารถรองรับข้อกำหนดทางกฎหมาย ข้อกำหนดด้านการกำกับดูแล และการดำเนินงานที่เกี่ยวข้องได้อย่างเหมาะสม

หัวข้อนี้กำหนดฟังก์ชันการทำงานที่หลักทรัพย์โทเคนควรรองรับ โดยแบ่งออกเป็นฟังก์ชันพื้นฐาน (Core Functions) ที่จำเป็นต่อการดำเนินงานของโทเคน ฟังก์ชันสำหรับผู้ดูแลระบบ (Administrative Functions) ฟังก์ชันสำหรับการกำกับดูแลและการปฏิบัติตามกฎหมาย (Compliance Functions) ตลอดจน ฟังก์ชันเพิ่มเติมตามลักษณะของหลักทรัพย์ (Additional Functions Based on Product Characteristics) ทั้งนี้ การกำหนดฟังก์ชันแต่ละประเภทควรเป็นไปตามหลักความจำเป็น ความเหมาะสม และสอดคล้องกับวัตถุประสงค์ของการออกหลักทรัพย์โทเคน

4.2.1 ฟังก์ชันพื้นฐาน (Core Functions)

หลักการทั่วไป

หลักทรัพย์โทเคนควรรองรับฟังก์ชันพื้นฐานที่จำเป็นต่อการดำเนินงานของโทเคน เพื่อให้สามารถจัดการอุปทาน การเปลี่ยนแปลงการถือครอง และการแสดงสถานะของโทเคนได้อย่างถูกต้อง สอดคล้องกับสิทธิและเงื่อนไขของหลักทรัพย์ที่โทเคนเป็นตัวแทน และสามารถรองรับการดำเนินงานตลอดวงจรชีวิตของหลักทรัพย์ได้อย่างเหมาะสม ทั้งนี้ ฟังก์ชันพื้นฐานควรได้รับการออกแบบให้มีความถูกต้อง เชื่อถือได้ และสามารถตรวจสอบย้อนหลังได้

ข้อเสนอแนะขั้นต่ำ

หลักทรัพย์โทเคนควรรองรับฟังก์ชันพื้นฐานอย่างน้อย ดังต่อไปนี้

(1) ฟังก์ชันการจัดการอุปทาน (Supply Management) : โทเคนควรมีฟังก์ชันสำหรับการจัดการอุปทานของโทเคนอย่างชัดเจน เพื่อรองรับการออกโทเคน การเพิ่มหรือลด

จำนวนโทเคน การเพิกถอน การทำลาย หรือการสิ้นผลของโทเคนตามลักษณะและเงื่อนไขของหลักทรัพย์ การดำเนินการที่มีผลต่ออุปทานของโทเคนควรสามารถระบุผลของการดำเนินการต่อจำนวนโทเคนทั้งหมดได้อย่างชัดเจน และสามารถตรวจสอบย้อนหลังได้ ทั้งนี้ ในกรณีที่โทเคนถูกออกแบบให้ไม่สามารถเปลี่ยนแปลงอุปทานได้ภายหลัง ระบบควรกำหนดลักษณะดังกล่าวไว้อย่างชัดเจน และไม่ควรเปิดช่องให้มีการเปลี่ยนแปลงอุปทานโดยขัดต่อข้อกำหนดที่กำหนดไว้

(2) **ฟังก์ชันการโอน (Transfer) :** โทเคนควรมีฟังก์ชันสำหรับการโอนโทเคนจากผู้ถือรายหนึ่งไปยังผู้ถืออีกรายหนึ่ง เพื่อให้การเปลี่ยนแปลงการถือครองเป็นไปอย่างถูกต้องสอดคล้องกับสิทธิและเงื่อนไขของหลักทรัพย์ และสามารถตรวจสอบย้อนหลังได้ ฟังก์ชันการโอนควรรองรับการตรวจสอบความถูกต้องของธุรกรรมก่อนการโอนมีผล (Pre-validation) อย่างน้อยให้สามารถตรวจสอบได้ว่า ผู้ดำเนินการมีสิทธิในการดำเนินธุรกรรมตามที่กำหนด ผู้โอนมียอดคงเหลือเพียงพอ และการโอนไม่ก่อให้เกิดสถานะหรือข้อมูลที่ไม่ถูกต้องของโทเคน เช่น ยอดคงเหลือของผู้โอนติดลบ (Negative Balance) จำนวนโทเคนรวม (Total Supply) ไม่ถูกต้อง เกิดการโอนซ้ำจากธุรกรรมเดียวกัน หรือการโอนไปยังบัญชีที่ไม่สามารถถือครองหลักทรัพย์โทเคนประเภทนั้นได้ (Transfer Restriction) เป็นต้น เมื่อการโอนมีผลสมบูรณ์ ระบบควรปรับปรุงสถานะการถือครองของผู้โอนและผู้รับโอนให้ถูกต้อง รวมทั้งบันทึกผลของธุรกรรมเพื่อให้สามารถตรวจสอบย้อนหลังได้

ทั้งนี้ ในกรณีที่หลักทรัพย์โทเคนกำหนดเงื่อนไขหรือข้อจำกัดเพิ่มเติมเกี่ยวกับการโอน ฟังก์ชันการโอนควรสามารถรองรับการตรวจสอบและบังคับใช้เงื่อนไขดังกล่าวก่อนที่การโอนจะมีผล

(3) **ฟังก์ชันการตรวจสอบยอดและสถานะ (Balance and State Inquiry) :** โทเคนควรมีฟังก์ชันสำหรับการตรวจสอบยอดคงเหลือหรือสถานะการถือครองของโทเคนของแต่ละบัญชีหรือข้อมูลที่ใช้ระบุการถือครองโทเคน เช่น ที่อยู่ของกระเป๋าสินทรัพย์ดิจิทัล (Wallet Address) เพื่อให้ผู้เกี่ยวข้องสามารถอ้างอิงข้อมูลสถานะล่าสุดของโทเคนได้อย่างชัดเจน

ฟังก์ชันดังกล่าวควรสามารถรองรับการตรวจสอบยอดคงเหลือของโทเคนของแต่ละบัญชีหรือข้อมูลที่ใช้ระบุการถือครองโทเคน การตรวจสอบจำนวนโทเคนทั้งหมดที่มีอยู่ในระบบ การแสดงสถานะการถือครองให้สอดคล้องกับผลของธุรกรรมล่าสุด

ในระบบ และการแสดงสถานะ สิทธิ หรือข้อจำกัดที่ผูกกับโทเคนหรือผู้ถือ ซึ่งอาจส่งผลต่อการใช้สิทธิ การโอน หรือการดำเนินการอื่นที่เกี่ยวข้องกับโทเคน เช่น การอายัด การระงับการโอน หรือข้อจำกัดอื่นตามเงื่อนไขของหลักทรัพย์หรือกฎหมายที่เกี่ยวข้อง

4.2.2 ฟังก์ชันการบริหารจัดการโทเคน (Administrative Functions)

หลักการทั่วไป

หลักทรัพย์โทเคนควรรองรับฟังก์ชันสำหรับการบริหารจัดการโทเคน (Administrative Functions) เพื่อให้สามารถดำเนินการเกี่ยวกับสถานะ การถือครอง และองค์ประกอบที่เกี่ยวข้องกับโทเคนได้อย่างเหมาะสมตลอดวงจรชีวิตของหลักทรัพย์ ทั้งนี้ ฟังก์ชันดังกล่าวมีวัตถุประสงค์เพื่อสนับสนุนการบริหารจัดการโทเคนในกรณีที่จำเป็นอันเนื่องมาจากการดำเนินงานของระบบ การเปลี่ยนแปลงสถานะของโทเคน หรือการดำเนินการอื่นที่เกี่ยวข้องกับการจัดการโทเคน โดยจะต้องไม่กระทบต่อความถูกต้อง ความสมบูรณ์ และความน่าเชื่อถือของข้อมูลที่เกี่ยวข้อง

ฟังก์ชันสำหรับการบริหารจัดการโทเคนควรได้รับการออกแบบให้สามารถรองรับการจัดการสถานะของโทเคน การจัดการการถือครอง และการปรับปรุงองค์ประกอบของโทเคนได้อย่างถูกต้อง โปร่งใส และสามารถตรวจสอบย้อนหลังได้ โดยไม่ก่อให้เกิดการเปลี่ยนแปลงสิทธิหรือเงื่อนไขของหลักทรัพย์นอกเหนือจากที่กำหนดไว้

ข้อเสนอแนะขั้นต่ำ

หลักทรัพย์โทเคนควรรองรับฟังก์ชันสำหรับผู้ดูแลระบบอย่างน้อย ดังต่อไปนี้

(1) ฟังก์ชันการจัดการสถานะของโทเคน (Token State Management) : โทเคนควรมีฟังก์ชันสำหรับการจัดการสถานะของโทเคน เพื่อรองรับการกำหนด เปลี่ยนแปลง หรือยกเลิกสถานะของโทเคนตามสิทธิ เงื่อนไข หรือข้อกำหนดที่เกี่ยวข้อง รวมทั้งสามารถกำหนดข้อจำกัดที่มีผลต่อการใช้สิทธิ การโอน หรือการดำเนินการอื่นที่เกี่ยวข้องกับโทเคนได้อย่างถูกต้อง ฟังก์ชันดังกล่าวควรรองรับการกำหนดสถานะของโทเคน เช่น การระงับการโอน (Freeze) การปลดการระงับ (Unfreeze) การระงับการใช้งาน (Suspend) หรือสถานะอื่นตามลักษณะของหลักทรัพย์ ทั้งนี้ การเปลี่ยนแปลงสถานะของโทเคนต้องสามารถระบุผลของการดำเนินการได้อย่างชัดเจน และสามารถตรวจสอบย้อนหลังได้

(2) ฟังก์ชันการหยุดและกลับมาดำเนินการโอนโทเคน (Pause and Unpause) : โทเคนควรมีฟังก์ชันสำหรับการหยุดการโอนโทเคนทั้งหมดภายใต้สัญญาอัจฉริยะที่เกี่ยวข้องเป็นการชั่วคราว เพื่อรองรับกรณีที่มีเหตุจำเป็นต้องควบคุมความเสี่ยงหรือ

ป้องกันความเสียหายจากการดำเนินธุรกรรม เช่น การตรวจพบช่องโหว่ของสัญญาอัจฉริยะ เหตุการณ์ด้านความมั่นคงปลอดภัย เป็นต้น โดยฟังก์ชันดังกล่าวควรรองรับการหยุดการโอน (Pause) และการยกเลิกการหยุดการโอน (Unpause) เพื่อให้สามารถกลับมาดำเนินธุรกรรมได้เมื่อเหตุจำเป็นได้รับการแก้ไขหรือสิ้นสุดลง ทั้งนี้ต้องกำหนดผู้มีอำนาจ เงื่อนไข และขอบเขตของการดำเนินการให้ชัดเจน โดยการหยุดการโอนต้องไม่ทำให้ข้อมูลการถือครองสูญหายหรือเปลี่ยนแปลงสิทธิที่ผูกกับหลักทรัพย์นอกเหนือจากเงื่อนไขที่กำหนด และต้องบันทึกเหตุผลและผลของการดำเนินการเพื่อให้สามารถตรวจสอบย้อนหลังได้

(3) ฟังก์ชันการกู้คืนหรือโอนย้ายการถือครองโทเคน (Recovery and Forced Transfer) : โทเคนควรมีฟังก์ชันสำหรับการกู้คืนหรือโอนย้ายการถือครองโทเคน เพื่อรองรับการเปลี่ยนแปลงผู้ถือครองในกรณีที่ไม่สามารถดำเนินการผ่านกระบวนการโอนตามปกติได้ โดยฟังก์ชันดังกล่าวควรรองรับการโอนย้ายการถือครองจากบัญชีหรือข้อมูลที่ใช้ระบุการถือครองโทเคนเดิมไปยังบัญชีหรือข้อมูลที่ใช้ระบุการถือครองโทเคนใหม่ เช่น การกู้คืนการถือครอง (Recovery) การโอนย้ายการถือครองโดยผู้มีอำนาจ (Forced Transfer) หรือการเปลี่ยนบัญชีผู้ถือครอง (Holder Migration) เพื่อรองรับกรณีที่ผู้ลงทุนไม่สามารถเข้าถึงหรือควบคุมกระเป๋าสินทรัพย์ดิจิทัล (Wallet) ได้ การโอนย้ายการถือครองตามคำสั่งของศาลหรือหน่วยงานที่มีอำนาจ หรือกรณีอื่นตามที่กฎหมายหรือเงื่อนไขของหลักทรัพย์กำหนด เป็นต้น ทั้งนี้ ต้องไม่กระทบต่อสิทธิคุณลักษณะ หรือสถานะของโทเคน รวมทั้งต้องสามารถรักษาความถูกต้องของข้อมูลการถือครอง และบันทึกผลของการดำเนินการเพื่อให้สามารถตรวจสอบย้อนหลังได้

(4) ฟังก์ชันการเรียกคืนหรือเพิกถอนโทเคน (Token Recall or Revocation) : โทเคนควรมีฟังก์ชันสำหรับการเรียกคืนหรือเพิกถอนโทเคน เพื่อรองรับการยุติการใช้งานหรือการสิ้นผลของโทเคนตามเหตุหรือเงื่อนไขที่กำหนด โดยฟังก์ชันดังกล่าวควรรองรับการเรียกคืน การเพิกถอน การยกเลิก หรือการยุติการใช้งานของโทเคน เช่น การเรียกคืนโทเคน (Token Recall) การเพิกถอนโทเคน (Token Revocation) หรือการยุติการใช้งานโทเคน (Token Deactivation) รวมทั้งต้องสามารถปรับปรุงข้อมูลของโทเคนที่เกี่ยวข้องให้สอดคล้องกับผลของการดำเนินการได้อย่างถูกต้อง เช่น สถานะของโทเคน จำนวนโทเคน ผู้ถือครอง หรือข้อมูลอื่นที่เกี่ยวข้องกับสิทธิหรือเงื่อนไขของหลักทรัพย์ และสามารถตรวจสอบย้อนหลังได้

(5) ฟังก์ชันการปรับปรุงหรือย้ายสัญญาอัจฉริยะ (Smart Contract Upgrade and Migration) : โทเคนควรมีฟังก์ชันสำหรับการปรับปรุงหรือย้ายสัญญาอัจฉริยะหรือองค์ประกอบของระบบที่เกี่ยวข้อง เพื่อรองรับการแก้ไขข้อบกพร่อง การปรับปรุงการทำงาน หรือการเปลี่ยนแปลงที่จำเป็นตลอดอายุของหลักทรัพย์โทเคน โดยสามารถรักษาความต่อเนื่องของการดำเนินงาน ความถูกต้องของข้อมูลการถือครอง ข้อมูลของโทเคน สิทธิและภาระที่ผูกกับโทเคนก่อนและหลังการดำเนินการ รวมทั้งสามารถบันทึกผลของการดำเนินการเพื่อให้สามารถตรวจสอบย้อนหลังได้

4.2.3 ฟังก์ชันสำหรับการกำกับดูแลและการปฏิบัติตามข้อกำหนด (Compliance Functions)

หลักการทั่วไป

หลักทรัพย์โทเคนควรรองรับฟังก์ชันสำหรับการกำกับดูแลและการปฏิบัติตามข้อกำหนด (Compliance Functions) เพื่อให้สามารถตรวจสอบและบังคับใช้ข้อกำหนด เงื่อนไข และข้อจำกัดที่เกี่ยวข้องกับหลักทรัพย์ได้อย่างเหมาะสมตลอดวงจรชีวิตของหลักทรัพย์ ทั้งนี้ ฟังก์ชันดังกล่าวมีวัตถุประสงค์เพื่อสนับสนุนการปฏิบัติตามกฎหมาย หลักเกณฑ์ ข้อกำหนดของผลิตภัณฑ์ และเงื่อนไขอื่นที่เกี่ยวข้องกับการออก การถือครอง การโอน การใช้สิทธิ และการดำเนินการอื่นที่เกี่ยวข้องกับโทเคน

ฟังก์ชันสำหรับการกำกับดูแลและการปฏิบัติตามข้อกำหนดควรได้รับการออกแบบให้สามารถตรวจสอบคุณสมบัติ สิทธิ และข้อจำกัดที่เกี่ยวข้องกับผู้ถือหรือโทเคน รวมทั้งสามารถบังคับใช้ข้อกำหนดดังกล่าวก่อนที่การดำเนินการหรือธุรกรรมจะมีผล โดยไม่ก่อให้เกิดการดำเนินการที่ขัดต่อกฎหมาย กฎเกณฑ์ หรือเงื่อนไขของหลักทรัพย์

ข้อเสนอแนะขั้นต่ำ

หลักทรัพย์โทเคนควรรองรับฟังก์ชันสำหรับการกำกับดูแลและการปฏิบัติตามข้อกำหนดอย่างน้อย ดังต่อไปนี้

(1) ฟังก์ชันการตรวจสอบคุณสมบัติของผู้ถือ (Investor Eligibility Validation) : โทเคนควรมีฟังก์ชันสำหรับการตรวจสอบคุณสมบัติของผู้ถือ เพื่อรองรับการกำหนดและตรวจสอบว่าผู้ถือหรือผู้ที่เกี่ยวข้องกับธุรกรรมมีคุณสมบัติเป็นไปตามกฎหมาย กฎเกณฑ์ หรือเงื่อนไขของหลักทรัพย์ก่อนที่การดำเนินการหรือธุรกรรมจะมีผล

ฟังก์ชันดังกล่าว อย่างน้อยต้องสามารถกำหนดบัญชีหรือข้อมูลที่ใช้ระบุการถือครองโทเคนที่ได้รับอนุญาต (Whitelist) และบัญชีหรือข้อมูลที่ใช้ระบุการถือครองโทเคนที่ถูกจำกัดหรือห้ามดำเนินการ (Blacklist) เพื่อใช้เป็นข้อมูลอ้างอิงในการตรวจสอบสิทธิของผู้ถือหรือผู้ที่เกี่ยวข้องกับธุรกรรมก่อนที่การดำเนินการหรือธุรกรรมจะมีผล โดยระบบควรรองรับการเพิ่ม แก้ไข ระงับ หรือเพิกถอนข้อมูลดังกล่าวตามการ

เปลี่ยนแปลงของคุณสมบัติผู้ถือ กฎหมาย กฎเกณฑ์ หรือเงื่อนไขของหลักทรัพย์ รวมทั้งสามารถนำข้อมูลดังกล่าวไปใช้ในการบังคับใช้ข้อกำหนดที่เกี่ยวข้องได้อย่างถูกต้อง และสามารถบันทึกผลของการดำเนินการเพื่อให้สามารถตรวจสอบย้อนหลังได้ ทั้งนี้ ระบบอาจรองรับการตรวจสอบคุณสมบัติหรือเงื่อนไขอื่นเพิ่มเติม เช่น ประเภทผู้ลงทุน (Investor Type) สถานะการมีสิทธิถือครองหลักทรัพย์ (Eligibility Status) ถิ่นที่อยู่หรือสัญชาติ (Jurisdiction) หรือข้อกำหนดอื่นตามกฎหมาย กฎเกณฑ์ หรือเงื่อนไขของหลักทรัพย์

(2) ฟังก์ชันการตรวจสอบเงื่อนไขของธุรกรรม (Transaction Validation) : โทเคนควรมีฟังก์ชันสำหรับการตรวจสอบว่าการดำเนินการหรือธุรกรรมเป็นไปตามกฎหมาย กฎเกณฑ์ และเงื่อนไขของหลักทรัพย์ ก่อนที่การดำเนินการหรือธุรกรรมจะมีผล เพื่อป้องกันการดำเนินการที่ไม่เป็นไปตามข้อกำหนดและรักษาความถูกต้องของการถือครองหลักทรัพย์โทเคน โดยฟังก์ชันดังกล่าวควรรองรับการตรวจสอบเงื่อนไขที่เกี่ยวข้องกับธุรกรรมก่อนการดำเนินการ ตามกฎหมาย กฎเกณฑ์ หรือเงื่อนไขของหลักทรัพย์ เช่น ข้อจำกัดในการโอน (Transfer Restriction) ระยะเวลาห้ามโอน (Lock-up Period) เพดานการถือครอง (Holding Limit) จำนวนผู้ถือครอง (Number of Holders) หรือเงื่อนไขอื่นที่เกี่ยวข้อง รวมทั้งสามารถปฏิเสธหรือไม่อนุญาตให้ธุรกรรมมีผลเมื่อไม่เป็นไปตามเงื่อนไขที่กำหนด และสามารถบันทึกผลของการตรวจสอบเพื่อให้สามารถตรวจสอบย้อนหลังได้

4.2.4 ฟังก์ชันเพิ่มเติม (Additional / Optional Functions)

หลักการทั่วไป

หลักทรัพย์โทเคนอาจรองรับฟังก์ชันเพิ่มเติมเพื่อสนับสนุนลักษณะเฉพาะของผลิตภัณฑ์ ความต้องการทางธุรกิจ หรือการออกแบบระบบ ทั้งนี้ ฟังก์ชันดังกล่าวมีวัตถุประสงค์เพื่อเพิ่มประสิทธิภาพ ความยืดหยุ่น และความสามารถในการรองรับกรณีการใช้งานที่หลากหลายของหลักทรัพย์โทเคน ตลอดจนสนับสนุนการดำเนินการตามสิทธิ หน้าที่ และเงื่อนไขของหลักทรัพย์ได้อย่างเหมาะสม

ฟังก์ชันเพิ่มเติมควรได้รับการออกแบบให้สอดคล้องกับลักษณะของผลิตภัณฑ์ วัตถุประสงค์ของการใช้งาน และข้อกำหนดทางธุรกิจ รวมทั้งไม่กระทบต่อความถูกต้อง ความน่าเชื่อถือ และความสามารถในการตรวจสอบย้อนหลังของการดำเนินงาน ทั้งนี้ หลักทรัพย์โทเคนอาจกำหนดฟังก์ชันเพิ่มเติมดังต่อไปนี้

(1) ฟังก์ชันการบันทึกสถานะ ณ เวลาใดเวลาหนึ่ง (Snapshot) : โทเคนอาจมีฟังก์ชันสำหรับการบันทึกสถานะการถือครองหรือข้อมูลที่เกี่ยวข้อง ณ เวลาใดเวลาหนึ่ง (Snapshot) เพื่อใช้เป็นข้อมูลอ้างอิงสำหรับการดำเนินการที่ต้องอาศัยข้อมูล ณ จุด

เวลาเฉพาะ เช่น การกำหนดสิทธิ การคำนวณสิทธิ การจ่ายผลตอบแทน การดำเนินการเกี่ยวกับสิทธิของผู้ถือหลักทรัพย์ หรือการดำเนินการอื่นตามเงื่อนไขของผลิตภัณฑ์

หากหลักทรัพย์โทเคนรองรับฟังก์ชันดังกล่าว ควรรองรับการกำหนดหรือระบุช่วงเวลาที่ใช้ในการบันทึกข้อมูลได้อย่างชัดเจน และสามารถเรียกใช้ข้อมูลที่บันทึกไว้เป็นข้อมูลอ้างอิงได้อย่างถูกต้อง โดยไม่กระทบต่อความถูกต้องของข้อมูลที่เกิดขึ้นภายหลัง รวมทั้งสามารถตรวจสอบย้อนหลังได้

(2) **ฟังก์ชันการแยกสถานะ สิทธิ หรือข้อจำกัดของโทเคน (Partition or Segregation) :** ฟังก์ชันดังกล่าวใช้สำหรับแยกสถานะ สิทธิ หรือข้อจำกัดของโทเคนออกเป็นส่วนย่อย เพื่อให้สามารถบริหารจัดการโทเคนแต่ละส่วนที่อยู่ภายใต้เงื่อนไขหรือข้อกำหนดที่แตกต่างกันได้อย่างชัดเจน เช่น โทเคนที่อยู่ภายใต้ภาระผูกพัน โทเคนที่ถูกอายัดหรือระงับการโอน โทเคนที่มีข้อจำกัดในการถือครองหรือการโอน หรือโทเคนที่มีสิทธิหรือเงื่อนไขเฉพาะตามลักษณะของผลิตภัณฑ์

หากหลักทรัพย์โทเคนรองรับฟังก์ชันดังกล่าว ควรสามารถกำหนด ระบุ และบริหารจัดการสถานะ สิทธิ หรือข้อจำกัดของโทเคนแต่ละส่วนได้อย่างชัดเจน โดยไม่กระทบต่อสถานะ สิทธิ หรือข้อจำกัดของโทเคนส่วนอื่น รวมทั้งสามารถตรวจสอบและติดตามข้อมูลที่เกี่ยวข้องได้ตลอดอายุของโทเคน

(3) **ฟังก์ชันการดำเนินการแบบกลุ่ม (Batch Operation) :** ฟังก์ชันดังกล่าวใช้สำหรับดำเนินการหรือประมวลผลรายการหลายรายการภายใต้กระบวนการเดียว เพื่อเพิ่มประสิทธิภาพในการดำเนินงาน ลดขั้นตอนการดำเนินการซ้ำ และสนับสนุนการดำเนินธุรกรรมที่มีลักษณะเดียวกันในคราวเดียว เช่น การโอนโทเคนหลายรายการ การปรับปรุงข้อมูลหรือสถานะของโทเคนหลายรายการ หรือการดำเนินการอื่นที่เกี่ยวข้อง

หากหลักทรัพย์โทเคนรองรับฟังก์ชันดังกล่าว ควรสามารถระบุผลของการดำเนินการในแต่ละรายการได้อย่างชัดเจน โดยไม่กระทบต่อความถูกต้องของรายการอื่น รวมทั้งสามารถบันทึกและตรวจสอบผลของการดำเนินการย้อนหลังได้

(4) ฟังก์ชันเพิ่มเติมอื่น (Other Additional Functions) : ฟังก์ชันดังกล่าวใช้สำหรับรองรับความสามารถเพิ่มเติมของหลักทรัพย์โทเคนที่มีลักษณะเฉพาะตามผลิตภัณฑ์ ความต้องการทางธุรกิจ หรือกรณีการใช้งานที่เฉพาะเจาะจง ซึ่งไม่อยู่ภายใต้ฟังก์ชันที่กำหนดไว้ข้างต้น เช่น ฟังก์ชันสำหรับการใช้สิทธิออกเสียง (Voting Function) ฟังก์ชันสำหรับการจ่ายผลตอบแทนหรือสิทธิประโยชน์ (Distribution Function) ฟังก์ชันสำหรับการแปลงสิทธิหรือเปลี่ยนแปลงสถานะของโทเคนตามเงื่อนไขของผลิตภัณฑ์ (Conversion Function) หรือฟังก์ชันอื่นที่เกี่ยวข้อง

หากหลักทรัพย์โทเคนรองรับฟังก์ชันดังกล่าว ควรมีการกำหนดวัตถุประสงค์ ขอบเขต เงื่อนไข และผลของการดำเนินการไว้อย่างชัดเจน รวมทั้งต้องสามารถดำเนินการได้อย่างถูกต้อง สอดคล้องกับกฎหมาย กฎเกณฑ์ และเงื่อนไขของหลักทรัพย์ ตลอดจนสามารถตรวจสอบย้อนหลังได้

4.3 ข้อกำหนดด้านข้อมูลของโทเคน (Token Data Requirements)

ข้อมูลของหลักทรัพย์โทเคนและข้อมูลอ้างอิงที่เกี่ยวข้องเป็นองค์ประกอบสำคัญที่ใช้ระบุตัวตนของโทเคน แสดงคุณลักษณะ สิทธิ และเงื่อนไขของหลักทรัพย์ที่โทเคนเป็นตัวแทน รวมถึงสนับสนุนการออกเสนอขาย การถือครอง การโอน การใช้สิทธิ การตรวจสอบ และการแลกเปลี่ยนข้อมูลระหว่างผู้เกี่ยวข้องและโครงสร้างพื้นฐานต่าง ๆ ตลอดวงจรชีวิตของหลักทรัพย์ ทั้งนี้ ข้อมูลดังกล่าวอาจจัดเก็บหรืออ้างอิงจากระบบ Distributed Ledger Technology (DLT) หรือ Blockchain ระบบภายนอก หรือทั้งสองรูปแบบร่วมกัน (Hybrid) โดยควรสามารถเชื่อมโยงกับโทเคนได้อย่างน่าเชื่อถือ ตรวจสอบได้ และสะท้อนสาระสำคัญของหลักทรัพย์ได้อย่างถูกต้อง

หัวข้อนี้กำหนดหลักการเกี่ยวกับข้อมูลที่หลักทรัพย์โทเคนควรรองรับ โดยครอบคลุมข้อมูลหลักของโทเคน (Core Token Data) ข้อมูลอ้างอิงและเอกสารที่เกี่ยวข้อง (Reference Information) และการกำกับดูแลข้อมูลของโทเคน (Token Data Governance) เพื่อให้ข้อมูลมีความถูกต้อง ครบถ้วน สอดคล้องกัน และสามารถตรวจสอบย้อนหลังได้ตลอดวงจรชีวิตของหลักทรัพย์ ทั้งนี้ มาตรฐานฉบับนี้มุ่งเน้นการกำหนดประเภทและหลักการของข้อมูลที่หลักทรัพย์โทเคนควรรองรับ มากกว่าการกำหนดรูปแบบการจัดเก็บ โครงสร้างข้อมูล หรือมาตรฐานทางเทคนิคเฉพาะ จึงไม่จำกัดว่าข้อมูลดังกล่าวจะจัดเก็บในรูปแบบ on-chain, off-chain หรือ hybrid ตราบเท่าที่สามารถเชื่อมโยงหรืออ้างอิงข้อมูลและเอกสารที่เกี่ยวข้อง รวมทั้งบริหารจัดการข้อมูลได้อย่างน่าเชื่อถือโดยไม่ก่อให้เกิดความคลาดเคลื่อนเกี่ยวกับคุณลักษณะ สิทธิ เงื่อนไข หรือสถานะของหลักทรัพย์โทเคน

4.3.1 ข้อมูลหลักของโทเคน (Core Token Data)

หลักการทั่วไป

หลักทรัพย์โทเคนควรรองรับข้อมูลหลักของโทเคน (Core Token Data) ที่จำเป็นสำหรับการระบุตัวตนของโทเคน การแสดงคุณลักษณะ สิทธิ และเงื่อนไขที่เป็นสาระสำคัญของหลักทรัพย์ที่โทเคนเป็นตัวแทน รวมทั้งสนับสนุนการดำเนินการที่เกี่ยวข้องตลอดวงจรชีวิตของหลักทรัพย์ เพื่อให้ผู้เกี่ยวข้องสามารถอ้างอิงและตีความหลักทรัพย์ที่โทเคนเป็นตัวแทนได้อย่างถูกต้องและสอดคล้องกัน

ข้อมูลหลักของโทเคนอาจจัดเก็บบนระบบ Distributed Ledger Technology (DLT) หรือ Blockchain จัดเก็บในระบบภายนอก หรือจัดเก็บในลักษณะผสมผสาน (Hybrid) ได้ตามความเหมาะสม โดยไม่จำกัดรูปแบบหรือสถานที่จัดเก็บ ตราบเท่าที่สามารถเชื่อมโยงข้อมูลดังกล่าวกับโทเคนได้อย่างถูกต้อง น่าเชื่อถือ และสามารถใช้อ้างอิงได้ตลอดวงจรชีวิตของหลักทรัพย์

ข้อเสนอแนะขั้นต่ำ

หลักทรัพย์โทเคนควรรองรับข้อมูลหลักอย่างน้อย ดังต่อไปนี้

(1) **ข้อมูลระบุตัวตนของโทเคน (Token Identifier) :** หลักทรัพย์โทเคนควรรองรับข้อมูลที่ใช้ระบุตัวตนของโทเคน (Token Identifier) เพื่อให้สามารถระบุ อ้างอิง และเชื่อมโยงโทเคนกับข้อมูลที่เกี่ยวข้องได้อย่างถูกต้องตลอดวงจรชีวิตของหลักทรัพย์
ตัวอย่าง : Token Identifier, Contract Address, Token ID หรือข้อมูลอื่นที่สามารถใช้ระบุตัวตนของโทเคนได้อย่างเป็นเอกลักษณ์

(2) **ข้อมูลอ้างอิงหลักทรัพย์ (Security Reference Information) :** หลักทรัพย์โทเคนควรรองรับข้อมูลที่ใช้ระบุหรืออ้างอิงหลักทรัพย์ที่โทเคนเป็นตัวแทน เพื่อให้สามารถเชื่อมโยงโทเคนกับหลักทรัพย์ได้อย่างถูกต้อง และสนับสนุนการอ้างอิงข้อมูลหรือการดำเนินการที่เกี่ยวข้องตลอดวงจรชีวิตของหลักทรัพย์
ตัวอย่าง : Security Identifier, ISIN, Internal Security ID, Issue ID หรือข้อมูลอื่นที่ใช้ระบุหรืออ้างอิงหลักทรัพย์

(3) **ข้อมูลผู้ออกหลักทรัพย์ (Issuer Information) :** หลักทรัพย์โทเคนควรรองรับข้อมูลที่ใช้ระบุผู้ออกหลักทรัพย์ เพื่อให้สามารถเชื่อมโยงโทเคนกับผู้ออกหลักทรัพย์ได้อย่างถูกต้อง และสนับสนุนการอ้างอิงข้อมูลหรือการดำเนินการที่เกี่ยวข้องตลอดวงจรชีวิตของหลักทรัพย์
ตัวอย่าง : ชื่อผู้ออกหลักทรัพย์ (Issuer Name), Legal Entity Identifier (LEI), เลขทะเบียนนิติบุคคล หรือข้อมูลอื่นที่ใช้ระบุผู้ออกหลักทรัพย์

(4) ข้อมูลคุณลักษณะของหลักทรัพย์ (Security Attributes) : หลักทรัพย์โทเคนควรรองรับข้อมูลที่ใช้แสดงคุณลักษณะพื้นฐานของหลักทรัพย์ที่โทเคนเป็นตัวแทน เพื่อให้ผู้เกี่ยวข้องสามารถระบุประเภทและลักษณะสำคัญของหลักทรัพย์ได้อย่างถูกต้อง และสนับสนุนการอ้างอิงข้อมูลหรือการดำเนินการที่เกี่ยวข้องตลอดวงจรชีวิตของหลักทรัพย์

ตัวอย่าง : ประเภทของหลักทรัพย์ (หุ้นกู้ หน่วยลงทุน เป็นต้น) สกุลเงิน หน่วยของหลักทรัพย์ จำนวนหลักทรัพย์ที่ออก หรือข้อมูลพื้นฐานอื่นที่เกี่ยวข้อง

(5) ข้อมูลสิทธิและเงื่อนไขของหลักทรัพย์ (Rights and Terms Information) : หลักทรัพย์โทเคนควรรองรับข้อมูลที่ใช้แสดงหรืออ้างอิงสิทธิ หน้าที่ และเงื่อนไขที่เป็นสาระสำคัญของหลักทรัพย์ที่โทเคนเป็นตัวแทน เพื่อให้ผู้เกี่ยวข้องสามารถรับทราบและใช้สิทธิ รวมทั้งปฏิบัติตามเงื่อนไขของหลักทรัพย์ได้อย่างถูกต้องตลอดวงจรชีวิตของหลักทรัพย์

ตัวอย่าง : สิทธิออกเสียง สิทธิรับเงินปันผล สิทธิรับดอกเบี้ย เงื่อนไขการไถ่ถอน วันครบกำหนด สิทธิในการแปลงสภาพ หรือเงื่อนไขสำคัญอื่นของหลักทรัพย์

4.3.2 ข้อมูลอ้างอิงและเอกสารที่เกี่ยวข้อง (Reference Information)

หลักการทั่วไป

หลักทรัพย์โทเคนควรรองรับการเชื่อมโยงหรือการอ้างอิงข้อมูลและเอกสารที่เกี่ยวข้องกับหลักทรัพย์ที่โทเคนเป็นตัวแทน เพื่อสนับสนุนการเปิดเผยข้อมูล การทำความเข้าใจคุณลักษณะ สิทธิ และเงื่อนไขของหลักทรัพย์ การใช้สิทธิ การตรวจสอบ และการปฏิบัติตามกฎหมายหรือข้อกำหนดที่เกี่ยวข้อง โดยการเชื่อมโยงหรือการอ้างอิงดังกล่าวควรสามารถระบุความสัมพันธ์ระหว่างโทเคนกับข้อมูลหรือเอกสารที่เกี่ยวข้องได้อย่างชัดเจน ถูกต้อง และตรวจสอบได้

ข้อมูลและเอกสารดังกล่าวอาจจัดเก็บบนระบบ Distributed Ledger Technology (DLT) หรือ Blockchain จัดเก็บในระบบภายนอก หรือจัดเก็บในลักษณะผสมผสาน (Hybrid) ได้ตามความเหมาะสม โดยไม่จำเป็นต้องจัดเก็บข้อมูลหรือเอกสารทั้งหมดไว้บนระบบ DLT หรือ Blockchain ตราบเท่าที่สามารถเชื่อมโยงหรืออ้างอิงกลับมายังโทเคนได้อย่างถูกต้อง น่าเชื่อถือ และรองรับการอ้างอิงได้ตลอดวงจรชีวิตของหลักทรัพย์

ข้อเสนอแนะขั้นต่ำ

หลักทรัพย์โทเคนควรรองรับการเชื่อมโยงหรือการอ้างอิงข้อมูลและเอกสารที่เกี่ยวข้องกับหลักทรัพย์อย่างเหมาะสม ดังต่อไปนี้

(1) ข้อมูลหรือเอกสารที่ควรเชื่อมโยงกับโทเคน : หลักทรัพย์โทเคนควรรองรับการเชื่อมโยงหรือการอ้างอิงข้อมูลหรือเอกสารที่มีนัยสำคัญต่อสิทธิ หน้าที่ เงื่อนไข

การออกและการเสนอขาย การเปิดเผยข้อมูล หรือข้อมูลอื่นที่เกี่ยวข้องกับหลักทรัพย์ตามกฎหมายหรือข้อกำหนดที่เกี่ยวข้อง เพื่อให้ผู้เกี่ยวข้องสามารถเข้าถึง อ้างอิง และตรวจสอบข้อมูลที่เกี่ยวข้องได้อย่างเหมาะสมตลอดวงจรชีวิตของหลักทรัพย์

ตัวอย่าง : ข้อกำหนดสิทธิ หนังสือชี้ชวน แบบแสดงรายการข้อมูลการเสนอขาย เอกสารหรือข้อมูลเกี่ยวกับการออกและการเสนอขาย ประกาศเกี่ยวกับการดำเนินการของหลักทรัพย์ (Corporate Action Notice) หรือเอกสารอื่นตามที่กฎหมายหรือข้อกำหนดที่เกี่ยวข้องกำหนด

(2) การเชื่อมโยงและการอ้างอิงข้อมูลหรือเอกสาร : หลักทรัพย์โทเคนควรรองรับการเชื่อมโยงหรือการอ้างอิงข้อมูลหรือเอกสารที่เกี่ยวข้องในลักษณะที่สามารถระบุได้อย่างชัดเจนว่าข้อมูลหรือเอกสารดังกล่าวเกี่ยวข้องกับหลักทรัพย์โทเคนใด หรือการออกหลักทรัพย์ครั้งใด และสามารถเชื่อมโยงกลับไปยังแหล่งข้อมูลหรือระบบจัดเก็บที่เกี่ยวข้องได้อย่างถูกต้อง น่าเชื่อถือ และตรวจสอบได้

ทั้งนี้ การเชื่อมโยงหรือการอ้างอิงดังกล่าวอาจดำเนินการโดยใช้ตัวระบุ (Identifier) ตัวชี้ตำแหน่งข้อมูล (Pointer) ลิงก์ (Link) รหัสอ้างอิง ค่าแฮช (Hash) หรือกลไกอื่นที่ให้ผลเทียบเท่า ทั้งนี้ โดยไม่จำกัดรูปแบบหรือเทคโนโลยีที่ใช้

ตัวอย่าง : Uniform Resource Identifier (URI)[3], Document Identifier, Document Hash, Uniform Resource Name (URN) [4] หรือกลไกอื่นที่สามารถเชื่อมโยงหรืออ้างอิงข้อมูลหรือเอกสารได้อย่างน่าเชื่อถือ

4.3.3 การกำกับดูแลข้อมูลของโทเคน (Token Data Governance)

หลักการทั่วไป

ข้อมูลของหลักทรัพย์โทเคน รวมถึงข้อมูลอ้างอิงและเอกสารที่เชื่อมโยงกับโทเคน ควรได้รับการกำกับดูแลและบริหารจัดการอย่างเหมาะสมตลอดวงจรชีวิตของหลักทรัพย์ เพื่อให้ข้อมูลมีความถูกต้อง ครบถ้วน สอดคล้องกัน น่าเชื่อถือ และสามารถตรวจสอบย้อนหลังได้ ทั้งนี้ การกำกับดูแลข้อมูลควรครอบคลุมการกำหนดแหล่งข้อมูลหลัก (Authoritative Source) การรักษาความสอดคล้องของข้อมูลระหว่างระบบ และการบริหารจัดการการเปลี่ยนแปลงและเวอร์ชันของข้อมูล

[3] Uniform Resource Identifier (URI) คือ ข้อความตามรูปแบบมาตรฐานที่ใช้ระบุสิ่งที่ต้องการอ้างถึง เช่น เอกสาร หรือข้อมูล

[4] Uniform Resource Name (URN) คือ URI ที่ใช้ชื่ออ้างอิงเพื่อระบุสิ่งใดสิ่งหนึ่งอย่างถาวร โดยไม่มีการเปลี่ยนแปลง

ในกรณีที่ข้อมูลหรือเอกสารที่เกี่ยวข้องกับหลักทรัพย์มีการแก้ไขเพิ่มเติม เปลี่ยนแปลง หรือมีข้อมูลจากหลายแหล่ง ระบบควรมีกลไกที่เหมาะสมเพื่อให้สามารถระบุแหล่งข้อมูลที่ใช้ยึดถือ ตรวจสอบความถูกต้องและความสอดคล้องของข้อมูล รวมทั้งสามารถติดตามและตรวจสอบประวัติการเปลี่ยนแปลงข้อมูลได้ตลอดวงจรชีวิตของหลักทรัพย์

ข้อเสนอแนะขั้นต่ำ

หลักทรัพย์โทเคนควรมีกลไกในการกำกับดูแลและบริหารจัดการข้อมูลของโทเคน รวมถึงข้อมูลอ้างอิงและเอกสารที่เชื่อมโยงกับโทเคนอย่างเหมาะสม ดังต่อไปนี้

(1) การกำหนดแหล่งข้อมูลหลัก (Authoritative Source) : หลักทรัพย์โทเคนควรกำหนดแหล่งข้อมูลหลัก (Authoritative Source) สำหรับข้อมูลแต่ละประเภทอย่างชัดเจน เพื่อใช้เป็นข้อมูลอ้างอิงที่ถูกต้องในกรณีที่ข้อมูลเดียวกันปรากฏอยู่ในหลายระบบ หลายแหล่ง หรือหลายรูปแบบ และเพื่อป้องกันความคลาดเคลื่อนที่อาจส่งผลต่อคุณลักษณะ สิทธิ เงื่อนไข หรือสถานะของหลักทรัพย์

ในกรณีที่ข้อมูลเดียวกันปรากฏทั้งบนระบบ DLT/Blockchain และระบบภายนอก เช่น ระบบทะเบียนหลักทรัพย์ หรือระบบงานภายในของผู้ออกหลักทรัพย์ ควรกำหนดให้ชัดเจนว่าระบบใดเป็นแหล่งข้อมูลหลัก (Authoritative Source) ที่ใช้ยึดถือเมื่อเกิดกรณีที่ข้อมูลไม่สอดคล้องกัน

(2) ความสอดคล้องของข้อมูล (Data Consistency) : หลักทรัพย์โทเคนควรมีกลไกในการรักษาความสอดคล้องของข้อมูลระหว่างข้อมูลของโทเคน ข้อมูลอ้างอิง เอกสารที่เกี่ยวข้อง และระบบที่เกี่ยวข้อง เพื่อให้ข้อมูลที่ใช้ในการออก การถือครอง การโอน การใช้สิทธิ และการดำเนินการอื่นเกี่ยวกับหลักทรัพย์มีความถูกต้อง สอดคล้องกัน และไม่ก่อให้เกิดความคลาดเคลื่อนหรือข้อโต้แย้งจากข้อมูลที่ไม่ตรงกัน

ในกรณีที่ข้อมูลเดียวกันปรากฏอยู่ในหลายระบบหรือหลายแหล่ง ระบบควรมีกลไกในการตรวจสอบ ระบุ และจัดการความไม่สอดคล้องของข้อมูลตามแหล่งข้อมูลหลัก (Authoritative Source) ที่กำหนดไว้

(3) การบริหารจัดการการเปลี่ยนแปลงและเวอร์ชันของข้อมูล (Data Change and Version Management) : หลักทรัพย์โทเคนควรมีกลไกในการบริหารจัดการการเปลี่ยนแปลงข้อมูลของโทเคน รวมถึงข้อมูลอ้างอิงและเอกสารที่เชื่อมโยงกับโทเคน เพื่อให้ข้อมูลมีความถูกต้อง สอดคล้องกัน และสามารถใช้อ้างอิงได้อย่างต่อเนื่องตลอดวงจรชีวิตของหลักทรัพย์

ในกรณีที่มีการแก้ไขเพิ่มเติม ปรับปรุง หรือเปลี่ยนแปลงข้อมูลหรือเอกสารที่เกี่ยวข้อง ระบบควรรองรับการระบุเวอร์ชัน สถานะการใช้บังคับ และการปรับปรุงข้อมูลหรือการเชื่อมโยงที่เกี่ยวข้อง เพื่อให้สามารถอ้างอิงข้อมูลหรือเอกสารที่ถูกต้องและใช้บังคับอยู่ในขณะนั้นได้อย่างถูกต้องและต่อเนื่อง

4.4 ข้อกำหนดด้านการทำงานร่วมกันระหว่างระบบ (Interoperability Requirements)

หลักทรัพย์โทเคนควรได้รับการออกแบบโดยคำนึงถึงความสามารถในการทำงานร่วมกันระหว่างระบบ (Interoperability) ตามความเหมาะสมกับวัตถุประสงค์ ลักษณะของผลิตภัณฑ์ และการใช้งาน เพื่อรองรับการเชื่อมโยงและการดำเนินงานร่วมกับผู้เกี่ยวข้อง ระบบ และโครงสร้างพื้นฐานที่เกี่ยวข้องตลอดวงจรชีวิตของหลักทรัพย์ ซึ่งอาจครอบคลุมตั้งแต่การออก การเสนอขาย การถือครอง การโอน การซื้อขาย การชำระราคาและส่งมอบหลักทรัพย์ การใช้สิทธิ ตลอดจนการสิ้นผลของหลักทรัพย์ ทั้งนี้ การออกแบบดังกล่าวควรมุ่งให้ข้อมูล เหตุการณ์ สถานะ และผลของการดำเนินการสามารถแลกเปลี่ยน ตีความ และประมวลผลระหว่างระบบได้อย่างถูกต้องและสอดคล้องกัน โดยไม่กระทบต่อสิทธิ เงื่อนไข คุณลักษณะ หรือสถานะของหลักทรัพย์โทเคน

การเตรียมความพร้อมด้านการทำงานร่วมกันระหว่างระบบ (Interoperability Readiness) ควรครอบคลุมการกำหนดขอบเขตของการทำงานร่วมกัน การจัดทำข้อกำหนดทางเทคนิค การกำหนดแนวทางการดำเนินงานร่วมกัน และการกำกับดูแลการทำงานร่วมกัน โดยมุ่งให้หลักทรัพย์โทเคนได้รับการออกแบบในลักษณะที่ไม่ปิดกั้นการเพิ่มผู้เกี่ยวข้อง การเชื่อมโยงกับระบบหรือโครงสร้างพื้นฐานอื่น หรือการรองรับมาตรฐานที่อาจเกิดขึ้นในอนาคต ทั้งนี้ มิได้หมายความว่าหลักทรัพย์โทเคนจะต้องรองรับการเชื่อมโยงกับทุกระบบหรือทุกกรณีการใช้งานตั้งแต่เริ่มต้น แต่ควรคำนึงถึงวัตถุประสงค์ ลักษณะการใช้งาน ความจำเป็น และความเสี่ยงที่เกี่ยวข้องในการกำหนดระดับของการทำงานร่วมกันอย่างเหมาะสม

4.4.1 การกำหนดขอบเขตการทำงานร่วมกัน (Defining the Interoperability Scope)

หลักการทั่วไป

การกำหนดขอบเขตการทำงานร่วมกันเป็นพื้นฐานสำคัญในการออกแบบหลักทรัพย์โทเคน เพื่อกำหนดว่าหลักทรัพย์โทเคนควรรองรับกิจกรรมใด เกี่ยวข้องกับผู้มีส่วนเกี่ยวข้องใด และอาจต้องทำงานร่วมกับระบบหรือโครงสร้างพื้นฐานใดตลอดวงจรชีวิตของหลักทรัพย์ ทั้งนี้ ขอบเขตดังกล่าวควรกำหนดให้สอดคล้องกับวัตถุประสงค์และลักษณะของหลักทรัพย์ รวมถึงความจำเป็นและความเสี่ยงที่เกี่ยวข้อง โดยอาจครอบคลุมทั้งการทำงานร่วมกันในปัจจุบันและที่อาจเกิดขึ้นในอนาคต

ข้อเสนอแนะขั้นต่ำ

การกำหนดขอบเขตการทำงานร่วมกันควรพิจารณาอย่างน้อยในประเด็นดังต่อไปนี้

(1) กิจกรรมทางธุรกิจ (Business Activities) : ควรพิจารณากิจกรรมและกระบวนการตลอดวงจรชีวิตของหลักทรัพย์ที่หลักทรัพย์โทเคนรองรับหรืออาจต้องเกี่ยวข้อง รวมถึงวัตถุประสงค์และผลลัพธ์ที่ต้องการ ของแต่ละกิจกรรม

ตัวอย่าง : ผู้ออกหลักทรัพย์โทเคนที่มีวัตถุประสงค์ในการเสนอขาย ซื้อขาย หรือชำระราคาและส่งมอบหลักทรัพย์โทเคนผ่านหลายแพลตฟอร์มหรือหลายโครงสร้างพื้นฐาน อาจกำหนดให้กิจกรรมการเสนอขาย การซื้อขาย การชำระราคาและส่งมอบหลักทรัพย์ และการปรับปรุงทะเบียนผู้ถือหลักทรัพย์ เป็นกิจกรรมที่อยู่ในขอบเขตของการทำงานร่วมกัน

(2) ผู้เกี่ยวข้อง (Participants) : ควรพิจารณาผู้เกี่ยวข้องที่มีหรืออาจมีบทบาทในกิจกรรมที่อยู่ในขอบเขตของการทำงานร่วมกัน รวมถึงบทบาท ความรับผิดชอบ และลักษณะของการมีส่วนร่วมของผู้เกี่ยวข้องแต่ละฝ่าย ตลอดจนความจำเป็นในการประสานงานหรือดำเนินงานร่วมกันระหว่างผู้เกี่ยวข้องดังกล่าว

ตัวอย่าง : ผู้ออกหลักทรัพย์โทเคนที่มีวัตถุประสงค์ให้บริการหลายแพลตฟอร์มหรือหลายโครงสร้างพื้นฐานตามตัวอย่างก่อนหน้านี้ อาจพิจารณาผู้เกี่ยวข้องให้ครอบคลุม เช่น ผู้จัดจำหน่ายหลักทรัพย์ นายหน้าซื้อขายหรือผู้ค้าหลักทรัพย์ ศูนย์ซื้อขายหลักทรัพย์ นายทะเบียนหลักทรัพย์ รวมถึงผู้ให้บริการโครงสร้างพื้นฐานที่เกี่ยวข้อง เป็นต้น

(3) ระบบหรือโครงสร้างพื้นฐาน (Systems and Infrastructure) : ควรพิจารณาระบบหรือโครงสร้างพื้นฐานที่หลักทรัพย์โทเคนใช้งาน เชื่อมโยง หรืออาจต้องทำงานร่วมกัน เพื่อสนับสนุนกิจกรรมที่อยู่ในขอบเขตของการทำงานร่วมกัน รวมถึงบทบาทหน้าที่ และความเกี่ยวข้องของแต่ละระบบหรือโครงสร้างพื้นฐาน ตลอดจนความสัมพันธ์ระหว่างระบบที่เกี่ยวข้องกับการดำเนินงาน

ตัวอย่าง : การทำงานร่วมกันอาจเกิดขึ้นระหว่างเครือข่าย DLT หรือ Blockchain หลายเครือข่าย หรือระหว่างเครือข่าย DLT หรือ Blockchain กับระบบหรือโครงสร้างพื้นฐานแบบดั้งเดิม (Legacy Systems) เช่น ระบบซื้อขาย ระบบนายทะเบียน ระบบรับฝากหลักทรัพย์ ระบบชำระราคาและส่งมอบหลักทรัพย์ หรือระบบอื่นที่เกี่ยวข้อง

4.4.2 ข้อกำหนดทางเทคนิคเพื่อการทำงานร่วมกัน (Interoperability Technical Specifications)

หลักการทั่วไป

การทำงานร่วมกันทางเทคนิคควรทำให้ข้อมูล ข้อความ คำสั่ง เหตุการณ์ และสถานะของหลักทรัพย์โทเคนที่แลกเปลี่ยนระหว่างระบบมีรูปแบบ ความหมาย และผลของการประมวลผลที่สอดคล้องกัน เพื่อให้แต่ละระบบสามารถแลกเปลี่ยน ตีความ และประมวลผลข้อมูลได้อย่างถูกต้อง โดยไม่กระทบต่อสิทธิ สถานะ จำนวน หรือผลของการดำเนินการที่เกี่ยวข้องกับหลักทรัพย์โทเคน

ข้อกำหนดทางเทคนิคควรกำหนดรายละเอียดที่จำเป็นสำหรับการทำงานร่วมกันระหว่างระบบอย่างชัดเจนและสอดคล้องกัน โดยควรพิจารณาใช้มาตรฐานหรือข้อกำหนดที่ได้รับการยอมรับและมีการใช้งานอยู่แล้ว หรือกำหนดกลไกที่เหมาะสมเพื่อรองรับการทำงานร่วมกับระบบหรือมาตรฐานอื่น ทั้งนี้ ไม่จำเป็นต้องกำหนดให้ทุกระบบใช้เทคโนโลยี โครงสร้างข้อมูล หรือวิธีการเชื่อมต่อเดียวกัน หากยังสามารถแลกเปลี่ยน ตีความ และประมวลผลข้อมูลได้อย่างถูกต้องและเหมาะสมสอดคล้องกัน

ข้อเสนอแนะขั้นต่ำ

การจัดทำข้อกำหนดทางเทคนิคเพื่อการทำงานร่วมกัน ควรพิจารณาอย่างน้อยในประเด็นดังต่อไปนี้

(1) แบบจำลองข้อมูลและโครงสร้างข้อมูล (Data Models and Data Structures) : ควรกำหนดองค์ประกอบ โครงสร้าง ความหมาย ชนิด และความสัมพันธ์ของข้อมูลที่ต้องใช้หรือแลกเปลี่ยนระหว่างระบบ รวมถึงรูปแบบการใช้ และข้อกำหนดของข้อมูลที่จำเป็นสำหรับการแลกเปลี่ยนระหว่างระบบ เช่น ชนิดข้อมูล หน่วยของข้อมูล รูปแบบวันที่และเวลา ชุดรหัส และสถานะที่เกี่ยวข้อง เพื่อให้แต่ละระบบสามารถตีความและประมวลผลข้อมูลได้อย่างถูกต้องและสอดคล้องกัน

ในกรณีที่ระบบต่าง ๆ ใช้แบบจำลองหรือโครงสร้างข้อมูลแตกต่างกัน ควรกำหนดหลักเกณฑ์หรือวิธีการเทียบเคียงและแปลงข้อมูลที่ชัดเจน โดยควรรักษาความหมายและสาระสำคัญของข้อมูลไว้ครบถ้วน และไม่ทำให้ข้อมูลเกี่ยวกับคุณลักษณะ สิทธิ เงื่อนไข หรือสถานะของหลักทรัพย์โทเคนเกิดความคลาดเคลื่อน

ตัวอย่าง : การกำหนดแบบจำลองข้อมูลและโครงสร้างข้อมูลอาจกำหนดชุดข้อมูล (Data Object) องค์ประกอบข้อมูล (Field) ชนิดข้อมูล ความจำเป็นของข้อมูล รูปแบบหรือมาตรฐานของข้อมูล และความหมายของข้อมูลแต่ละรายการ ดังตัวอย่างต่อไปนี้

```
Data Model and Structure Specification

Object : Token Information

-------------------------------------------------------------------------
Field Name      Data Type     M/O     Format / Standard       Description
-------------------------------------------------------------------------
SecurityID      String        M       ISIN                    Securities Identifier
TokenID         String        M       DTI                     Token Identifier
Quantity        Integer       M       Unit                    Number of Tokens
Currency        String        M       ISO 4217                Currency
EffectiveDate   Date          M       YYYY-MM-DD              Effective Date
Status          Enum          M       ACTIVE / FROZEN / ...   Token Status
-------------------------------------------------------------------------
```

ส่วน	ความหมาย
Object	ระบุชุดข้อมูล (Data Object) หรือโครงสร้างข้อมูลที่ใช้สำหรับจัดเก็บหรือแลกเปลี่ยนข้อมูลระหว่างระบบ
Field Name	ระบุองค์ประกอบข้อมูลหรือชื่อข้อมูล (Field) ที่อยู่ภายในชุดข้อมูล
Data Type	ระบุชนิดของข้อมูล เช่น String, Integer, Date หรือ Enum
M/O	ระบุว่าข้อมูลเป็นข้อมูลที่จำเป็น (Mandatory) หรือข้อมูลที่อาจเลือกใช้ (Optional)
Format / Standard	ระบุรูปแบบข้อมูลหรือมาตรฐานที่ใช้ เช่น รูปแบบวันที่ มาตรฐานรหัส หรือชุดค่าที่กำหนด
Description	อธิบายความหมายหรือวัตถุประสงค์ของข้อมูลแต่ละรายการ

(2) การเชื่อมต่อและการแลกเปลี่ยนข้อมูล (Interfaces and Information Exchange) : ควรกำหนดรูปแบบและข้อกำหนดของการเชื่อมต่อระหว่างระบบ รวมถึงจุดเชื่อมต่อ รูปแบบของคำขอและคำตอบ (Request/Response) ข้อความและข้อมูลที่แลกเปลี่ยน วิธีการตอบรับ การแจ้งสถานะ และการจัดการข้อผิดพลาด เพื่อให้การแลกเปลี่ยนข้อมูลและคำสั่งระหว่างระบบเป็นไปอย่างถูกต้อง ครบถ้วน และสามารถติดตามผลได้

ข้อกำหนดดังกล่าวควรคำนึงถึงลำดับและเงื่อนไขของการแลกเปลี่ยนข้อความ การตรวจสอบความถูกต้องและความครบถ้วนของข้อมูล การป้องกันการประมวลผลข้อความหรือคำสั่งซ้ำ รวมถึงการเชื่อมโยงข้อความหรือข้อมูลที่เกี่ยวข้องกับธุรกรรมเดียวกัน ทั้งนี้ รูปแบบการเชื่อมต่ออาจแตกต่างกันได้ตามลักษณะของระบบหรือกรณีการใช้งาน ตราบเท่าที่สามารถแลกเปลี่ยนข้อมูลได้อย่างถูกต้อง สอดคล้องกัน และตรวจสอบผลการดำเนินการได้

ตัวอย่าง : การกำหนดข้อกำหนดของการเชื่อมต่อระหว่างระบบอาจครอบคลุมจุดเชื่อมต่อ (Endpoint) รูปแบบของคำขอและคำตอบ (Request/Response) ข้อมูลที่ใช้แลกเปลี่ยน วิธีการตอบรับ การแจ้งสถานะ และรูปแบบการแจ้งข้อผิดพลาด ดังตัวอย่างต่อไปนี้

```
Interface Specification

Endpoint
POST /api/v1/token/transfer

Request
{
  "TokenID": "TOKEN-000001",
  "Quantity": 100,
  "FromAccount": "ACC001",
  "ToAccount": "ACC002"
}

Response
{
  "RequestID": "REQ-000001",
  "Status": "Accepted"
}

Acknowledgement
HTTP Status : 202 Accepted

Status Notification
Processing → Completed

Error Response
{
  "ErrorCode": "INSUFFICIENT_BALANCE",
  "ErrorMessage": "Available balance is insufficient."
}
```

ความหมายของแต่ละส่วนคือ

ส่วน	ความหมาย
Endpoint	ระบุจุดเชื่อมต่อหรือบริการที่อีกระบบต้องเรียกใช้งาน
Request	กำหนดข้อมูลที่ระบบผู้เรียกต้องส่ง เช่น ชื่อข้อมูล (Field) และค่าที่ต้องส่ง
Response	กำหนดข้อมูลที่ระบบปลายทางตอบกลับเมื่อรับคำขอแล้ว
Acknowledgement	ระบุวิธีตอบรับว่าระบบได้รับคำขอแล้วหรือไม่ เช่น HTTP Status 202 Accepted หมายถึงรับคำขอไว้แล้ว แต่ยังไม่ได้ดำเนินการเสร็จ
Status Notification	ระบุวิธีแจ้งความคืบหน้าหรือผลของการดำเนินการ เช่น จาก `Processing` เปลี่ยนเป็น `Completed`
Error Response	ระบุรูปแบบการแจ้งข้อผิดพลาดและข้อมูลที่ต้องส่งกลับเมื่อดำเนินการไม่สำเร็จ

(3) เหตุการณ์และพฤติกรรมของหลักทรัพย์โทเคน (Events and Token Behaviors) : ควรกำหนดชื่อ ความหมาย เงื่อนไขการเกิด และผลของเหตุการณ์ (Events) และการดำเนินการหรือพฤติกรรมของหลักทรัพย์โทเคน (Token Behaviors) รวมถึงสถานะก่อนและหลังการดำเนินการ และผลกระทบต่อจำนวน การถือครอง สิทธิ เงื่อนไข หรือสถานะของหลักทรัพย์โทเคน เพื่อให้ระบบที่เกี่ยวข้องสามารถรับรู้ ตีความ และดำเนินการต่อจากเหตุการณ์เดียวกันได้อย่างถูกต้องและสอดคล้องกัน

ในกรณีที่แต่ละระบบใช้ชื่อเหตุการณ์ สถานะ หรือผลของการดำเนินการแตกต่างกัน ควรกำหนดหลักเกณฑ์ในการเทียบเคียงให้ชัดเจน เพื่อให้แต่ละระบบสามารถตีความและประมวลผลเหตุการณ์เดียวกันได้อย่างสอดคล้องกัน

รวมทั้งกำหนดสถานะที่สำคัญของการดำเนินการให้มีความหมายที่ชัดเจน เพื่อป้องกันการตีความผลของการดำเนินการแตกต่างกันระหว่างระบบ

ตัวอย่าง : การกำหนดข้อกำหนดของเหตุการณ์และพฤติกรรมของหลักทรัพย์โทเคนอาจระบุชื่อเหตุการณ์ เงื่อนไขการเกิด สถานะก่อนและหลังการดำเนินการ ตลอดจนผลของการดำเนินการต่อหลักทรัพย์โทเคน ดังตัวอย่างต่อไปนี้

Event Specification

Event	Trigger/Condition	Pre-State	Post-State	Token Behavior
Mint	Issuance Approved	N/A	ACTIVE	Total Supply +100
Transfer	Transfer Instruction	ACTIVE	ACTIVE	Ownership Changed
Freeze	Freeze Instruction	ACTIVE	FROZEN	Transfer Disabled
Unfreeze	Unfreeze Instruction	FROZEN	ACTIVE	Transfer Enabled
Burn	Redemption / Cancellation	ACTIVE	BURNED	Total Supply -100

คอลัมน์	ความหมาย
Event	ระบุชื่อเหตุการณ์หรือการดำเนินการที่เกิดขึ้นกับหลักทรัพย์โทเคน เช่น การออก (Mint) การโอน (Transfer) หรือการทำลาย (Burn)
Trigger / Condition	ระบุเหตุหรือเงื่อนไขที่ทำให้เกิดเหตุการณ์หรือการดำเนินการนั้น เช่น การอนุมัติการออกหลักทรัพย์ คำสั่งโอน หรือคำสั่งระงับการโอน
Pre-State	ระบุสถานะของหลักทรัพย์โทเคนก่อนเกิดเหตุการณ์หรือก่อนดำเนินการ
Post-State	ระบุสถานะของหลักทรัพย์โทเคนหลังเกิดเหตุการณ์หรือหลังดำเนินการเสร็จสิ้น
Token Behavior	ระบุผลของเหตุการณ์หรือการดำเนินการที่มีต่อหลักทรัพย์โทเคน เช่น การเปลี่ยนแปลงการถือครอง จำนวนโทเคน สิทธิ หรือข้อจำกัดของหลักทรัพย์โทเคน

(4) ตัวระบุและข้อมูลอ้างอิงร่วม (Identifiers and Common References) : ควรใช้ตัวระบุและข้อมูลอ้างอิงที่มีความเป็นเอกลักษณ์ และสามารถเชื่อมโยงหรืออ้างอิงข้อมูลที่เกี่ยวข้องระหว่างระบบได้อย่างถูกต้องและสอดคล้องกัน โดยควรกำหนดรูปแบบ ขอบเขต หน่วยงานหรือผู้รับผิดชอบในการกำหนดตัวระบุ (Identifier Authority) และวิธีการนำตัวระบุไปใช้อ้างอิงให้ชัดเจน

ตัวระบุดังกล่าวอาจครอบคลุมหลักทรัพย์โทเคน รุ่นในการออกหลักทรัพย์ (Issue/Tranche) ผู้ออกหลักทรัพย์และผู้ให้บริการที่เกี่ยวข้อง บัญชีหรือ

ข้อมูลที่ใช้ระบุการถือครอง เครือข่าย ธุรกรรม ข้อความ และเอกสารที่เกี่ยวข้อง ในกรณีที่ระบบต่าง ๆ ใช้ตัวระบุภายในแตกต่างกัน ควรกำหนดหลักเกณฑ์หรือกลไกในการเชื่อมโยงหรือเทียบเคียงตัวระบุดังกล่าว เพื่อให้สามารถอ้างอิงถึงข้อมูลเดียวกันได้อย่างถูกต้องและสอดคล้องกัน

ตัวอย่าง : การกำหนดตัวระบุและข้อมูลอ้างอิงร่วมอาจกำหนดประเภทของตัวระบุ รูปแบบ และค่าที่ใช้อ้างอิงสำหรับข้อมูลหรือรายการที่เกี่ยวข้อง เพื่อให้ระบบที่ทำงานร่วมกันสามารถอ้างอิงข้อมูลเดียวกันได้อย่างถูกต้องและสอดคล้องกัน ดังตัวอย่างต่อไปนี้

```
Identifier Specification

Token Identifier
DTI                : DTI-TH-000001

Issuance Identifier
Issuance ID        : ISSUE-2026-001

Issuer Identifier
LEI                : 5493001KJTIIGC8Y1R12

Participant Identifier
Participant ID     : SEC-BROKER-001

Holding Identifier
Wallet Address     : 0xA1B2...C3D4

Network Identifier
Network ID         : Ethereum Mainnet

Transaction Identifier
Transaction ID     : TX-000001

Message Identifier
Message ID         : MSG-20260806-000001

Document Identifier
Document ID        : DOC-2026-001
```

ส่วน	ความหมาย
Token Identifier	ระบุตัวระบุที่ใช้สำหรับอ้างอิงหลักทรัพย์โทเคน เพื่อให้สามารถอ้างอิงโทเคนเดียวกันได้อย่างสอดคล้องกันระหว่างระบบ
Issuance Identifier	ระบุตัวระบุที่ใช้สำหรับอ้างอิงการออกหลักทรัพย์ (Issuance) หรือชุดการออกหลักทรัพย์ เพื่อแยกความแตกต่างของการออกแต่ละครั้ง
Issuer Identifier	ระบุตัวระบุของผู้ออกหลักทรัพย์ เพื่อให้สามารถอ้างอิงผู้ออกหลักทรัพย์เดียวกันได้อย่างถูกต้องระหว่างระบบ
Participant Identifier	ระบุตัวระบุของผู้เกี่ยวข้องหรือผู้ให้บริการที่เกี่ยวข้อง เพื่อให้สามารถอ้างอิงผู้เกี่ยวข้องแต่ละรายได้อย่างสอดคล้องกัน
Holding Identifier	ระบุตัวระบุของบัญชีหรือข้อมูลที่ใช้ระบุการถือครองหลักทรัพย์โทเคน เช่น Wallet Address หรือ Account ID
Network Identifier	ระบุตัวระบุของเครือข่ายหรือโครงสร้างพื้นฐานที่เกี่ยวข้อง เพื่อแยกความแตกต่างของแต่ละเครือข่ายหรือระบบ
Transaction Identifier	ระบุตัวระบุของธุรกรรม เพื่อให้สามารถติดตามและอ้างอิงธุรกรรมเดียวกันได้ตลอดกระบวนการ
Message Identifier	ระบุตัวระบุของข้อความที่แลกเปลี่ยนระหว่างระบบ เพื่อเชื่อมโยงและติดตามข้อความที่เกี่ยวข้อง
Document Identifier	ระบุตัวระบุของเอกสารที่เกี่ยวข้อง เช่น เอกสารการออกหลักทรัพย์ หรือเอกสารประกอบธุรกรรม เพื่อให้สามารถอ้างอิงเอกสารเดียวกันได้อย่างถูกต้อง

(5) การเลือกใช้มาตรฐานและการบริหารจัดการเพื่อรองรับการทำงานร่วมกัน (Standards Adoption, Compatibility and Phased Participation) : ในการกำหนดข้อกำหนดทางเทคนิคด้านการทำงานร่วมกัน ควรพิจารณาเลือกใช้มาตรฐาน แบบจำลองข้อมูล รูปแบบข้อความ ตัวระบุ หรือข้อกำหนดทางเทคนิคที่ได้รับการยอมรับหรือมีการใช้งานอยู่แล้วเป็นลำดับแรก โดยเฉพาะมาตรฐานที่เกี่ยวข้องกับระบบหรือโครงสร้างพื้นฐานที่คาดว่าจะต้องทำงานร่วมกัน เพื่อส่งเสริมให้ข้อกำหนดที่จัดทำขึ้นมีความสอดคล้อง

กับแนวปฏิบัติที่เป็นที่ยอมรับ ลดการจัดทำข้อกำหนดเฉพาะที่ซ้ำซ้อน และเอื้อต่อการเชื่อมต่อ การทดสอบ และการขยายการทำงานร่วมกันในอนาคต

ในกรณีที่ยังไม่มีมาตรฐานหรือข้อกำหนดที่เหมาะสม ผู้เกี่ยวข้องอาจร่วมกันกำหนดข้อกำหนดทางเทคนิคให้สอดคล้องกับวัตถุประสงค์และกรณีการใช้งานได้ โดยข้อกำหนดดังกล่าวควรมีความชัดเจน สามารถนำไปใช้ในการพัฒนา เชื่อมต่อ และทดสอบการทำงานร่วมกันได้ รวมทั้งไม่ควรกำหนดในลักษณะที่ผูกติดกับผู้ให้บริการ ระบบ เครือข่าย หรือเทคโนโลยีเฉพาะรายโดยไม่มีเหตุผลอันสมควร

ในกรณีที่ระบบหรือผู้เกี่ยวข้องใช้มาตรฐานหรือข้อกำหนดทางเทคนิคที่แตกต่างกัน หรือเข้าร่วมการทำงานร่วมกันในช่วงเวลาที่แตกต่างกัน ควรรองรับการนำมาตรฐานหรือข้อกำหนดที่มีอยู่ไปใช้ หรือมีกลไกสำหรับการเทียบเคียง (Mapping) การแปลง (Transformation) หรือการเชื่อมต่อ (Integration) ระหว่างข้อกำหนดที่แตกต่างกัน เพื่อให้สามารถทำงานร่วมกันได้โดยไม่จำเป็นต้องปรับเปลี่ยนระบบเดิมทั้งหมด

นอกจากนี้ ควรกำหนดแนวทางในการบริหารจัดการการเปลี่ยนแปลงของข้อกำหนดทางเทคนิค เช่น การบริหารจัดการเวอร์ชัน (Version Management) การรองรับความเข้ากันได้กับข้อกำหนดเดิม (Backward Compatibility) ระยะเวลาเปลี่ยนผ่าน (Transition Period) และแนวทางการยุติการรองรับข้อกำหนดหรือเวอร์ชันที่ล้าสมัย (Deprecation) เพื่อให้การปรับปรุงข้อกำหนด การเพิ่มระบบ หรือการเข้าร่วมของผู้เกี่ยวข้องรายใหม่ ไม่ส่งผลกระทบต่อการทำงานร่วมกันของระบบที่เชื่อมต่ออยู่เดิมเกินสมควร

ตัวอย่าง : มาตรฐานหรือข้อกำหนดที่ใช้กันอย่างแพร่หลาย ซึ่งอาจพิจารณาเลือกใช้หรือนำมาอ้างอิงในการจัดทำข้อกำหนดทางเทคนิคเพื่อการทำงานร่วมกัน มีดังต่อไปนี้

หมวดของข้อกำหนดทางเทคนิค	ตัวอย่างมาตรฐานหรือข้อกำหนดที่ใช้กันอย่างแพร่หลาย
แบบจำลองข้อมูลและโครงสร้างข้อมูล (Data Models and Data Structures)	ISO 20022, Common Domain Model (CDM), Financial Industry Business Ontology (FIBO)
การเชื่อมต่อและการแลกเปลี่ยนข้อมูล (Interfaces and Information Exchange)	OpenAPI Specification, AsyncAPI Specification, WebSocket (RFC 6455), gRPC
เหตุการณ์และพฤติกรรมของหลักทรัพย์โทเคน (Events and Token Behaviors)	**ERC-3643, ERC-1400 หรือข้อกำหนดของ Token Standards ที่กำหนดเหตุการณ์ (Events) และพฤติกรรม (Behaviors) ของโทเคน**
ตัวระบุและข้อมูลอ้างอิงร่วม (Identifiers and Common References)	ISIN (ISO 6166), LEI (ISO 17442), DTI (ISO 24165), ISO 4217, ISO 8601

ทั้งนี้ มาตรฐานหรือข้อกำหนดข้างต้นเป็นเพียงตัวอย่างประกอบการพิจารณา ผู้พัฒนาระบบอาจเลือกใช้มาตรฐานหรือข้อกำหนดอื่นที่เหมาะสมกับลักษณะของระบบและกรณีการใช้งานได้ โดยควรคำนึงถึงการรองรับการทำงานร่วมกัน ความเข้ากันได้ และการขยายการเชื่อมต่อในอนาคตเป็นสำคัญ

4.4.3 การปฏิบัติงานร่วมกันระหว่างผู้เกี่ยวข้อง (Operational Interoperability)

หลักการทั่วไป

การปฏิบัติงานร่วมกันระหว่างผู้เกี่ยวข้องให้เกิดผลในทางปฏิบัติ จำเป็นต้องอาศัยมากกว่าการเชื่อมต่อทางเทคนิค เมื่อกิจกรรมหรือธุรกรรมที่เกี่ยวข้องกับหลักทรัพย์โทเคนต้องดำเนินการผ่านผู้เกี่ยวข้องหรือระบบหลายฝ่าย ควรกำหนดกระบวนการปฏิบัติงานร่วมกัน (Common Workflow) ให้มีความชัดเจนและสอดคล้องกัน โดยครอบคลุมลำดับการดำเนินงาน บทบาทและความรับผิดชอบ เงื่อนไขในการดำเนินการต่อ การยืนยันผล และการสิ้นสุดกระบวนการ เพื่อให้ผู้เกี่ยวข้องแต่ละฝ่ายสามารถดำเนินงาน ประสานงาน และรับรู้ผลของการดำเนินการได้อย่างถูกต้องและสอดคล้องกัน

การปฏิบัติงานร่วมกันควรกำหนดให้สอดคล้องกับขอบเขตการทำงานร่วมกันตามข้อ 4.4.1 และข้อกำหนดทางเทคนิคตามข้อ 4.4.2 ทั้งนี้ ไม่จำเป็นต้องกำหนดให้กระบวนการดำเนินงานภายในของผู้เกี่ยวข้องแต่ละฝ่ายมีรูปแบบเดียวกัน ตราบเท่าที่ลำดับการดำเนินงาน ข้อมูลที่ต้องแลกเปลี่ยน เงื่อนไขในการดำเนินการต่อ ระยะเวลา สถานะ และผลลัพธ์ที่ต้องประสานร่วมกัน มีความชัดเจนและสอดคล้องกัน เพื่อให้ผู้เกี่ยวข้องสามารถดำเนินงานร่วมกันได้อย่างถูกต้องและต่อเนื่อง

ทั้งนี้ หัวข้อนี้มุ่งกำหนดเฉพาะการปฏิบัติงาน ณ จุดที่ผู้เกี่ยวข้องต้องประสานงานหรือดำเนินงานร่วมกัน มิได้ครอบคลุมกระบวนการดำเนินงานภายในทั้งหมดของผู้ให้บริการแต่ละราย

ข้อเสนอแนะขั้นต่ำ

การปฏิบัติงานร่วมกันระหว่างผู้เกี่ยวข้องควรพิจารณากำหนดองค์ประกอบอย่างน้อยดังต่อไปนี้

(1) บทบาทและความรับผิดชอบ (Roles and Responsibilities) : ควรกำหนดบทบาท หน้าที่ และความรับผิดชอบของผู้เกี่ยวข้องแต่ละฝ่ายตลอดกระบวนการ

ปฏิบัติงานร่วมกัน รวมถึงผู้เริ่มต้นคำสั่ง ผู้ตรวจสอบหรืออนุมัติ ผู้ดำเนินการ ผู้บันทึกข้อมูล ผู้ยืนยันผล ผู้ติดตามสถานะ และผู้กระทบยอดข้อมูล เพื่อให้สามารถระบุได้อย่างชัดเจนว่าแต่ละขั้นตอนอยู่ในความรับผิดชอบของฝ่ายใด และลดความเสี่ยงจากการกำหนดบทบาทหรือความรับผิดชอบที่ซ้ำซ้อน ไม่ชัดเจน หรือไม่มีผู้รับผิดชอบ

ในกรณีที่มีผู้เกี่ยวข้องหลายฝ่าย หรือมีระบบต้นทาง ระบบปลายทาง หรือผู้ให้บริการตัวกลาง ควรกำหนดขอบเขตความรับผิดชอบ และเงื่อนไขในการส่งต่อและรับช่วงการดำเนินงานระหว่างแต่ละฝ่ายให้ชัดเจน ทั้งนี้ บทบาทตามหัวข้อนี้หมายถึงบทบาทในการปฏิบัติงานร่วมกันและการดำเนินธุรกรรม ส่วนอำนาจในการกำหนดกฎ การอนุมัติการเปลี่ยนแปลง หรือการกำกับดูแลความสัมพันธ์ระหว่างผู้เกี่ยวข้องให้เป็นไปตามข้อ 4.4.4

(2) กระบวนการและลำดับการดำเนินงาน (Operational Processes and Workflow) : ควรกำหนดกระบวนการและลำดับการดำเนินงานสำหรับกิจกรรมที่ต้องอาศัยการทำงานร่วมกันให้ครบถ้วนตลอดกระบวนการ โดยครอบคลุมเงื่อนไขก่อนเริ่มดำเนินการ จุดเริ่มต้นของกระบวนการ ลำดับและความสัมพันธ์ระหว่างขั้นตอน จุดส่งต่องานระหว่างผู้เกี่ยวข้องหรือระบบ (Handover Points) เงื่อนไขในการดำเนินการต่อ ตลอดจนเงื่อนไขที่ถือว่ากระบวนการเสร็จสมบูรณ์ ถูกปฏิเสธ หรือไม่สามารถดำเนินการต่อได้

กระบวนการดังกล่าวควรกำหนดสถานะของรายการในแต่ละช่วง เงื่อนไขในการเปลี่ยนผ่านของแต่ละสถานะ (State Transition) การยืนยันผล กรอบเวลาในการดำเนินงาน และการกระทบยอดข้อมูล (Reconciliation) ตามความเหมาะสม เพื่อให้ผู้เกี่ยวข้องสามารถติดตามความคืบหน้าและรับรู้ผลของการดำเนินงานได้อย่างสอดคล้องกัน

ในกรณีที่ธุรกรรมประกอบด้วยการดำเนินการหลายส่วน หรือมีการเชื่อมโยงระหว่างหลายระบบหรือผู้เกี่ยวข้อง ควรกำหนดเงื่อนไขที่ทำให้แต่ละขั้นตอนสามารถดำเนินการต่อได้ รวมถึงแนวทางในการจัดการเมื่อการดำเนินการบางส่วนไม่สำเร็จ

เพื่อป้องกันการเกิดข้อมูล สถานะ หรือผลของธุรกรรมที่ไม่สอดคล้องกันระหว่างผู้เกี่ยวข้อง

(3) การประสานงานและการแลกเปลี่ยนข้อมูลระหว่างผู้เกี่ยวข้อง (Coordination and Information Exchange) : ควรกำหนดแนวทางการประสานงานและการสื่อสารระหว่างผู้เกี่ยวข้องให้ชัดเจน โดยกำหนดผู้ที่ต้องประสานงานกัน ข้อมูลหรือการแจ้งที่แต่ละฝ่ายต้องสื่อสารระหว่างกัน ผู้รับผิดชอบในการประสานงาน ระยะเวลาและความถี่ในการแจ้งหรือรายงานข้อมูล การตอบรับ การยืนยัน การรับทราบ และการติดตามผล เพื่อให้ผู้เกี่ยวข้องแต่ละฝ่ายสามารถปฏิบัติงานตามบทบาทของตนได้อย่างต่อเนื่อง และรับทราบสถานะของกระบวนการได้อย่างสอดคล้องกัน

ข้อมูลหรือการแจ้งที่สื่อสารระหว่างผู้เกี่ยวข้องควรครอบคลุมสาระที่จำเป็นต่อการปฏิบัติงาน เช่น คำสั่งหรือคำขอ ผลการตรวจสอบ การตอบรับ สถานะการดำเนินการ เหตุผลของการปฏิเสธหรือข้อผิดพลาด ผลการยืนยัน และข้อมูลสำหรับการกระทบยอด (Reconciliation) ทั้งนี้ ควรกำหนดผู้ประสานงาน (Point of Contact) ช่องทางการติดต่อ (Communication Channels) สำหรับการปฏิบัติงานตามปกติและกรณีเร่งด่วน รวมถึงแนวทางการติดตามรายการที่อยู่ระหว่างดำเนินการหรือยังไม่ได้รับการยืนยัน ตลอดจนแนวทางการแจ้งหรือส่งต่อประเด็น (Escalation) เมื่อเกิดเหตุผิดปกติหรือไม่สามารถดำเนินการได้ โดยรูปแบบโครงสร้าง และวิธีการแลกเปลี่ยนข้อมูลทางเทคนิคให้เป็นไปตามข้อ 4.4.2

(4) การจัดการกรณีผิดปกติและเหตุขัดข้อง (Exception and Incident Handling) : ควรกำหนดแนวทางในการระบุ ประเมิน จัดการ และติดตามกรณีผิดปกติหรือเหตุขัดข้องที่เกิดขึ้นระหว่างการปฏิบัติงาน โดยครอบคลุมทั้งกรณีผิดปกติที่เกิดขึ้นกับธุรกรรมหรือกระบวนการดำเนินงาน เช่น การตรวจสอบไม่ผ่าน การดำเนินธุรกรรมไม่เป็นไปตามเงื่อนไข หรือการได้รับข้อมูลไม่ครบถ้วน และเหตุขัดข้องที่เกิดขึ้นกับระบบหรือการเชื่อมต่อ เช่น ระบบไม่พร้อมให้บริการ การเชื่อมต่อระหว่างระบบขัดข้อง หรือไม่สามารถแลกเปลี่ยนข้อมูลได้ รวมถึงกำหนดผู้รับผิดชอบ ระดับความ

รุนแรง ขั้นตอนการแจ้งเหตุ การยกระดับการดำเนินการ (Escalation) และแนวทางการประสานงานระหว่างผู้เกี่ยวข้อง

แนวทางดังกล่าวควรรองรับการจัดการและจำกัดผลกระทบของกรณีผิดปกติหรือเหตุขัดข้อง รวมทั้งกำหนดมาตรการที่เหมาะสมเพื่อแก้ไขและกู้คืนการดำเนินงาน โดยครอบคลุมการระบุรายการ ผู้เกี่ยวข้อง หรือระบบที่ได้รับผลกระทบ การป้องกันการประมวลผลซ้ำหรือการเกิดข้อมูลที่ไม่สอดคล้องกัน การระงับการดำเนินการในส่วนที่ได้รับผลกระทบ รวมถึงการดำเนินการอื่นใดที่จำเป็นเพื่อแก้ไขและกู้คืน เช่น การดำเนินการซ้ำ (Retry) การย้อนกลับสู่สถานะเดิม (Rollback) หรือการทำรายการชดเชยตามความเหมาะสม (Compensating Transaction) เมื่อเหตุการณ์ได้รับการแก้ไขแล้ว ควรมีการตรวจสอบและกระทบยอดข้อมูล (Reconciliation) ระหว่างผู้เกี่ยวข้อง รวมทั้งกำหนดเงื่อนไขในการกลับมาดำเนินงานหรือกลับมาให้บริการ เพื่อให้ข้อมูล การถือครอง สถานะ และผลของธุรกรรมกลับมาถูกต้องและสอดคล้องกัน

แนวทางการปฏิบัติงานร่วมกันควรจัดทำเป็นเอกสารในระดับที่ผู้เกี่ยวข้องสามารถนำไปใช้ปฏิบัติ ทดสอบ ติดตาม และตรวจสอบย้อนหลังได้ โดยควรระบุขอบเขต ผู้รับผิดชอบ ขั้นตอน สถานะ กรอบเวลา จุดประสานงาน และแนวทางจัดการกรณีผิดปกติหรือเหตุขัดข้องไว้อย่างชัดเจน ทั้งนี้ แม้ผู้เกี่ยวข้องแต่ละฝ่ายอาจมีกระบวนการดำเนินงานภายในแตกต่างกัน แต่กระบวนการ ณ จุดที่ต้องประสานงานร่วมกันและผลลัพธ์ที่ต้องร่วมกันรับรอง ควรมีความสอดคล้องกัน และไม่ก่อให้เกิดช่องว่างในการประสานงานระหว่างผู้เกี่ยวข้อง

4.4.4. การกำกับดูแลการทำงานร่วมกันระหว่างผู้เกี่ยวข้อง (Interoperability Governance)

หลักการทั่วไป

การทำงานร่วมกันระหว่างผู้เกี่ยวข้องมักประกอบด้วยผู้เกี่ยวข้องหลายฝ่าย ซึ่งอาจมีบทบาท หน้าที่ ความรับผิดชอบ วัตถุประสงค์ ระบบที่ใช้ และช่วงเวลาในการเข้าร่วมแตกต่างกัน แม้จะมีการกำหนดขอบเขตการทำงานร่วมกัน ข้อกำหนดทางเทคนิค และกระบวนการปฏิบัติงานร่วมกันแล้ว ยังควรมีกลไกการกำกับดูแลที่ชัดเจน เพื่อกำหนดกติกา อำนาจตัดสินใจ ความรับผิดชอบ และแนวทางบริหารจัดการประเด็นที่มีผลกระทบต่อการทำงานร่วมกัน อันจะช่วยให้การทำงานร่วมกันมีความต่อเนื่อง โปร่งใส และสามารถปรับตัวต่อการเปลี่ยนแปลงได้อย่างเหมาะสม

กลไกการกำกับดูแลควรสอดคล้องกับขอบเขตและระดับความสำคัญของการทำงานร่วมกัน จำนวนและลักษณะของผู้เกี่ยวข้อง ตลอดจนความเสี่ยงที่อาจเกิดขึ้น โดยอาจกำหนดในรูปแบบข้อตกลงระหว่างผู้เกี่ยวข้อง การกำกับดูแลร่วมกันระหว่างผู้เกี่ยวข้อง หรือการมอบหมายให้ผู้ดำเนินการระบบหรือหน่วยงานกลางทำหน้าที่ตามความเหมาะสม ทั้งนี้ หัวข้อนี้มุ่งกำหนดการกำกับดูแลเฉพาะส่วนที่เกี่ยวข้องกับการทำงานร่วมกันระหว่างผู้เกี่ยวข้อง มิได้ครอบคลุมการกำกับดูแลกิจการหรือการบริหารจัดการภายในของผู้เกี่ยวข้องแต่ละฝ่าย

ข้อเสนอแนะขั้นต่ำ

การกำกับดูแลการทำงานร่วมกันระหว่างผู้เกี่ยวข้องควรพิจารณากำหนดองค์ประกอบอย่างน้อย ดังต่อไปนี้

(1) บทบาทและความรับผิดชอบในการกำกับดูแล (Governance Roles and Responsibilities) : ควรกำหนดโครงสร้างการกำกับดูแล บทบาท อำนาจตัดสินใจ และความรับผิดชอบของผู้เกี่ยวข้องแต่ละฝ่ายให้ชัดเจน โดยครอบคลุมการกำหนดและตีความกติกา ข้อกำหนด หรือมาตรฐานร่วม การอนุมัติการเชื่อมต่อหรือการเข้าร่วม การพิจารณาการเปลี่ยนแปลงที่มีนัยสำคัญ การพิจารณาและบริหารความเสี่ยงตลอดจน การระงับหรือยุติการเข้าร่วมของผู้เกี่ยวข้อง หรือการเชื่อมต่อ เมื่อมีเหตุจำเป็น

ควรกำหนดผู้รับผิดชอบ คณะทำงาน หรือกลไกที่ทำหน้าที่ดูแลข้อกำหนดทางเทคนิค กระบวนการปฏิบัติงาน และเอกสารหรือมาตรฐานที่ใช้ร่วมกัน รวมทั้งกำหนดกลไกการตัดสินใจและการพิจารณาข้อขัดแย้งเพื่อหาข้อยุติในกรณีที่ผู้เกี่ยวข้องมีความเห็นแตกต่างกัน ทั้งนี้ บทบาทตามหัวข้อนี้เป็นบทบาทในระดับการกำหนดกติกา การกำกับดูแล และการตัดสินใจร่วมกัน ซึ่งแตกต่างจากบทบาทในการปฏิบัติงานปกติตามข้อ 4.4.3

ตัวอย่าง : การกำหนดคณะกรรมการ คณะทำงาน ผู้ดำเนินการระบบ หรือหน่วยงานกลางให้ทำหน้าที่ดูแลข้อกำหนดและเอกสารที่ใช้ร่วมกัน กำหนดหลักเกณฑ์ในการตัดสินใจ และพิจารณาประเด็นที่มีผลกระทบต่อผู้เกี่ยวข้องหลายฝ่าย เช่น การเปลี่ยนแปลงข้อกำหนด การรับผู้เกี่ยวข้องรายใหม่ หรือการระงับการเข้าร่วม

(2) การบริหารจัดการการเปลี่ยนแปลง (Change Management) : ควรมีกระบวนการสำหรับเสนอ ประเมิน อนุมัติ พัฒนา ทดสอบ และนำการเปลี่ยนแปลงที่เกี่ยวข้องกับการทำงานร่วมกันไปใช้ โดยควรพิจารณาผลกระทบต่อผู้เกี่ยวข้องและระบบที่เชื่อมต่ออยู่ กระบวนการปฏิบัติงาน ความเข้ากันได้กับข้อกำหนดหรือเวอร์ชันเดิม และความต่อเนื่องในการดำเนินงานหรือการให้บริการ

การบริหารจัดการการเปลี่ยนแปลงควรรองรับทั้งการเปลี่ยนแปลงตามแผนและการเปลี่ยนแปลงเร่งด่วน โดยควรกำหนดระยะเวลาแจ้งล่วงหน้า แนวทางการสื่อสารและการทดสอบ ระยะเปลี่ยนผ่าน การรองรับหลายเวอร์ชัน และแนวทางแก้ไขหรือย้อนกลับ (Rollback) ในกรณีที่การเปลี่ยนแปลงไม่เป็นไปตามที่คาดหมาย ทั้งนี้ควรดำเนินการให้ผู้เกี่ยวข้องสามารถรับทราบ ประเมินผลกระทบ และเตรียมความพร้อมก่อนการเปลี่ยนแปลงมีผลใช้บังคับตามความเหมาะสม

ตัวอย่าง : กำหนดให้การเปลี่ยนแปลงใดที่มีผลกระทบต่อการทำงานร่วมกันต้องจัดทำคำขอเปลี่ยนแปลง (Change Request) พร้อมการประเมินผลกระทบเสนอให้คณะทำงานหรือผู้รับผิดชอบพิจารณาและอนุมัติ ก่อนแจ้งผู้เกี่ยวข้องทดสอบร่วมกัน และกำหนดวันที่มีผลใช้บังคับ ทั้งนี้ การเปลี่ยนแปลงดังกล่าวอาจครอบคลุม เช่น การปรับปรุงข้อกำหนดทางเทคนิค แบบจำลองข้อมูล (Data Model) รูปแบบข้อความ (Message Format) API มาตรฐานที่ใช้อ้างอิง กระบวนการปฏิบัติงาน เกณฑ์หรือกติกาที่ใช้ร่วมกัน การเพิ่มหรือยกเลิกผู้เกี่ยวข้อง การเปลี่ยนแปลงบทบาทและความรับผิดชอบ หรือการปรับปรุงกลไกการกำกับดูแลที่เกี่ยวข้องกับการทำงานร่วมกัน เป็นต้น

(3) การสื่อสารและการประสานงานระหว่างผู้เกี่ยวข้อง (Stakeholder Communication and Coordination) : ควรกำหนดแนวทางและช่องทางการสื่อสารระหว่างผู้เกี่ยวข้อง เพื่อให้สามารถสื่อสารและรับทราบกติกา ข้อกำหนดการเปลี่ยนแปลง และผลการตัดสินใจที่เกี่ยวข้องกับการทำงานร่วมกันได้อย่างเหมาะสม โดยควรกำหนดประเภทของข้อมูลที่ต้องสื่อสาร ผู้รับผิดชอบ ผู้รับข้อมูล ระยะเวลาในการแจ้ง และช่องทางที่ใช้สำหรับการสื่อสารตามปกติและกรณีเร่งด่วน

ควรมีช่องทางสำหรับเผยแพร่และแจ้งให้ผู้เกี่ยวข้องรับทราบกติกา ข้อกำหนด เวอร์ชันที่ใช้บังคับ มติหรือผลการตัดสินใจ ประวัติและแผนการเปลี่ยนแปลง ตลอดจนข้อมูลอื่นที่มีผลต่อการทำงานร่วมกัน รวมทั้งควรจัดเก็บบันทึกการสื่อสาร การตัดสินใจ และการเปลี่ยนแปลงที่สำคัญ เพื่อให้สามารถอ้างอิงและตรวจสอบย้อนหลังได้ โดยคำนึงถึงการรักษาความลับและสิทธิในการเข้าถึงข้อมูลตามความเหมาะสม

ตัวอย่าง : การกำหนดให้มีช่องทางกลางสำหรับการสื่อสารและเผยแพร่ข้อมูลที่เกี่ยวข้องกับการทำงานร่วมกัน เช่น เว็บไซต์หรือระบบจัดเก็บเอกสารกลาง (Document Repository) สำหรับเผยแพร่กติกา ข้อกำหนด และเวอร์ชันที่ใช้บังคับ รวมถึงระบบแจ้งเตือนหรือจดหมายอิเล็กทรอนิกส์สำหรับแจ้งการเปลี่ยนแปลงที่มีนัยสำคัญ เมื่อมีการเปลี่ยนแปลงข้อกำหนดหรือมาตรฐานที่ใช้ร่วมกัน ผู้รับผิดชอบหรือคณะทำงานควรเผยแพร่เอกสารฉบับใหม่ แจ้งผู้เกี่ยวข้องผ่านช่องทางที่กำหนด และอาจจัดประชุมหรือช่องทางหารือเพื่อชี้แจงสาระสำคัญ ผลกระทบ และกำหนดวันมีผลใช้บังคับ ตลอดจนเปิดโอกาสให้ผู้เกี่ยวข้องสอบถามหรือเสนอข้อคิดเห็นก่อนการบังคับใช้ตามความเหมาะสม

(4) การติดตามและทบทวนการกำกับดูแล (Governance Monitoring and Review) : ควรมีกระบวนการติดตามและทบทวนว่ากลไกการกำกับดูแล กติกา ข้อกำหนด และข้อตกลงที่ใช้ร่วมกันยังคงเหมาะสม และสามารถสนับสนุนการทำงานร่วมกันได้อย่างมีประสิทธิภาพ โดยควรพิจารณาผลการดำเนินงานด้านการทำงานร่วมกัน ปัญหาและข้อขัดแย้งที่เกิดขึ้น การปฏิบัติตามข้อกำหนดร่วม ตลอดจนการเปลี่ยนแปลงด้านกฎหมาย เทคโนโลยี รูปแบบธุรกิจ และลักษณะหรือจำนวนของผู้เกี่ยวข้อง เพื่อประเมินความจำเป็นในการปรับปรุงกลไกการกำกับดูแลหรือข้อกำหนดที่เกี่ยวข้องตามความเหมาะสม

ควรกำหนดรอบการทบทวน ผู้รับผิดชอบ ข้อมูลที่ใช้ประกอบการประเมิน และแนวทางติดตามผลการปรับปรุงอย่างชัดเจน ทั้งนี้ ควรมีการทบทวนเพิ่มเติมเมื่อเกิดเหตุการณ์ที่มีนัยสำคัญ เช่น การเปลี่ยนแปลงรูปแบบการทำงานร่วมกัน การเพิ่มหรือลดผู้เกี่ยวข้อง การเปลี่ยนแปลงข้อกำหนดหรือมาตรฐานสำคัญ หรือเหตุขัดข้องที่ส่งผลกระทบต่อการทำงานร่วมกัน โดยหากผลการทบทวนนำไปสู่ความจำเป็นในการ

ปรับปรุงกติกา ข้อกำหนด หรือกลไกการกำกับดูแล ควรดำเนินการตามกระบวนการบริหารจัดการการเปลี่ยนแปลงที่กำหนดไว้ตามความเหมาะสม

ตัวอย่าง : กำหนดให้คณะกรรมการ คณะทำงาน หรือผู้รับผิดชอบด้านการกำกับดูแล จัดให้มีการประชุมทบทวนการทำงานร่วมกันเป็นระยะ โดยรวบรวมข้อมูลที่เกี่ยวข้อง เช่น ผลการดำเนินงานด้านการทำงานร่วมกัน ปัญหาและข้อขัดแย้งที่เกิดขึ้น เหตุขัดข้องหรือกรณีผิดปกติ ผลการปฏิบัติตามข้อกำหนดร่วม ข้อเสนอแนะจากผู้เกี่ยวข้อง และการเปลี่ยนแปลงด้านกฎหมาย เทคโนโลยี หรือมาตรฐานที่เกี่ยวข้อง เพื่อนำมาประเมินว่ากลไกการกำกับดูแล กติกา ข้อกำหนด หรือกระบวนการที่ใช้ร่วมกันยังคงเหมาะสมและมีประสิทธิภาพหรือไม่ ทั้งนี้ อาจจัดทำรายงานสรุปผลการทบทวน ประเด็นที่พบ ข้อเสนอแนะ และแผนการปรับปรุง เพื่อใช้ประกอบการตัดสินใจ ติดตามความคืบหน้าของการดำเนินการ และเป็นข้อมูลสำหรับการทบทวนในรอบถัดไป รวมทั้งหากจำเป็นต้องมีการปรับปรุงข้อกำหนดหรือกลไกการกำกับดูแล ควรดำเนินการตามกระบวนการบริหารจัดการการเปลี่ยนแปลงที่กำหนดไว้

5. มาตรฐานของผู้ให้บริการสนับสนุนการออกและเสนอขายหลักทรัพย์โทเคน (Standard for Securities Tokenizer)

การออกและให้บริการเกี่ยวกับหลักทรัพย์โทเคนต้องอาศัยระบบงานและกลไกสนับสนุนที่สามารถรองรับการดำเนินงานเกี่ยวกับหลักทรัพย์ได้ตลอดวงจรชีวิต ตั้งแต่การออกและบันทึกข้อมูล การส่งมอบและโอน การจัดการสิทธิและข้อจำกัดที่เกี่ยวข้องกับหลักทรัพย์ การดูแลรักษาหลักทรัพย์โทเคน ตลอดจนการชำระราคาและส่งมอบหลักทรัพย์ ทั้งนี้ การดำเนินงานดังกล่าวต้องสามารถเชื่อมโยงข้อมูลและสถานะของหลักทรัพย์กับสิทธิของผู้ถือหลักทรัพย์ตามกฎหมายและเงื่อนไขที่เกี่ยวข้องได้อย่างถูกต้อง

ผู้ให้บริการสนับสนุนการออกและเสนอขายหลักทรัพย์โทเคน (Securities Tokenizer) มีบทบาทในการจัดให้มีหรือให้บริการระบบงานและกระบวนการที่สนับสนุนการดำเนินงานดังกล่าว โดยอาจดำเนินการได้หลายลักษณะตามขอบเขตหน้าที่และความรับผิดชอบของตน ไม่ว่าจะเป็นการให้บริการด้านการออกและบันทึกข้อมูลหลักทรัพย์โทเคน การให้บริการเกี่ยวกับกระเป๋าอิเล็กทรอนิกส์ (Wallet) และการรับฝากเก็บรักษาหลักทรัพย์โทเคน หรือการให้บริการด้านการชำระราคาและส่งมอบหลักทรัพย์โทเคน โดยผู้ให้บริการแต่ละรายไม่จำเป็นต้องให้บริการครบทุกประเภท แต่ต้องมีคุณสมบัติ ความพร้อมระบบงาน และกลไกควบคุมที่เหมาะสมกับบริการที่ตนรับผิดชอบ

มาตรฐานในบทนี้จึงกำหนดหลักเกณฑ์เกี่ยวกับบทบาทและขอบเขตการให้บริการ คุณสมบัติและความพร้อมของผู้ให้บริการ แนวทางการปฏิบัติหน้าที่ และข้อกำหนดในการดำเนินงานตามประเภทบริการ เพื่อให้การดำเนินงานเกี่ยวกับหลักทรัพย์โทเคนมีความถูกต้อง ครบถ้วน มั่นคงปลอดภัย โปร่งใส และสามารถตรวจสอบย้อนหลังได้ รวมทั้งคำนึงถึงความเป็นหนึ่งเดียวของหลักทรัพย์โทเคน การควบคุมหลักทรัพย์โดยผู้มีสิทธิ และความสอดคล้องระหว่างข้อมูลในระบบกับสิทธิของผู้ถือหลักทรัพย์ตามกฎหมาย ตลอดจนหลักการที่เกี่ยวข้องกับตราสารเปลี่ยนมืออิเล็กทรอนิกส์ (Electronic Transferable Records: ETR) ตามแนวทางของ UNCITRAL Model Law on Electronic Transferable Records (MLETR) ในส่วนที่เกี่ยวข้อง นอกจากนี้ มาตรฐานในบทนี้ยังมีวัตถุประสงค์เพื่อส่งเสริมให้ผู้ให้บริการสนับสนุนการออกและเสนอขายหลักทรัพย์โทเคนสามารถดำเนินงานได้อย่างเหมาะสมกับลักษณะและความเสี่ยงของบริการ สนับสนุนการเชื่อมโยงและการทำงานร่วมกันระหว่างผู้เกี่ยวข้องในระบบนิเวศหลักทรัพย์โทเคน และรักษาความเชื่อมั่นและความน่าเชื่อถือของตลาดทุน โดยคำนึงถึงการคุ้มครองผู้ลงทุนและการรักษาความมั่นคงของระบบตลาดทุนเป็นสำคัญ

5.1 บทบาทและขอบเขตของผู้ให้บริการ (Scope of Services)

ผู้ให้บริการสนับสนุนการออกหลักทรัพย์ในรูปแบบโทเคน (Securities Tokenizer) อาจมีรูปแบบการประกอบธุรกิจและขอบเขตการให้บริการที่แตกต่างกัน โดยอาจให้บริการหรือดำเนินการในด้านต่าง ๆ ที่เกี่ยวข้องกับวงจรชีวิตของหลักทรัพย์โทเคน เช่น การออก การจัดทำและบันทึกข้อมูล การส่งมอบ การโอน การใช้เป็นหลักประกัน การให้บริการด้านกระเป๋าอิเล็กทรอนิกส์ (Wallet) หรือการรับฝากหรือเก็บรักษาหลักทรัพย์โทเคน เป็นต้น ทั้งนี้ Securities Tokenizer ไม่จำเป็นต้องดำเนินการทุกด้าน และอาจแบ่งหน้าที่กับผู้ออกหลักทรัพย์ นายทะเบียน ผู้รับฝากทรัพย์สิน หรือผู้ให้บริการโครงสร้างพื้นฐานรายอื่นตามรูปแบบการให้บริการ

กลุ่มงานที่ Securities Tokenizer อาจให้บริการหรือดำเนินการ อาจครอบคลุมงานหลักดังต่อไปนี้

(1) งานด้านการออก การบันทึก การทำรายการ และการดูแลหลักทรัพย์โทเคน

งานในกลุ่มนี้เกี่ยวข้องกับการจัดให้หลักทรัพย์สามารถถูกสร้างและออกในรูปแบบโทเคน การจัดทำและบันทึกข้อมูลเกี่ยวกับหลักทรัพย์และผู้ถือหลักทรัพย์ ตลอดจนการดำเนินการที่ทำให้เกิดหรือเปลี่ยนแปลงสถานะ สิทธิ หรือความเป็นเจ้าของในหลักทรัพย์โทเคนตลอดวงจรชีวิตของหลักทรัพย์

การให้บริการในกลุ่มนี้อาจครอบคลุมตั้งแต่การออกหลักทรัพย์ การจัดทำและดูแลข้อมูลหรือทะเบียนหลักทรัพย์ การส่งมอบและรับมอบ การโอนและรับโอน การใช้หลักทรัพย์เป็นหลักประกัน ตลอดจนการดำเนินการที่เกี่ยวข้องกับสิทธิประโยชน์และการดำเนินการตามสิทธิของผู้ถือหลักทรัพย์ตลอดอายุของหลักทรัพย์หรือเมื่อสิ้นสุดอายุของหลักทรัพย์ ทั้งนี้ Securities Tokenizer อาจรับผิดชอบเฉพาะบางงาน หรือดำเนินการหลายงานร่วมกันตามรูปแบบการให้บริการและการแบ่งหน้าที่กับผู้ออกหลักทรัพย์ นายทะเบียน หรือผู้ให้บริการโครงสร้างพื้นฐานรายอื่น

งานที่อาจอยู่ในกลุ่มนี้ เช่น

- **การออกหลักทรัพย์โทเคน (Token Issuance)** - การจัดให้มีระบบหรือกลไกสำหรับการสร้างและออกหลักทรัพย์ในรูปแบบโทเคนตามรายละเอียดและเงื่อนไขของหลักทรัพย์ที่กำหนด
- **การจัดทำและบันทึกข้อมูลหลักทรัพย์โทเคน (Registration / Record)** - การจัดทำและบันทึกข้อมูลที่ใช้ระบุหลักทรัพย์ ผู้ถือหลักทรัพย์ และสิทธิหรือสถานะที่เกี่ยวข้อง รวมถึงการปรับปรุงข้อมูลดังกล่าวตามการเปลี่ยนแปลงที่เกิดขึ้น
- **การส่งมอบและรับมอบหลักทรัพย์โทเคน (Delivery)** – การดำเนินการเพื่อส่งมอบหลักทรัพย์โทเคนให้แก่ผู้รับตามเงื่อนไขของการออกหรือธุรกรรมที่เกี่ยวข้อง

- **การโอนและรับโอนหลักทรัพย์โทเคน (Transfer)** – การดำเนินการเพื่อเปลี่ยนแปลงผู้ถือหรือสิทธิในหลักทรัพย์โทเคนจากบุคคลหนึ่งไปยังอีกบุคคลหนึ่ง
- **การใช้หลักทรัพย์โทเคนเป็นหลักประกัน (Pledge)** - การดำเนินการที่เกี่ยวข้องกับการนำหลักทรัพย์โทเคนไปเป็นหลักประกัน รวมถึงการสร้าง เปลี่ยนแปลง หรือปลดภาระที่เกี่ยวข้องกับหลักประกัน
- **การให้บริการด้านสิทธิประโยชน์และการดำเนินการตามสิทธิของผู้ถือหลักทรัพย์โทเคน (Asset Servicing / Corporate Actions)** – การดำเนินการที่เกี่ยวข้องกับสิทธิประโยชน์หรือสิทธิของผู้ถือหลักทรัพย์โทเคนตลอดอายุของหลักทรัพย์ เช่น การจ่ายดอกเบี้ย เงินปันผล การไถ่ถอน การครบกำหนด การแปลงสภาพ หรือการดำเนินการอื่นที่มีผลต่อสิทธิของผู้ถือหลักทรัพย์

(2) งานด้านการถือครองและการดูแลรักษาหลักทรัพย์โทเคน

งานในกลุ่มนี้เกี่ยวข้องกับการจัดให้ผู้ลงทุนหรือผู้มีสิทธิสามารถถือครอง เข้าถึง และควบคุมหลักทรัพย์โทเคนผ่านกลไกทางอิเล็กทรอนิกส์ที่เหมาะสม โดยอาจครอบคลุมตั้งแต่การจัดให้มีโครงสร้างพื้นฐานหรือระบบกระเป๋าอิเล็กทรอนิกส์ (Wallet) ไปจนถึงการรับฝากหรือเก็บรักษาหลักทรัพย์โทเคนแทนผู้ลงทุน ทั้งนี้ รูปแบบการให้บริการและระดับการควบคุมหลักทรัพย์โทเคนของ Securities Tokenizer อาจแตกต่างกันได้

งานในกลุ่มนี้อาจดำเนินการโดย Securities Tokenizer เอง หรือ Securities Tokenizer อาจจัดให้มีหรือเชื่อมต่อกับผู้ให้บริการรายอื่นเพื่อรองรับการถือครองและการควบคุมหลักทรัพย์โทเคน โดยเฉพาะในกรณีที่ Securities Tokenizer ให้บริการในลักษณะรับฝากหรือเก็บรักษาหลักทรัพย์โทเคน (Custody) ซึ่งอาจเกี่ยวข้องกับการควบคุมกุญแจหรือกลไกอื่นที่ทำให้สามารถควบคุมหลักทรัพย์โทเคนได้

งานที่อาจอยู่ในกลุ่มนี้ เช่น

- **การจัดให้มีหรือให้บริการเกี่ยวกับ Non-Custodial Wallet** – การจัดให้มีระบบหรือโครงสร้างพื้นฐานสำหรับการถือครองและเข้าถึงหลักทรัพย์โทเคน โดยผู้ลงทุนเป็นผู้ถือครองหรือควบคุมหลักทรัพย์โทเคนด้วยตนเอง หรือการเชื่อมต่อหรืออำนวยให้ผู้ลงทุนสามารถใช้ Wallet ที่จัดให้โดยผู้ให้บริการรายอื่น
- **การรับฝากหรือเก็บรักษาหลักทรัพย์โทเคน (Custodial Service)** – การรับฝากหรือเก็บรักษาหลักทรัพย์โทเคนหรือทรัพย์สินของลูกค้า รวมถึงการดูแลรักษาหรือควบคุมกุญแจหรือกลไกอื่นที่ใช้ในการควบคุมหลักทรัพย์โทเคนแทนลูกค้า

(3) งานด้านการชำระราคาและการส่งมอบหลักทรัพย์โทเคน (Settlement)

งานในกลุ่มนี้เกี่ยวข้องกับการจัดให้มีกระบวนการและกลไกสำหรับการชำระธุรกรรมหลักทรัพย์โทเคน ภายหลังจากมีการทำรายการซื้อขายหรือธุรกรรมที่กำหนดให้มีการแลกเปลี่ยนหลักทรัพย์กับเงินหรือทรัพย์สินอื่นที่ใช้ชำระราคา เพื่อให้การชำระราคาและการส่งมอบหลักทรัพย์เป็นไปตามเงื่อนไขของธุรกรรม

การให้บริการในกลุ่มนี้อาจครอบคลุมตั้งแต่การจัดการและประมวลผลธุรกรรมที่เข้าสู่กระบวนการชำระราคา การจัดให้มีกลไกสำหรับการชำระราคาและส่งมอบหลักทรัพย์ที่เชื่อมโยงกันตลอดจนการเชื่อมต่อกับระบบหรือสินทรัพย์ที่ใช้ในการชำระราคา ทั้งนี้ Securities Tokenizer อาจรับผิดชอบเฉพาะบางส่วนของกระบวนการ หรือให้บริการโครงสร้างพื้นฐานสำหรับการชำระราคาทั้งกระบวนการตามรูปแบบการให้บริการ

งานที่อาจอยู่ในกลุ่มนี้ เช่น

- **การจัดการกระบวนการชำระราคา (Settlement Processing)** - การรับและประมวลผลข้อมูลหรือคำสั่งที่เกี่ยวข้องกับการชำระราคา และการดำเนินการที่ทำให้ธุรกรรมเข้าสู่กระบวนการชำระราคา
- **การชำระราคาและส่งมอบหลักทรัพย์แบบ Delivery-versus-Payment : DvP**[5] - การจัดให้มีกลไกที่เชื่อมโยงการส่งมอบหลักทรัพย์โทเคนกับการชำระเงิน เพื่อให้การส่งมอบและการชำระเงินเกิดขึ้นตามเงื่อนไขที่กำหนด
- **การเชื่อมต่อกับระบบหรือสินทรัพย์ที่ใช้ในการชำระราคา** - การเชื่อมต่อกับระบบการชำระเงิน หรือสินทรัพย์ที่ใช้ชำระราคา เช่น เงินหรือเงินในรูปแบบโทเคน เพื่อรองรับการชำระธุรกรรมหลักทรัพย์โทเคน
- **การติดตามและจัดการสถานะการชำระราคา** - การจัดให้มีกลไกสำหรับติดตาม ตรวจสอบ และปรับปรุงสถานะของธุรกรรมในกระบวนการชำระราคา รวมถึงการระบุผลของการชำระราคาและการส่งมอบหลักทรัพย์

5.2 คุณสมบัติและความพร้อมของผู้ให้บริการสนับสนุนการออกและเสนอขายหลักทรัพย์โทเคน (Eligibility and Qualifications)

ผู้ให้บริการสนับสนุนการออกและเสนอขายหลักทรัพย์โทเคนต้องมีความพร้อมในการประกอบธุรกิจและให้บริการตามบทบาทและขอบเขตการให้บริการที่ตนรับผิดชอบ โดยมีฐานะ

[5] **Delivery versus Payment (DvP)** คือกลไกที่กำหนดให้การโอนหรือส่งมอบหลักทรัพย์โทเคนและการชำระเงินที่เกี่ยวข้องเกิดขึ้นโดยเชื่อมโยงกัน เพื่อให้การส่งมอบหลักทรัพย์โทเคนเกิดขึ้นต่อเมื่อมีการชำระเงิน และการชำระเงินเกิดขึ้นต่อเมื่อมีการส่งมอบหลักทรัพย์โทเคนที่เกี่ยวข้อง

ทางการเงิน โครงสร้างองค์กร บุคลากร และระบบงานที่เพียงพอและเหมาะสมกับลักษณะ ขนาด ความซับซ้อน และระดับความเสี่ยงของการให้บริการ

ทั้งนี้ ผู้ให้บริการควรจัดให้มีการกำกับดูแลและควบคุมการดำเนินงานอย่างเหมาะสม เพื่อให้สามารถปฏิบัติหน้าที่ได้อย่างมีประสิทธิภาพ มีความน่าเชื่อถือ และสามารถรองรับความเสี่ยงและเหตุการณ์ที่อาจกระทบต่อการให้บริการได้อย่างเหมาะสม รวมถึงควรมีการติดตาม ทบทวน และปรับปรุงความพร้อมดังกล่าวให้สอดคล้องกับการเปลี่ยนแปลงของบทบาท ขอบเขต และลักษณะการให้บริการ

5.2.1 ฐานะทางการเงินและเงินทุน

หลักการทั่วไป

ผู้ให้บริการสนับสนุนการออกและเสนอขายหลักทรัพย์โทเคนต้องมีฐานะทางการเงินและแหล่งเงินทุนที่เพียงพอและเหมาะสมกับลักษณะ ขนาด และความเสี่ยงของการประกอบธุรกิจ เพื่อให้สามารถดำเนินธุรกิจได้อย่างต่อเนื่อง รองรับค่าใช้จ่ายและความเสี่ยงที่อาจเกิดขึ้นจากการประกอบธุรกิจ และรักษาความพร้อมในการให้บริการได้อย่างเหมาะสม รวมทั้งต้องมีแผนรองรับกรณีที่แหล่งเงินทุนไม่เพียงพอ

ข้อเสนอแนะ : เพื่อให้ผู้ให้บริการมีฐานะทางการเงินและแหล่งเงินทุนที่เพียงพอต่อการดำเนินธุรกิจอย่างต่อเนื่องและสามารถรองรับความเสี่ยงที่อาจเกิดขึ้น ผู้ให้บริการควรพิจารณาดำเนินการ ดังนี้

(1) ผู้ให้บริการควรดำรงส่วนของผู้ถือหุ้นหรือแหล่งเงินทุนที่มีคุณภาพและมีสภาพคล่องเพียงพอสำหรับรองรับค่าใช้จ่ายในการประกอบธุรกิจอย่างต่อเนื่อง **โดยในเบื้องต้นควรมีมูลค่าไม่น้อยกว่าค่าใช้จ่ายในการประกอบธุรกิจในระยะเวลา 6 เดือน โดยคำนวณจากงบการเงินล่าสุด** ทั้งนี้อาจกำหนดระดับเงินทุนที่สูงขึ้นตามลักษณะ ขนาด ความซับซ้อน และความเสี่ยงของการประกอบธุรกิจ

(2) ผู้ให้บริการควรจัดให้มีการประเมินความเพียงพอของเงินทุนและแหล่งเงินทุนอย่างสม่ำเสมอ โดยคำนึงถึงความเสี่ยงที่อาจเกิดขึ้นจากบริการที่ตนให้บริการ รวมถึงภาระผูกพันที่อาจเกิดขึ้นจากการดำเนินงาน

(3) ผู้ให้บริการควรจัดให้มีแผนรองรับกรณีที่เงินทุนหรือสภาพคล่องไม่เพียงพอต่อการดำเนินธุรกิจ รวมถึงแนวทางในการจัดหาเงินทุนเพิ่มเติม การลดหรือปรับขอบเขตการให้บริการ และการดำเนินการเพื่อให้สามารถให้บริการที่มีความสำคัญได้อย่างต่อเนื่อง

5.2.2 โครงสร้างองค์กรและการกำกับดูแล

หลักการทั่วไป

ผู้ให้บริการควรจัดให้มีโครงสร้างองค์กรและการกำกับดูแลที่ชัดเจนและเหมาะสมกับลักษณะ ขนาด ความซับซ้อน และขอบเขตการให้บริการ โดยกำหนดหน้าที่ ความรับผิดชอบ และอำนาจ

ในการตัดสินใจของผู้เกี่ยวข้องอย่างเหมาะสม รวมทั้งมีกลไกในการกำกับ ติดตาม และสอบทานการดำเนินงาน เพื่อให้การให้บริการเป็นไปอย่างมีประสิทธิภาพ โปร่งใส และสามารถจัดการความเสี่ยงและความขัดแย้งทางผลประโยชน์ได้อย่างเหมาะสม

ข้อเสนอแนะ : เพื่อให้โครงสร้างองค์กรและการกำกับดูแลสามารถรองรับการประกอบธุรกิจและขอบเขตการให้บริการ ผู้ให้บริการควรพิจารณาดำเนินการ ดังนี้

(1) โครงสร้างองค์กรและการแบ่งหน้าที่ความรับผิดชอบ : ผู้ให้บริการควรจัดให้มีโครงสร้างองค์กรที่ชัดเจนและเหมาะสมกับลักษณะ ขนาด ความซับซ้อน และขอบเขตการให้บริการ โดยควรกำหนดบทบาท หน้าที่ ความรับผิดชอบ และอำนาจในการตัดสินใจของคณะกรรมการ ผู้บริหาร และผู้ปฏิบัติงานที่เกี่ยวข้องกับการให้บริการไว้อย่างชัดเจน และจัดให้มีการมอบหมายหน้าที่ที่สอดคล้องกับอำนาจและความรับผิดชอบของแต่ละตำแหน่ง

ผู้ให้บริการควรสามารถระบุผู้รับผิดชอบหลักของแต่ละบทบาทหน้าที่หรืองานที่มีความสำคัญต่อการให้บริการได้อย่างชัดเจน รวมถึงกำหนดสายการบังคับบัญชาและการรายงานที่เหมาะสม เพื่อให้สามารถกำกับ ติดตาม และแก้ไขปัญหาที่เกิดขึ้นในแต่ละงานได้อย่างทันท่วงที ทั้งนี้ โครงสร้างดังกล่าวควรครอบคลุมบทบาทหน้าที่ที่ผู้ให้บริการเลือกดำเนินการตามขอบเขตการให้บริการที่กำหนดไว้ในข้อ 5.1

ในกรณีที่งานใดมีการแบ่งหน้าที่ระหว่างหลายหน่วยงานหรือหลายบุคคล ผู้ให้บริการควรกำหนดขอบเขตความรับผิดชอบและจุดเชื่อมต่อระหว่างแต่ละฝ่ายให้ชัดเจน เพื่อไม่ให้เกิดช่องว่างหรือความซ้ำซ้อนของความรับผิดชอบ และควรจัดให้มีการทบทวนโครงสร้างและการแบ่งหน้าที่ดังกล่าวเมื่อมีการเปลี่ยนแปลงขอบเขตการให้บริการ โครงสร้างองค์กร หรือความเสี่ยงที่เกี่ยวข้องอย่างมีนัยสำคัญ

(2) การแบ่งแยกหน้าที่และการสอบทานการปฏิบัติงาน : ผู้ให้บริการควรจัดให้มีการแบ่งแยกหน้าที่และความรับผิดชอบระหว่างบุคคลหรือหน่วยงานที่เกี่ยวข้องกับงานที่มีความเสี่ยงหรืออาจก่อให้เกิดความขัดแย้งทางผลประโยชน์อย่างเหมาะสม เพื่อให้การปฏิบัติงาน การอนุมัติ และการตรวจสอบหรือสอบทานการปฏิบัติงานมีการควบคุมและถ่วงดุลที่เหมาะสม และลดความเสี่ยงจากการที่บุคคลใดบุคคลหนึ่งสามารถดำเนินการที่สำคัญได้โดยลำพังโดยไม่มีการควบคุมหรือสอบทานที่เหมาะสม

ทั้งนี้ ระดับของการแบ่งแยกหน้าที่ควรสอดคล้องกับ ลักษณะ ความสำคัญ และความเสี่ยงของแต่ละบทบาทหน้าที่ โดยเฉพาะงานที่เกี่ยวข้องกับการสร้าง ออก โอน หรือเปลี่ยนแปลงสิทธิในหลักทรัพย์โทเคน การควบคุมหรืออนุมัติธุรกรรม การควบคุมกุญแจหรือสิทธิในการดำเนินการที่สำคัญ

และการชำระราคาและส่งมอบหลักทรัพย์ โดยผู้ให้บริการควรพิจารณา จัดให้มีการอนุมัติหรือ สอบทานโดยบุคคลอื่นก่อนหรือภายหลังการดำเนินการตามความเหมาะสม

ในกรณีที่ขนาดหรือโครงสร้างของผู้ให้บริการไม่เอื้อให้สามารถแบ่งแยกหน้าที่ระหว่างบุคคลหรือหน่วยงานได้อย่างสมบูรณ์ ผู้ให้บริการควรจัดให้มีกลไกการควบคุมหรือการสอบทานอื่นที่มีประสิทธิผลเพียงพอเพื่อให้บรรลุวัตถุประสงค์เดียวกัน และควรมีการทบทวนความเหมาะสมของการแบ่งแยกหน้าที่ดังกล่าวเป็นระยะ

(3) การกำกับดูแลและการตัดสินใจ : ผู้ให้บริการควรจัดให้มีกลไกหรือโครงสร้างการกำกับดูแลที่เหมาะสมกับลักษณะ ขนาด ความซับซ้อน และขอบเขตการให้บริการ เพื่อกำกับดูแลการดำเนินงานของผู้ให้บริการให้เป็นไปอย่างมีประสิทธิภาพ โปร่งใส และสอดคล้องกับหน้าที่และความรับผิดชอบที่กำหนดไว้ โดยควรกำหนดบทบาท หน้าที่ และความรับผิดชอบของคณะกรรมการหรือผู้ทำหน้าที่กำกับดูแล และผู้บริหารไว้อย่างชัดเจน รวมถึงจัดให้มีการติดตามและประเมินการปฏิบัติหน้าที่ของบุคคลดังกล่าวอย่างเหมาะสม

ผู้ให้บริการควรกำหนดกระบวนการในการตัดสินใจและการอนุมัติในเรื่องที่มีนัยสำคัญต่อการดำเนินงานหรือความเสี่ยงของผู้ใช้บริการ โดยกำหนดเรื่องที่ต้องได้รับการพิจารณาหรืออนุมัติจากคณะกรรมการหรือผู้มีอำนาจกำกับดูแลในระดับที่เหมาะสม และจัดให้มีการรายงานข้อมูลที่จำเป็นต่อการกำกับดูแลและการตัดสินใจอย่างเพียงพอ ถูกต้อง และทันต่อเหตุการณ์

ทั้งนี้ กลไกการกำกับดูแลควรครอบคลุมการติดตามและทบทวนการดำเนินงานของผู้ให้บริการว่าเป็นไปตามนโยบาย ขอบเขตการให้บริการ และหน้าที่ที่กำหนด รวมถึงการทบทวนและปรับปรุงนโยบายหรือกระบวนการที่เกี่ยวข้องเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญต่อการประกอบธุรกิจหรือความเสี่ยงของผู้ให้บริการ

ตัวอย่างเรื่องที่ควรพิจารณากำหนดให้มีการยกระดับการตัดสินใจหรือรายงาน เช่น

- การเปลี่ยนแปลงขอบเขตหรือรูปแบบการให้บริการที่มีนัยสำคัญ
- การเริ่มให้บริการในรูปแบบหรือระบบงานใหม่ที่มีความเสี่ยงสูง
- เหตุการณ์ที่อาจกระทบต่อสิทธิหรือทรัพย์สินของผู้ใช้บริการอย่างมีนัยสำคัญ
- การเปลี่ยนแปลงที่มีผลต่อความถูกต้องหรือความน่าเชื่อถือของข้อมูลหลักทรัพย์หรือทะเบียน
- เหตุการณ์ที่อาจกระทบต่อความต่อเนื่องในการให้บริการหรือการทำรายการของผู้ใช้บริการ

(4) การป้องกันและจัดการความขัดแย้งทางผลประโยชน์ : ผู้ให้บริการควรจัดให้มีนโยบายและกระบวนการในการ ระบุ ป้องกัน และจัดการความขัดแย้งทางผลประโยชน์ ที่อาจเกิดขึ้นจากการประกอบธุรกิจ โดยควรครอบคลุมความขัดแย้งทางผลประโยชน์ระหว่างผู้ให้บริการกับผู้ใช้บริการระหว่างผู้ใช้บริการแต่ละราย หรือระหว่างการให้บริการแต่ละประเภท รวมถึงความขัดแย้งที่อาจเกิดจากการประกอบธุรกิจอื่นของผู้ให้บริการหรือบุคคลที่เกี่ยวข้อง

ผู้ให้บริการควรจัดให้มีมาตรการที่เหมาะสมในการป้องกันมิให้บุคคลที่เกี่ยวข้องกับการให้บริการ ได้แก่ กรรมการ ผู้บริหาร พนักงาน หรือผู้ปฏิบัติงานที่เกี่ยวข้อง ใช้ข้อมูลหรืออำนาจหน้าที่ที่ได้รับจากการปฏิบัติงานเพื่อแสวงหาประโยชน์โดยมิชอบ หรือก่อให้เกิดความเสียหายแก่ผู้ใช้บริการ รวมถึงควรกำหนดแนวทางในการเปิดเผย การจัดการ หรือการหลีกเลี่ยงความขัดแย้งทางผลประโยชน์เมื่อไม่สามารถป้องกันไม่ให้เกิดขึ้นได้

ในกรณีที่ผู้ให้บริการประกอบธุรกิจอื่น หรือให้บริการหลายด้านที่อาจก่อให้เกิดความขัดแย้งทางผลประโยชน์ ผู้ให้บริการควรประเมินความเสี่ยงดังกล่าวและจัดให้มีมาตรการควบคุมที่เหมาะสม เช่น การแบ่งแยกหน้าที่หรือการเข้าถึงข้อมูล การกำหนดผู้มีอำนาจอนุมัติหรือสอบทานการเปิดเผยความขัดแย้งทางผลประโยชน์ หรือการกำหนดข้อจำกัดในการดำเนินการ ทั้งนี้ ระดับของมาตรการควรสอดคล้องกับลักษณะและความรุนแรงของความขัดแย้งที่อาจเกิดขึ้น

5.2.3 บุคลากรและความเหมาะสมในการปฏิบัติหน้าที่

หลักการทั่วไป

ผู้ให้บริการควรจัดให้มีบุคลากรที่มีจำนวน ความรู้ ความสามารถ และประสบการณ์ที่เหมาะสมกับลักษณะ ขนาด ความซับซ้อน และขอบเขตการให้บริการ เพื่อให้สามารถปฏิบัติหน้าที่และบริหารความเสี่ยงที่เกี่ยวข้องกับการให้บริการได้อย่างมีประสิทธิภาพ ทั้งนี้ บุคลากรที่รับผิดชอบในแต่ละหน้าที่ควรมีคุณสมบัติและความสามารถสอดคล้องกับลักษณะและความเสี่ยงของหน้าที่ที่ได้รับมอบหมาย

ข้อเสนอแนะ : ผู้ให้บริการควรจัดให้มีบุคลากรที่มีจำนวนและคุณสมบัติเหมาะสมเพื่อให้สามารถปฏิบัติหน้าที่และบริหารจัดการความเสี่ยงที่เกี่ยวข้องได้อย่างมีประสิทธิภาพและต่อเนื่อง โดยควรพิจารณาดำเนินการ ดังนี้

(1) ความเพียงพอของบุคลากร : ผู้ให้บริการควรจัดให้มีบุคลากรในจำนวนที่เพียงพอและเหมาะสมกับขนาด ความซับซ้อน และขอบเขตการให้บริการ เพื่อให้สามารถดำเนินงานในแต่ละหน้าที่ได้อย่างต่อเนื่อง และรองรับภาระงานหรือสถานการณ์ที่อาจเกิดขึ้นจากการประกอบธุรกิจได้อย่างเหมาะสม

ในการพิจารณาความเพียงพอของบุคลากร ผู้ให้บริการควรคำนึงถึงลักษณะและปริมาณงาน ความสำคัญของแต่ละหน้าที่ ความจำเป็นในการปฏิบัติงานหรือให้บริการอย่างต่อเนื่อง

รวมถึงการจัดให้มีบุคลากรทดแทนในกรณีที่บุคลากรที่รับผิดชอบหลักไม่สามารถปฏิบัติหน้าที่ได้ เพื่อไม่ให้การดำเนินงานที่มีความสำคัญต้องหยุดชะงักหรือพึ่งพาบุคคลใดบุคคลหนึ่งมากเกินสมควร

(2) ความรู้ ความสามารถ และประสบการณ์ตามหน้าที่ : ผู้ให้บริการควรจัดให้บุคลากรที่รับผิดชอบในแต่ละหน้าที่ มีความรู้ ความสามารถ และประสบการณ์ที่เหมาะสมกับหน้าที่และความรับผิดชอบที่ได้รับมอบหมาย โดยควรคำนึงถึงลักษณะ ความซับซ้อน และความเสี่ยงของงานที่รับผิดชอบ ควรมีความรู้ความเข้าใจเกี่ยวกับระบบ DLT ระบบหรือกลไกของโทเคน การจัดการ Wallet หรือ Key การรับฝากหรือเก็บรักษาทรัพย์สิน และกระบวนการชำระราคาและส่งมอบตามลักษณะของหน้าที่ที่รับผิดชอบ นอกจากนี้ ผู้ให้บริการควรจัดให้มีการประเมินความเหมาะสมของบุคลากรกับหน้าที่ที่ได้รับมอบหมาย และไม่ควรมอบหมายหน้าที่ที่มีความสำคัญหรือมีความเสี่ยงสูงแก่บุคลากรที่ไม่มีความรู้ความสามารถ หรือประสบการณ์ที่เพียงพอต่อการปฏิบัติหน้าที่ดังกล่าว

บุคลากรที่ปฏิบัติหน้าที่ที่เกี่ยวข้องกับการออกและให้บริการหลักทรัพย์โทเคนควรมีความรู้หรือประสบการณ์ที่เกี่ยวข้องกับหลักทรัพย์ กระบวนการทำงานของตลาดทุน และเทคโนโลยีที่ใช้ในการให้บริการในระดับที่เหมาะสมกับหน้าที่

(3) การพัฒนาและทบทวนความรู้ความสามารถของบุคลากร: ผู้ให้บริการควรจัดให้มีการพัฒนาและทบทวนความรู้ ความสามารถ และประสบการณ์ของบุคลากรอย่างเหมาะสมและต่อเนื่อง เพื่อให้บุคลากรสามารถปฏิบัติหน้าที่ได้สอดคล้องกับการเปลี่ยนแปลงของลักษณะและขอบเขตการให้บริการ เทคโนโลยี กฎเกณฑ์ และความเสี่ยงที่เกี่ยวข้อง

ผู้ให้บริการควรจัดให้มีการอบรมหรือพัฒนาความรู้ที่จำเป็นต่อการปฏิบัติหน้าที่ รวมถึงควรประเมินความเหมาะสมของบุคลากรเป็นระยะ และเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญต่อหน้าที่หรือความรับผิดชอบ เพื่อให้มั่นใจว่าบุคลากรยังคงมีความรู้และความสามารถที่เหมาะสมกับหน้าที่ที่ได้รับมอบหมาย

5.2.4 ระบบงานและความพร้อมในการให้บริการ

ผู้ให้บริการสนับสนุนการออกและเสนอขายหลักทรัพย์โทเคนควรจัดให้มีระบบงาน กระบวนการ และการควบคุมที่เพียงพอและเหมาะสมกับลักษณะ ขนาด ความซับซ้อน และระดับความเสี่ยงของการให้บริการ เพื่อให้สามารถดำเนินงานได้อย่างถูกต้อง มีประสิทธิภาพ ปลอดภัย และต่อเนื่อง รวมทั้งสามารถบริหารจัดการความเสี่ยง เหตุการณ์ผิดปกติ และสถานการณ์ที่อาจส่งผลกระทบต่อการให้บริการได้อย่างเหมาะสม นอกจากนี้ ผู้ให้บริการยังต้องคำนึงถึงความมั่นคงปลอดภัย ความถูกต้องครบถ้วน และความพร้อมใช้ของระบบงานและข้อมูลที่เกี่ยวข้องกับการให้บริการร่วมด้วย

ระบบงานและกระบวนการดังกล่าวควรครอบคลุมระบบงานและกลไกสนับสนุนการประกอบธุรกิจและการควบคุมการปฏิบัติงาน ทั้งในภาวะปกติและกรณีที่เกิดเหตุการณ์ผิดปกติหรือ

การหยุดชะงัก โดยคำนึงถึงความสำคัญของงานที่ให้บริการ การพึ่งพาระบบหรือผู้ให้บริการอื่น และผลกระทบที่อาจเกิดขึ้นต่อผู้ใช้บริการ ผู้ถือหลักทรัพย์โทเคน และผู้ที่เกี่ยวข้อง ทั้งนี้ ระดับของระบบงานและการควบคุมควรสอดคล้องกับบทบาทและขอบเขตการให้บริการของ Securities Tokenizer

ผู้ให้บริการสนับสนุนการออกและเสนอขายหลักทรัพย์โทเคนควรจัดให้มี ระบบงานสนับสนุนดังต่อไปนี้

- **ระบบบริหารความเสี่ยงและการควบคุมภายใน**

หลักการทั่วไป

ผู้ให้บริการสนับสนุนการออกและเสนอขายหลักทรัพย์โทเคนต้องจัดให้มีกระบวนการบริหารจัดการและควบคุมความเสี่ยงที่เหมาะสมกับลักษณะ ขนาด ความซับซ้อน และความเสี่ยงของการให้บริการ โดยครอบคลุมความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินงาน รวมถึงความเสี่ยงด้านเทคโนโลยี กฎหมาย และความเสี่ยงอื่นที่เกี่ยวข้อง ตลอดจนจัดให้มีระบบควบคุมภายในที่เหมาะสมเพื่อให้การปฏิบัติงานเป็นไปตามกฎหมาย หลักเกณฑ์ และกระบวนการที่กำหนด

ทั้งนี้ ระบบดังกล่าวควรช่วยให้ผู้ให้บริการสามารถระบุ ประเมิน ติดตาม ควบคุม และจัดการความเสี่ยงได้อย่างเหมาะสม รวมถึงสามารถทบทวนและปรับปรุงมาตรการควบคุมให้สอดคล้องกับการเปลี่ยนแปลงของธุรกิจ เทคโนโลยี และความเสี่ยงที่เกี่ยวข้องได้อย่างต่อเนื่อง

ข้อเสนอแนะ : ผู้ให้บริการควรจัดให้มีกรอบการบริหารความเสี่ยงและระบบควบคุมภายในที่เหมาะสมกับลักษณะและความเสี่ยงของการให้บริการ โดยอย่างน้อยควรครอบคลุมเรื่องดังต่อไปนี้

(1) การระบุและประเมินความเสี่ยง : ผู้ให้บริการควรจัดให้มีกระบวนการในการระบุและประเมินความเสี่ยงที่อาจเกิดขึ้นจากการให้บริการอย่างเป็นระบบ โดยครอบคลุมความเสี่ยงที่เกี่ยวข้องกับลักษณะและขอบเขตการให้บริการของตน รวมถึงความเสี่ยงด้านการดำเนินงาน เทคโนโลยี กฎหมาย และความเสี่ยงอื่นที่เกี่ยวข้อง ทั้งนี้ ควรพิจารณาถึงโอกาสที่จะเกิดขึ้นและผลกระทบของความเสี่ยงดังกล่าว รวมถึงการเปลี่ยนแปลงของกิจกรรม กระบวนการ ระบบงาน หรือเทคโนโลยีที่อาจทำให้ระดับหรือประเภทของความเสี่ยงเปลี่ยนแปลงไป

(2) การกำหนดมาตรการควบคุมและจัดการความเสี่ยง : ผู้ให้บริการควรจัดให้มีมาตรการในการควบคุมและจัดการความเสี่ยงที่ระบุและประเมินไว้ตาม (1) อย่างเหมาะสมกับลักษณะและระดับความเสี่ยงของการให้บริการ โดยควรกำหนดวิธีการควบคุม ผู้รับผิดชอบ และแนวทางดำเนินการเมื่อเกิดเหตุการณ์หรือความเสี่ยงขึ้น เพื่อให้สามารถป้องกัน ลด หรือจำกัดผลกระทบจากความเสี่ยงดังกล่าวได้อย่างเหมาะสม

(3) การติดตาม ทบทวน และรายงานความเสี่ยง : ผู้ให้บริการควรจัดให้มีกระบวนการติดตามและทบทวนการบริหารความเสี่ยงและมาตรการควบคุมภายในอย่างสม่ำเสมอ เพื่อประเมินว่ามาตรการดังกล่าวยังมีความเหมาะสมและมีประสิทธิผลในการจัดการความเสี่ยงที่เกี่ยวข้องกับการให้บริการ รวมทั้งควรมีการรายงานและยกระดับความเสี่ยงหรือข้อบกพร่องที่มีนัยสำคัญต่อผู้บริหารหรือคณะกรรมการตามระดับความสำคัญ เช่น กรณีที่ความเสี่ยงเพิ่มขึ้นจนเกินระดับที่กำหนด หรือพบว่ามาตรการควบคุมที่มีอยู่ไม่สามารถจัดการความเสี่ยงดังกล่าวได้อย่างเหมาะสม ทั้งนี้ ควรมีการปรับปรุงมาตรการบริหารความเสี่ยงและการควบคุมภายในเมื่อพบข้อบกพร่อง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญต่อการประกอบธุรกิจ ระบบงาน เทคโนโลยี หรือระดับความเสี่ยงของผู้ให้บริการ

(4) การจัดทำและเก็บรักษาข้อมูลและหลักฐานที่เกี่ยวข้อง : ผู้ให้บริการควรจัดให้มีการจัดทำและเก็บรักษาข้อมูลและหลักฐานที่เกี่ยวข้องกับการบริหารความเสี่ยงและการควบคุมภายในอย่างเหมาะสม เพื่อให้สามารถตรวจสอบและติดตามการดำเนินงานย้อนหลังได้ รวมถึงสามารถแสดงให้เห็นถึงการระบุและประเมินความเสี่ยง การกำหนดและดำเนินมาตรการควบคุม การติดตามและทบทวน ตลอดจนการดำเนินการแก้ไขเมื่อพบข้อบกพร่อง

ทั้งนี้ ข้อมูลและหลักฐานดังกล่าวควรมีความถูกต้อง ครบถ้วน และอยู่ในรูปแบบที่สามารถเรียกดูหรือตรวจสอบได้ภายในระยะเวลาที่เหมาะสม และควรจัดเก็บเป็นระยะเวลาที่สอดคล้องกับกฎหมายหรือหลักเกณฑ์ที่เกี่ยวข้อง

- **ระบบการจัดทำและจัดเก็บข้อมูลและหลักฐานการประกอบธุรกิจ**

หลักการทั่วไป

ผู้ให้บริการสนับสนุนการออกและเสนอขายหลักทรัพย์โทเคนต้องจัดให้มีระบบการจัดทำ บันทึก จัดเก็บ และเรียกดูข้อมูลและหลักฐานที่เกี่ยวข้องกับการประกอบธุรกิจอย่างเพียงพอ ถูกต้อง ครบถ้วน และสามารถตรวจสอบย้อนหลังได้ เพื่อสนับสนุนการปฏิบัติงาน การกำกับดูแล การตรวจสอบ และการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง โดยต้องคำนึงถึงความมั่นคงปลอดภัยและความพร้อมในการเข้าถึงข้อมูลดังกล่าวตามลักษณะและความสำคัญของข้อมูล

ระบบดังกล่าวควรครอบคลุมข้อมูลและหลักฐานที่จำเป็นต่อการตรวจสอบการปฏิบัติงาน รวมถึงข้อมูลเกี่ยวกับการดำเนินการ การอนุมัติ การเปลี่ยนแปลง และรายการที่เกี่ยวข้องกับการให้บริการ โดยต้องสามารถเรียกดูและนำมาใช้ตรวจสอบย้อนหลังได้ภายในระยะเวลาที่เหมาะสม ทั้งนี้ ให้คำนึงถึงความถูกต้องครบถ้วน ความมั่นคงปลอดภัย และความพร้อมในการเข้าถึงข้อมูลตามลักษณะและความสำคัญของข้อมูล โดยรายละเอียดด้านการควบคุมทางเทคโนโลยีให้เป็นไปตามมาตรฐานส่วนที่เกี่ยวกับความเสี่ยงด้านเทคโนโลยี

ข้อเสนอแนะ : ผู้ให้บริการควรจัดให้มีระบบการจัดทำ บันทึก และจัดเก็บข้อมูลและหลักฐานที่เกี่ยวข้องกับการประกอบธุรกิจอย่างเป็นระบบ โดยควรดำเนินการอย่างน้อยดังต่อไปนี้

(1) การจัดทำและบันทึกข้อมูลและหลักฐาน : ผู้ให้บริการควรจัดให้มีการจัดทำและบันทึกข้อมูลและหลักฐานที่จำเป็นต่อการแสดงและตรวจสอบการปฏิบัติงานของตน โดยอย่างน้อยควรสามารถระบุ การดำเนินการที่เกิดขึ้น ผู้ดำเนินการ ผู้อนุมัติ วันและเวลาที่เกี่ยวข้อง รวมถึงการเปลี่ยนแปลงข้อมูลหรือการดำเนินการที่สำคัญ ได้อย่างเหมาะสม เพื่อให้สามารถตรวจสอบลำดับและที่มาของการดำเนินการย้อนหลังได้

ทั้งนี้ ข้อมูลและหลักฐานที่จัดทำและบันทึกควรสอดคล้องกับลักษณะและขอบเขตการให้บริการของ Securities Tokenizer และเพียงพอสำหรับการกำกับดูแล การตรวจสอบและการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง โดยไม่จำเป็นต้องกำหนดรูปแบบหรือวิธีการจัดเก็บข้อมูลเป็นการเฉพาะ หากสามารถบรรลุวัตถุประสงค์ดังกล่าวได้อย่างเหมาะสม

(2) การจัดเก็บและการเรียกดูข้อมูลและหลักฐาน : ผู้ให้บริการควรจัดให้มีการจัดเก็บข้อมูลและหลักฐานที่เกี่ยวข้องกับการประกอบธุรกิจอย่างเหมาะสม และสามารถค้นหา เรียกดู และนำมาใช้ตรวจสอบย้อนหลังได้ภายในระยะเวลาที่เหมาะสม โดยควรกำหนดระยะเวลาในการเก็บรักษาให้สอดคล้องกับลักษณะและความสำคัญของข้อมูล รวมถึงกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง

ทั้งนี้ ระบบการจัดเก็บควรคำนึงถึงความครบถ้วน ความถูกต้อง และความพร้อมในการเรียกดูข้อมูลตลอดระยะเวลาที่กำหนด รวมถึงมีมาตรการรองรับกรณีที่ระบบหรือข้อมูลไม่สามารถเข้าถึงได้ตามปกติ โดยรายละเอียดด้านความมั่นคงปลอดภัยและความพร้อมใช้งานให้เป็นไปตามมาตรฐานด้านความมั่นคงปลอดภัยทางไซเบอร์ ความเสี่ยงด้านเทคโนโลยี และความพร้อมในการดำเนินงาน

(3) การควบคุมความครบถ้วนและความน่าเชื่อถือของข้อมูลและหลักฐาน : ผู้ให้บริการควรจัดให้มีมาตรการเพื่อให้ข้อมูลและหลักฐานที่จัดทำและจัดเก็บมีความถูกต้อง ครบถ้วน และสามารถตรวจสอบได้ โดยควรสามารถระบุได้ว่าข้อมูลดังกล่าวถูกจัดทำหรือแก้ไขโดยผู้ใด และมีการเปลี่ยนแปลงเมื่อใดตามความเหมาะสม

ทั้งนี้ ควรมีมาตรการป้องกันการสูญหาย การแก้ไข หรือการทำลายข้อมูลและหลักฐานโดยไม่ได้รับอนุญาต รวมถึงมีแนวทางรองรับกรณีที่ข้อมูลหรือระบบจัดเก็บเกิดความเสียหายหรือไม่สามารถใช้งานได้ โดยให้เป็นไปตามมาตรฐานด้านความมั่นคงปลอดภัยทางไซเบอร์ ความเสี่ยงด้านเทคโนโลยี และความพร้อมในการดำเนินงาน

- **ระบบการบริหารจัดการเหตุการณ์และความต่อเนื่องในการดำเนินธุรกิจ (Incident Management and Business Continuity)**

หลักการทั่วไป

ผู้ให้บริการต้องจัดให้มีระบบและกระบวนการที่เพียงพอและเหมาะสมสำหรับรองรับเหตุการณ์ผิดปกติหรือเหตุการณ์ที่อาจส่งผลกระทบต่อการให้บริการ เพื่อให้สามารถตรวจพบ ประเมิน และจัดการเหตุการณ์ดังกล่าวได้อย่างเหมาะสมและทันท่วงที รวมทั้งสามารถให้บริการที่สำคัญได้อย่างต่อเนื่อง หรือสามารถกลับมาให้บริการได้ภายในระยะเวลาที่เหมาะสม โดยคำนึงถึงลักษณะ ขนาด ความซับซ้อน และระดับความเสี่ยงของการให้บริการ

การบริหารจัดการดังกล่าวควรครอบคลุมตั้งแต่การกำหนดกระบวนการและผู้รับผิดชอบในการจัดการเหตุการณ์ การรายงานและยกระดับเหตุการณ์ที่มีนัยสำคัญ การประสานงานกับผู้ใช้บริการและผู้ที่เกี่ยวข้อง ตลอดจนการจัดทำและทดสอบแผนการบริหารความต่อเนื่องในการให้บริการ และการทบทวนปรับปรุงกระบวนการจากเหตุการณ์หรือผลการทดสอบอย่างเหมาะสม

ข้อเสนอแนะ : ผู้ให้บริการควรจัดให้มีระบบและกระบวนการในการบริหารจัดการเหตุการณ์และความต่อเนื่องในการให้บริการ โดยควรดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

(1) การจัดการเหตุการณ์ (Incident Management) : ผู้ให้บริการควรจัดให้มีกระบวนการในการบริหารจัดการเหตุการณ์ผิดปกติที่มีหรืออาจมีผลกระทบต่อการให้บริการอย่างเหมาะสมและทันท่วงที โดยครอบคลุมตั้งแต่การตรวจพบ ประเมิน ตอบสนอง และจัดการเหตุการณ์ รวมถึงกำหนดบทบาท หน้าที่ และผู้รับผิดชอบในการดำเนินการไว้อย่างชัดเจน

ผู้ให้บริการควรจัดให้มีการกำหนดระดับความรุนแรงหรือความมีนัยสำคัญของเหตุการณ์ และแนวทางในการรายงานและยกระดับเหตุการณ์ต่อผู้บริหารหรือผู้มีอำนาจตัดสินใจตามความเหมาะสม รวมถึงการประสานงานกับผู้ใช้บริการและผู้ที่เกี่ยวข้องในกรณีที่เหตุการณ์อาจส่งผลกระทบต่อการให้บริการ

ทั้งนี้ ผู้ให้บริการควรจัดให้มีการบันทึกและทบทวนเหตุการณ์ที่เกิดขึ้นเพื่อวิเคราะห์สาเหตุ ผลกระทบ และแนวทางป้องกันหรือแก้ไข รวมถึงนำผลที่ได้ไปปรับปรุงกระบวนการบริหารจัดการเหตุการณ์และการดำเนินธุรกิจอย่างเหมาะสม โดยควรมีการ ทดสอบและทบทวนกระบวนการดังกล่าวอย่างน้อยปีละ 1 ครั้ง และปรับปรุงเมื่อมีเหตุการณ์สำคัญหรือมีการเปลี่ยนแปลงที่มีนัยสำคัญต่อการให้บริการ

(2) การบริหารความต่อเนื่องในการดำเนินธุรกิจ (Business Continuity Management) : ผู้ให้บริการควรจัดให้มีนโยบายและแผนการบริหารความต่อเนื่องในการดำเนินธุรกิจ

ที่เหมาะสมกับลักษณะ ขนาด ความซับซ้อน และระดับความเสี่ยงของการให้บริการ เพื่อรองรับเหตุการณ์ไม่ปกติหรือเหตุฉุกเฉินที่อาจส่งผลกระทบต่อการดำเนินธุรกิจ และเพื่อให้บริการหรือกระบวนการทางธุรกิจที่สำคัญสามารถดำเนินต่อไปได้ หรือสามารถกลับมาให้บริการได้ภายในระยะเวลาที่เหมาะสม

โดยควรจัดให้มีการกำหนดบริการหรือกระบวนการทางธุรกิจที่มีความสำคัญ การประเมินผลกระทบที่อาจเกิดขึ้นต่อการดำเนินธุรกิจ (**Business Impact Analysis: BIA**) รวมถึงกำหนดแนวทาง ขั้นตอน และผู้รับผิดชอบในการรองรับเหตุการณ์ดังกล่าวอย่างชัดเจน และควรคำนึงถึงการประสานงานกับผู้ใช้บริการและผู้ที่เกี่ยวข้องในกรณีที่เหตุการณ์ดังกล่าวอาจส่งผลกระทบต่อการให้บริการ

ทั้งนี้ ผู้ให้บริการควรจัดให้มีการ ทดสอบและทบทวน นโยบายและแผนการบริหารความต่อเนื่องในการดำเนินธุรกิจ อย่างน้อยปีละ 1 ครั้ง และควรปรับปรุงนโยบาย แผน และกระบวนการที่เกี่ยวข้องให้สอดคล้องกับผลการทดสอบ เหตุการณ์ที่เกิดขึ้นจริง หรือการเปลี่ยนแปลงที่มีนัยสำคัญต่อการดำเนินธุรกิจ

- **การใช้บริการจากผู้ให้บริการภายนอก (Outsourcing)**

หลักการทั่วไป

ผู้ให้บริการสามารถใช้บริการจากผู้ให้บริการภายนอกได้ตามความเหมาะสม โดยต้องจัดให้มีกระบวนการในการประเมิน คัดเลือก กำกับดูแล และบริหารความเสี่ยงจากการใช้บริการดังกล่าวอย่างเหมาะสม เพื่อให้มั่นใจว่าการใช้บริการจากผู้ให้บริการภายนอกไม่ส่งผลกระทบต่อความสามารถในการปฏิบัติหน้าที่ตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง รวมถึงไม่กระทบต่อความต่อเนื่อง ความมั่นคงปลอดภัย และคุณภาพของการให้บริการ

การใช้บริการจากผู้ให้บริการภายนอกยังทำให้ผู้ให้บริการยังคงมีความรับผิดชอบต่อการให้บริการอยู่ตามเดิม และควรสามารถติดตาม ตรวจสอบ และประเมินการปฏิบัติงานของผู้ให้บริการภายนอกได้อย่างเหมาะสม รวมถึงควรจัดให้มีการทบทวนความเหมาะสมของการใช้บริการ และมีมาตรการรองรับกรณีที่ผู้ให้บริการภายนอกไม่สามารถให้บริการได้ตามที่กำหนด

ข้อเสนอแนะ : ผู้ให้บริการควรจัดให้มีนโยบายและกระบวนการในการใช้บริการจากผู้ให้บริการภายนอกที่เป็นลายลักษณ์อักษร โดยควรดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

(1) การประเมินและคัดเลือกผู้ให้บริการภายนอก : ควรประเมินความเหมาะสมและความเสี่ยงก่อนใช้บริการ โดยคำนึงถึงลักษณะ ความสำคัญ และความเสี่ยงของงานที่จะมอบหมาย รวมถึงความรู้ ความสามารถ ประสบการณ์ ฐานะทางการเงิน และประวัติการดำเนินงานของผู้ให้บริการภายนอก ตลอดจนประวัติการถูกร้องเรียนหรือถูกฟ้องร้องดำเนินคดีในเรื่องที่เกี่ยวกับงาน

ที่จะให้ดำเนินการ โดยควรทบทวนความเหมาะสมและความเสี่ยงดังกล่าวเป็นระยะ ทั้งนี้ กรณีที่ผู้ให้บริการภายนอกอยู่ที่ต่างประเทศ ควรคำนึงถึงการเปลี่ยนแปลงหรือความไม่แน่นอนทางเศรษฐกิจ การเมือง สังคม และกฎหมายของประเทศของผู้ให้บริการภายนอกดังกล่าว ตลอดจนความซับซ้อนในการบริหารความต่อเนื่องทางธุรกิจที่เกี่ยวข้องกับการให้บริการจากต่างประเทศ

(2) การกำหนดขอบเขตและเงื่อนไขการให้บริการ : ควรจัดทำข้อตกลงเป็นลายลักษณ์อักษรที่กำหนดขอบเขตและลักษณะงาน หน้าที่และความรับผิดชอบของแต่ละฝ่าย เงื่อนไขหรือระดับการให้บริการที่จำเป็นอย่างชัดเจน ค่าตอบแทนและค่าใช้จ่ายที่มีการเรียกเก็บ รวมถึงกำหนดมาตรการรักษาความปลอดภัยและความลับของข้อมูล การบริหารความเสี่ยงและการรองรับความต่อเนื่องในการดำเนินธุรกิจ ตลอดจนสิทธิในการตรวจสอบของผู้ให้บริการ (ในฐานะผู้มอบหมาย) เงื่อนไขและวิธีการในการยกเลิกสัญญาหรือระงับการดำเนินการหรือเปลี่ยนแปลงการมอบหมายงาน เพื่อให้การมอบหมายงานเป็นไปอย่างเหมาะสม มีประสิทธิภาพ และสามารถกำกับดูแลได้อย่างต่อเนื่อง

(3) การกำกับดูแลและติดตามการให้บริการ : ควรจัดให้มีกระบวนการติดตามและประเมินการปฏิบัติงานของผู้ให้บริการภายนอกอย่างเหมาะสมและต่อเนื่อง เพื่อให้มั่นใจว่าการให้บริการเป็นไปตามข้อตกลง ระดับการให้บริการ และกฎหมายหรือหลักเกณฑ์ที่เกี่ยวข้อง รวมถึงควรสามารถเข้าถึงข้อมูล เอกสาร หรือหลักฐานที่จำเป็นต่อการกำกับดูแลและตรวจสอบการให้บริการได้ ทั้งนี้ ผู้ให้บริการควรจัดให้มีการรายงานและยกระดับประเด็นหรือเหตุการณ์ที่มีนัยสำคัญจากการให้บริการภายนอกต่อผู้บริหารหรือผู้มีอำนาจตัดสินใจตามความเหมาะสม และควรทบทวนผลการให้บริการและความเหมาะสมของการใช้บริการจากผู้ให้บริการภายนอกเป็นระยะ

(4) การบริหารความต่อเนื่องและการสิ้นสุดการใช้บริการ : ควรจัดให้มีแนวทางรองรับกรณีที่ผู้ให้บริการภายนอกไม่สามารถให้บริการได้ตามปกติ รวมถึงกรณีที่มีการเปลี่ยนแปลงหรือสิ้นสุดการใช้บริการ เพื่อให้สามารถเปลี่ยนหรือจัดหาผู้ให้บริการทดแทนหรือดำเนินการอื่นที่จำเป็นได้อย่างเหมาะสมและไม่ส่งผลกระทบอย่างมีนัยสำคัญต่อการให้บริการของผู้ให้บริการสนับสนุนการออกและเสนอขายหลักทรัพย์โทเคน

- **ระบบการกอบกู้และการเลิกประกอบกิจการอย่างเป็นระเบียบ**

หลักการทั่วไป

ผู้ให้บริการต้องจัดให้มีการเตรียมความพร้อมสำหรับการกอบกู้กิจการ (Recovery) หรือการเลิกประกอบกิจการอย่างเป็นระเบียบ (Orderly Wind-down) เนื่องจากผู้ให้บริการมีบทบาทสำคัญในการสนับสนุนการออกและการให้บริการเกี่ยวกับหลักทรัพย์โทเคน และอาจเป็นผู้ที่ดูแลหรือมีหน้าที่เกี่ยวข้องกับข้อมูล ทรัพย์สิน หรือกระบวนการที่เกี่ยวข้องกับสิทธิของผู้ใช้บริการและลูกค้า ดังนั้น หากผู้ให้บริการประสบปัญหารุนแรงจนไม่สามารถดำเนินธุรกิจหรือปฏิบัติหน้าที่ที่สำคัญได้

ก็ควรต้องมีแนวทางรองรับที่เหมาะสมและช่วยให้สามารถจัดการสถานการณ์ดังกล่าวได้อย่างเป็นระเบียบและลดผลกระทบต่อผู้ใช้บริการ ลูกค้า และผู้ที่เกี่ยวข้อง

ในกรณีที่เกิดสถานการณ์รุนแรง เช่น ปัญหาทางการเงินที่กระทบต่อความสามารถในการดำเนินธุรกิจ การสูญเสียความสามารถในการปฏิบัติหน้าที่ที่สำคัญ หรือเหตุการณ์อื่นที่ทำให้ไม่สามารถให้บริการที่สำคัญได้อย่างต่อเนื่อง ผู้ให้บริการควรสามารถประเมินได้ว่ามีความเป็นไปได้ที่จะกลับมาดำเนินธุรกิจและให้บริการที่สำคัญได้หรือไม่ และกำหนดแนวทางที่เหมาะสมสำหรับการกอบกู้กิจการ หรือหากไม่สามารถดำเนินธุรกิจต่อไปได้ ให้สามารถเลิกประกอบกิจการอย่างเป็นระเบียบ โดยคำนึงถึงการรักษาสิทธิ ทรัพย์สิน และข้อมูลของผู้ใช้บริการและลูกค้า การเตรียมความพร้อมดังกล่าวควรคำนึงถึงลักษณะ ขนาด ความซับซ้อน และระดับความเสี่ยงของการให้บริการ รวมถึงการกำหนดงานหรือหน้าที่ที่มีความสำคัญ แนวทางในการจัดการหรือส่งต่อการดำเนินงาน และการจัดการหลักทรัพย์โทเคน ทรัพย์สิน และข้อมูลของผู้ใช้บริการและลูกค้า เพื่อให้การกอบกู้หรือการเลิกประกอบกิจการสามารถดำเนินการได้อย่างเป็นระเบียบและลดผลกระทบต่อผู้ใช้บริการและลูกค้า

ข้อเสนอแนะ : ผู้ให้บริการควรจัดให้มีแผนการกอบกู้หรือการเลิกประกอบกิจการอย่างเป็นระเบียบที่เหมาะสม โดยควรดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้ ทั้งนี้ แผนดังกล่าวควรได้รับอนุมัติจากคณะกรรมการของผู้ให้บริการ

(1) การกำหนดสถานการณ์และเงื่อนไขสำหรับการกอบกู้หรือการเลิกประกอบกิจการ : ผู้ให้บริการควรจัดให้มีการกำหนดและประเมินสถานการณ์หรือเงื่อนไขที่อาจทำให้ไม่สามารถดำเนินธุรกิจหรือปฏิบัติหน้าที่ที่มีความสำคัญได้ตามปกติ เพื่อใช้ประกอบการพิจารณาว่าควรดำเนินการกอบกู้กิจการหรือเลิกประกอบกิจการอย่างเป็นระเบียบ โดยควรกำหนดแนวทางในการยกระดับสถานการณ์และการตัดสินใจ รวมถึงผู้มีอำนาจในการตัดสินใจและบทบาทของผู้ที่เกี่ยวข้องไว้อย่างชัดเจน

(2) การจัดการงานที่มีความสำคัญและการคุ้มครองสิทธิของผู้ใช้บริการและลูกค้า :

ผู้ให้บริการควรกำหนดแนวทางและมาตรการที่เหมาะสมสำหรับการกอบกู้กิจการ ในกรณีที่ผู้ให้บริการยังสามารถกลับมาดำเนินธุรกิจหรือให้บริการที่มีความสำคัญได้ โดยควรพิจารณาถึงการแก้ไขหรือจัดการปัจจัยที่เป็นสาเหตุของสถานการณ์ดังกล่าว รวมถึงกำหนดงานที่ต้องดำเนินการ ผู้รับผิดชอบ และอำนาจในการตัดสินใจที่จำเป็น เพื่อให้ผู้ให้บริการสามารถกลับมาดำเนินธุรกิจและให้บริการที่มีความสำคัญได้อย่างเหมาะสม

ในกรณีที่ไม่สามารถหรือไม่เหมาะสมที่จะดำเนินธุรกิจต่อไป ผู้ให้บริการควรกำหนดแนวทางในการเลิกประกอบกิจการอย่างเป็นระเบียบ โดยควรกำหนดงานหรือหน้าที่

ที่มีความสำคัญต่อการให้บริการ และแนวทางในการดำเนินการหรือส่งต่องานดังกล่าว เพื่อให้การดำเนินงานที่จำเป็นต่อผู้ใช้บริการและลูกค้าสามารถดำเนินต่อไปได้ หรือสามารถส่งต่อให้ผู้ที่มีความสามารถในการดำเนินการแทนได้อย่างเหมาะสม โดยควรกำหนดลำดับความสำคัญของงาน ผู้รับผิดชอบ และอำนาจในการดำเนินการไว้อย่างชัดเจน

ทั้งนี้ ควรพิจารณาถึงงานที่เกี่ยวข้องกับการออก การโอนหรือส่งมอบหลักทรัพย์โทเคน การจัดการทรัพย์สินและข้อมูลของลูกค้า ตลอดจนงานอื่นที่จำเป็นต่อการรักษาสิทธิของผู้ใช้บริการและลูกค้า รวมถึงควรกำหนดแนวทางในการจัดการหลักทรัพย์โทเคน ทรัพย์สิน สิทธิ ข้อมูล และหลักฐานที่เกี่ยวข้อง เพื่อให้สามารถระบุ ตรวจสอบ และดำเนินการกับสิ่งดังกล่าวได้อย่างเหมาะสม และไม่ทำให้ผู้ใช้บริการหรือลูกค้าเสียสิทธิอันเนื่องมาจากการหยุดหรือเลิกประกอบกิจการของผู้ให้บริการ

ในกรณีที่มีการส่งต่องานหรือหน้าที่ให้แก่ผู้ให้บริการรายอื่นหรือบุคคลที่เกี่ยวข้อง ผู้ให้บริการควรกำหนดแนวทางและขั้นตอนในการส่งต่อให้ชัดเจน รวมถึงการส่งมอบข้อมูล เอกสาร และหลักฐานที่จำเป็น เพื่อให้การดำเนินงานที่สำคัญสามารถดำเนินต่อไปได้ และเพื่อให้หลักทรัพย์โทเคน ทรัพย์สิน และสิทธิของผู้ใช้บริการและลูกค้ายังคงสามารถเข้าถึง ตรวจสอบ และใช้สิทธิได้อย่างเหมาะสม แม้ผู้ให้บริการจะไม่สามารถดำเนินการตามปกติหรือเลิกประกอบกิจการแล้ว

(3) การทบทวนและปรับปรุงแผน : ผู้ให้บริการควรจัดให้มีการทบทวนแผนการกอบกู้หรือการเลิกประกอบกิจการอย่างเป็นระเบียบเป็นระยะ เพื่อให้แผนยังคงเหมาะสมและสามารถนำไปใช้ได้จริง โดยควรพิจารณาถึงการเปลี่ยนแปลงที่มีนัยสำคัญต่อการดำเนินธุรกิจ โครงสร้างหรือขอบเขตการให้บริการ การเปลี่ยนแปลงของผู้ที่เกี่ยวข้อง รวมถึงบทเรียนหรือข้อสังเกตจากเหตุการณ์ที่เกิดขึ้นจริงหรือการดำเนินการตามแผน

ทั้งนี้ เมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ ผู้ให้บริการควรปรับปรุงแผนและแนวทางที่เกี่ยวข้องให้สอดคล้องกับสถานการณ์ รวมถึงควรสื่อสารการเปลี่ยนแปลงให้ผู้รับผิดชอบและผู้ที่เกี่ยวข้องทราบ เพื่อให้สามารถดำเนินการตามแผนได้อย่างเหมาะสมเมื่อมีความจำเป็น

5.3 แนวทางการปฏิบัติหน้าที่และการให้บริการ (Conduct Standards)

ผู้ให้บริการสนับสนุนการออกและเสนอขายหลักทรัพย์โทเคนควรปฏิบัติหน้าที่ด้วยความซื่อสัตย์ สุจริต เป็นธรรม และคำนึงถึงประโยชน์ของผู้ใช้บริการและผู้ถือหลักทรัพย์ โดยให้บริการตามบทบาทและหน้าที่ที่ตนรับผิดชอบอย่างเหมาะสม โปร่งใส และไม่กระทำการที่อาจก่อให้เกิดความเสียหายแก่ผู้ใช้บริการหรือผู้ถือหลักทรัพย์โดยไม่เหมาะสม

ทั้งนี้ การปฏิบัติหน้าที่ควรคำนึงถึงลักษณะและขอบเขตของบริการที่ผู้ให้บริการรับผิดชอบ รวมถึงความเสี่ยงที่อาจเกิดขึ้นจากการให้บริการ และควรมีแนวทางในการจัดการประเด็นที่อาจกระทบต่อความเป็นธรรมและประโยชน์ของผู้ใช้บริการและผู้ถือหลักทรัพย์อย่างเหมาะสม

5.3.1 การปฏิบัติหน้าที่ด้วยความซื่อสัตย์ สุจริต และเป็นธรรม

หลักการทั่วไป

ผู้ให้บริการสนับสนุนการออกและเสนอขายหลักทรัพย์โทเคนควรปฏิบัติหน้าที่ด้วยความซื่อสัตย์ สุจริต และเป็นธรรม โดยใช้ความรู้ ความสามารถ และความระมัดระวังที่เหมาะสมกับลักษณะและความซับซ้อนของการให้บริการ และคำนึงถึงสิทธิและประโยชน์ของผู้ใช้บริการ ผู้ถือหลักทรัพย์โทเคน และผู้ที่เกี่ยวข้อง เพื่อให้การให้บริการมีความน่าเชื่อถือ มีประสิทธิภาพ และสอดคล้องกับวัตถุประสงค์และขอบเขตของการให้บริการ ในการปฏิบัติหน้าที่ ผู้ให้บริการควรคำนึงถึงผลกระทบที่การดำเนินงานของตนอาจมีต่อผู้ใช้บริการและผู้ถือหลักทรัพย์โทเคน โดยเฉพาะในกรณีที่เกี่ยวข้องกับการออก การโอนหรือส่งมอบ การชำระราคา การรับฝาก หรือการบันทึกและจัดการสิทธิในหลักทรัพย์โทเคน และควรดำเนินการอย่างเหมาะสมเพื่อให้บริการดังกล่าวเป็นไปอย่างมีประสิทธิภาพและไม่ก่อให้เกิดความเสียหายโดยไม่จำเป็น

ข้อเสนอแนะ : ผู้ให้บริการควรจัดให้มีแนวทางในการปฏิบัติหน้าที่ให้สอดคล้องกับหลักการดังกล่าว โดยอย่างน้อยควรดำเนินการในเรื่องดังต่อไปนี้

(1) การปฏิบัติหน้าที่ด้วยความซื่อสัตย์ สุจริต และเป็นธรรม : ผู้ให้บริการควรปฏิบัติหน้าที่ตามกฎหมาย หลักเกณฑ์ ขอบเขต และวัตถุประสงค์ของการให้บริการ โดยปฏิบัติต่อผู้ใช้บริการและผู้ถือหลักทรัพย์โทเคนอย่างเป็นธรรม และไม่ดำเนินการโดยมิชอบหรือเอื้อประโยชน์แก่ตนเองหรือบุคคลหนึ่งบุคคลใดอย่างไม่เหมาะสม

(2) การปฏิบัติหน้าที่ด้วยความรู้ ความสามารถ และความระมัดระวัง : ผู้ให้บริการควรจัดให้บุคคลที่เกี่ยวข้องกับการให้บริการปฏิบัติหน้าที่ด้วยความรู้ ความสามารถ และความระมัดระวังที่เหมาะสมกับหน้าที่และความรับผิดชอบ รวมทั้งคำนึงถึงลักษณะ ความซับซ้อน และความเสี่ยงของการให้บริการ

(3) การคำนึงถึงประโยชน์และสิทธิของผู้ใช้บริการและผู้ถือหลักทรัพย์โทเคน : ผู้ให้บริการควรคำนึงถึงสิทธิและประโยชน์ของผู้ใช้บริการและผู้ถือหลักทรัพย์โทเคนในการดำเนินการที่อาจมีผลต่อการให้บริการหรือสิทธิในหลักทรัพย์โทเคน และควรดำเนินการให้บริการอย่างมีประสิทธิภาพสอดคล้องกับความต้องการของผู้ใช้บริการและลักษณะของตลาดที่ให้บริการ

(4) การไม่ใช้ข้อมูลหรืออำนาจหน้าที่โดยมิชอบ : ผู้ให้บริการควรไม่ใช้ข้อมูล อำนาจหน้าที่ หรือโอกาสที่ได้รับจากการปฏิบัติหน้าที่เพื่อแสวงหาประโยชน์โดยมิชอบหรือก่อให้เกิดความเสียหายแก่ผู้ใช้บริการหรือผู้ถือหลักทรัพย์โทเคน

5.3.2 การจัดการความขัดแย้งทางผลประโยชน์

หลักการทั่วไป

ผู้ให้บริการสนับสนุนการออกและเสนอขายหลักทรัพย์โทเคนควรจัดให้มีการระบุ ป้องกัน และจัดการความขัดแย้งทางผลประโยชน์ที่อาจเกิดขึ้นจากการประกอบธุรกิจและการให้บริการ เพื่อให้การปฏิบัติหน้าที่และการตัดสินใจที่เกี่ยวข้องกับการให้บริการเป็นไปอย่างเป็นธรรม และไม่ทำให้ผู้ใช้บริการหรือลูกค้าได้รับความเสียหายหรือเสียประโยชน์จากความขัดแย้งดังกล่าว

ผู้ให้บริการควรคำนึงถึงความขัดแย้งทางผลประโยชน์ที่อาจเกิดขึ้นระหว่างผู้ให้บริการกับผู้ใช้บริการหรือลูกค้า ระหว่างผู้ใช้บริการหรือลูกค้าแต่ละราย หรือระหว่างการให้บริการกับกิจกรรมหรือบทบาทอื่นของผู้ให้บริการ รวมถึงกรณีที่ผู้ให้บริการทำหน้าที่หลายบทบาทที่อาจก่อให้เกิดความขัดแย้งทางผลประโยชน์

ข้อเสนอแนะ : ผู้ให้บริการควรจัดให้มีกระบวนการในการจัดการความขัดแย้งทางผลประโยชน์ที่อาจเกิดขึ้นจากการให้บริการ โดยควรดำเนินการอย่างน้อยดังต่อไปนี้

(1) **การระบุและประเมินความขัดแย้งทางผลประโยชน์ :** ผู้ให้บริการควรพิจารณาและประเมินความขัดแย้งทางผลประโยชน์ที่อาจเกิดขึ้นจากลักษณะการประกอบธุรกิจ ขอบเขตการให้บริการ และบทบาทหรือหน้าที่ที่ผู้ให้บริการรับผิดชอบ **โดยเฉพาะกรณีที่ผู้ให้บริการมีหลายบทบาทหรือให้บริการหลายประเภทที่อาจมีผลประโยชน์ไม่สอดคล้องกัน เช่น การทำหน้าที่เป็นผู้ให้บริการสนับสนุนการออกและเสนอขายหลักทรัพย์โทเคนควบคู่กับการทำหน้าที่เป็นนายทะเบียน ผู้รับฝากทรัพย์สิน หรือผู้ให้บริการด้านเทคโนโลยี** หรือกรณีที่ผู้ให้บริการหรือบุคคลที่เกี่ยวข้องมีส่วนได้เสียในธุรกิจหรือกิจกรรมที่เกี่ยวข้องกับการให้บริการ เพื่อให้สามารถระบุสถานการณ์ที่อาจก่อให้เกิดความขัดแย้งทางผลประโยชน์และกำหนดแนวทางจัดการได้อย่างเหมาะสม

(2) **การป้องกันและจัดการความขัดแย้งทางผลประโยชน์ :** เมื่อพบหรืออาจเกิดความขัดแย้งทางผลประโยชน์ ผู้ให้บริการควรจัดให้มีแนวทางในการป้องกัน หลีกเลี่ยง หรือจัดการความขัดแย้งดังกล่าวตามความเหมาะสม เพื่อไม่ให้ความขัดแย้งดังกล่าวส่งผลกระทบต่อการปฏิบัติหน้าที่หรือการตัดสินใจที่เกี่ยวข้องกับการให้บริการอย่างไม่เป็นธรรม

(3) **การเปิดเผยความขัดแย้งทางผลประโยชน์ :** ในกรณีที่ไม่สามารถป้องกันหรือจัดการความขัดแย้งทางผลประโยชน์ได้อย่างเพียงพอ ผู้ให้บริการควรพิจารณาเปิดเผยข้อมูลเกี่ยวกับ

ความขัดแย้งทางผลประโยชน์ให้แก่ผู้ใช้บริการหรือลูกค้าที่เกี่ยวข้องทราบตามความเหมาะสม เพื่อให้สามารถพิจารณาถึงผลกระทบหรือความเสี่ยงที่เกี่ยวข้องได้

5.3.3 การเปิดเผยข้อมูลและความโปร่งใส

หลักการทั่วไป

ผู้ให้บริการสนับสนุนการออกและเสนอขายหลักทรัพย์โทเคนควรเปิดเผยข้อมูลที่จำเป็นและมีนัยสำคัญเกี่ยวกับการให้บริการแก่ผู้ใช้บริการและผู้ที่เกี่ยวข้องอย่างเพียงพอ ชัดเจน ถูกต้อง และเป็นปัจจุบัน เพื่อให้ผู้ใช้บริการสามารถเข้าใจบทบาทและขอบเขตความรับผิดชอบของผู้ให้บริการ กระบวนการที่เกี่ยวข้อง ตลอดจนความเสี่ยงและเงื่อนไขที่สำคัญของการให้บริการ และสามารถใช้ข้อมูลดังกล่าวประกอบการตัดสินใจและติดตามการให้บริการได้อย่างเหมาะสม

การเปิดเผยข้อมูลควรสอดคล้องกับลักษณะ ขนาด ความซับซ้อน และขอบเขตการให้บริการของ Securities Tokenizer และควรคำนึงถึงข้อมูลที่จำเป็นต่อการทำความเข้าใจการให้บริการและสิทธิของผู้ใช้บริการและผู้ถือหลักทรัพย์โทเคน โดยไม่จำเป็นต้องกำหนดรูปแบบหรือวิธีการเปิดเผยข้อมูลเป็นการเฉพาะ หากสามารถบรรลุวัตถุประสงค์ดังกล่าวได้อย่างเหมาะสม

ข้อเสนอแนะ : ผู้ให้บริการควรจัดให้มีแนวทางในการเปิดเผยข้อมูลที่เกี่ยวข้องกับการให้บริการ โดยควรดำเนินการอย่างน้อยดังต่อไปนี้

(1) ข้อมูลเกี่ยวกับบทบาทและขอบเขตการให้บริการ : ผู้ให้บริการควรเปิดเผยข้อมูลเกี่ยวกับลักษณะและขอบเขตการให้บริการ บทบาท หน้าที่ และความรับผิดชอบของผู้ให้บริการ รวมถึงขอบเขตของงานที่ผู้ให้บริการไม่ได้รับผิดชอบหรือมีการดำเนินการโดยบุคคลอื่น เพื่อให้ผู้ใช้บริการสามารถเข้าใจได้อย่างชัดเจนว่า Securities Tokenizer มีหน้าที่และความรับผิดชอบในส่วนใด

(2) ข้อมูลเกี่ยวกับกระบวนการและเงื่อนไขการให้บริการ : ผู้ให้บริการควรเปิดเผยข้อมูลเกี่ยวกับกระบวนการและเงื่อนไขที่สำคัญของการให้บริการ รวมถึงค่าธรรมเนียม ค่าใช้จ่าย และเงื่อนไขอื่นที่ผู้ใช้บริการควรทราบ ตลอดจนข้อมูลเกี่ยวกับการใช้บริการจากผู้ให้บริการภายนอกหรือบุคคลอื่นที่มีนัยสำคัญต่อการให้บริการตามความเหมาะสม

(3) ข้อมูลเกี่ยวกับความเสี่ยงและข้อจำกัดของการให้บริการ : ผู้ให้บริการควรเปิดเผยความเสี่ยงและข้อจำกัดที่สำคัญซึ่งอาจส่งผลต่อการให้บริการ สิทธิของผู้ใช้บริการหรือหลักทรัพย์โทเคนตามลักษณะของบริการ เพื่อให้ผู้ใช้บริการสามารถเข้าใจและประเมินผลกระทบที่อาจเกิดขึ้นได้อย่างเหมาะสม

(4) การเข้าถึงข้อมูลและการปรับปรุงข้อมูล : ผู้ให้บริการควรจัดให้ผู้ใช้บริการและผู้ที่เกี่ยวข้องสามารถเข้าถึงข้อมูลที่จำเป็นเกี่ยวกับการให้บริการได้อย่างเหมาะสม และควรปรับปรุงข้อมูลดังกล่าวเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ เพื่อให้ข้อมูลที่เปิดเผยยังคงถูกต้องและเป็นปัจจุบัน

(5) ช่องทางอิเล็กทรอนิกส์สำหรับข้อมูลที่เกี่ยวข้องกับหลักทรัพย์โทเคน : ในกรณีที่เหมาะสมตามลักษณะการให้บริการ ผู้ให้บริการควรจัดให้มีช่องทางอิเล็กทรอนิกส์ที่ผู้ใช้บริการหรือบุคคลทั่วไปสามารถเข้าถึงข้อมูลที่จำเป็นเกี่ยวกับหลักทรัพย์โทเคนและสถานะหรือการเปลี่ยนแปลงที่เกี่ยวข้องได้อย่างเหมาะสม เพื่อส่งเสริมความโปร่งใสและความสามารถในการตรวจสอบข้อมูล เช่น ข้อมูลหรือเครื่องมือที่ช่วยให้สามารถตรวจสอบสถานะของหลักทรัพย์โทเคนหรือรายการที่เกิดขึ้นบนระบบ DLT ที่เกี่ยวข้องกับการให้บริการได้ตามความเหมาะสม

5.3.4 การรักษาความลับและข้อมูล

หลักการทั่วไป

ผู้ให้บริการสนับสนุนการออกและเสนอขายหลักทรัพย์โทเคนควรรักษาความลับและข้อมูลของผู้ใช้บริการ ลูกค้า และผู้ถือหลักทรัพย์โทเคนที่ได้รับหรือเข้าถึงจากการปฏิบัติหน้าที่ และควรใช้หรือเปิดเผยข้อมูลดังกล่าวเท่าที่จำเป็นและเหมาะสมกับวัตถุประสงค์ของการให้บริการและตามกฎหมายหรือหลักเกณฑ์ที่เกี่ยวข้อง

ทั้งนี้ ผู้ให้บริการควรจัดให้มีการควบคุมการใช้และเปิดเผยข้อมูลดังกล่าวอย่างเหมาะสม โดยคำนึงถึงลักษณะและความสำคัญของข้อมูล รวมถึงบทบาทและขอบเขตการให้บริการของผู้ให้บริการ

ข้อเสนอแนะ : ผู้ให้บริการควรจัดให้มีแนวทางในการรักษาความลับและการใช้ข้อมูลของผู้ใช้บริการ ลูกค้า และผู้ถือหลักทรัพย์โทเคน โดยควรดำเนินการอย่างน้อยดังต่อไปนี้

(1) การใช้และเปิดเผยข้อมูล : ผู้ให้บริการควรใช้ข้อมูลที่ได้รับจากการปฏิบัติหน้าที่เท่าที่จำเป็นต่อการให้บริการหรือการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง และไม่ควรนำข้อมูลดังกล่าวไปใช้เพื่อประโยชน์อื่นโดยไม่เหมาะสม รวมถึงไม่ควรเปิดเผยข้อมูลแก่บุคคลอื่นเว้นแต่มีเหตุอันสมควรหรือเป็นไปตามกฎหมาย หลักเกณฑ์ หรือหน้าที่ที่เกี่ยวข้อง

(2) การจำกัดการเข้าถึงข้อมูล : ผู้ให้บริการควรกำหนดให้บุคคลที่เกี่ยวข้องสามารถเข้าถึงข้อมูลของผู้ใช้บริการ ลูกค้า และผู้ถือหลักทรัพย์โทเคนได้เท่าที่จำเป็นต่อการปฏิบัติหน้าที่และควรมีแนวทางในการป้องกันการนำข้อมูลดังกล่าวไปใช้โดยมิชอบ

(3) การรักษาความลับภายหลังสิ้นสุดหน้าที่ : ผู้ให้บริการควรจัดให้มีแนวทางในการรักษาความลับของข้อมูลที่ได้รับหรือเข้าถึงจากการปฏิบัติหน้าที่ แม้การปฏิบัติหน้าที่หรือความสัมพันธ์ในการให้บริการกับผู้ใช้บริการหรือลูกค้าจะสิ้นสุดลง โดยควรรักษาความลับและควบคุมการใช้หรือเปิดเผยข้อมูลดังกล่าวตลอดระยะเวลาที่ผู้ให้บริการยังมีหน้าที่หรือความจำเป็นในการเก็บรักษาข้อมูลตามกฎหมาย หลักเกณฑ์ หรือวัตถุประสงค์ที่เกี่ยวข้อง

5.3.5 การจัดการข้อร้องเรียนและข้อพิพาท

หลักการทั่วไป

ผู้ให้บริการสนับสนุนการออกและเสนอขายหลักทรัพย์โทเคนควรจัดให้มีระบบและกระบวนการในการรับ พิจารณา และจัดการข้อร้องเรียนหรือข้อพิพาทที่เกี่ยวข้องกับการให้บริการอย่างเหมาะสมและมีประสิทธิภาพ เพื่อให้ผู้ใช้บริการและผู้ถือหลักทรัพย์สามารถแจ้งปัญหาหรือข้อร้องเรียนและได้รับการพิจารณาอย่างเป็นธรรม รวมทั้งสามารถติดตามผลการดำเนินการได้อย่างเหมาะสม

กระบวนการดังกล่าวควรครอบคลุมข้อร้องเรียนหรือข้อพิพาทที่เกี่ยวข้องกับการให้บริการของผู้ให้บริการ ตลอดจนการดำเนินการที่อาจมีผลต่อสิทธิหรือประโยชน์ของผู้ใช้บริการหรือผู้ถือหลักทรัพย์โทเคน เช่น การดำเนินการเกี่ยวกับการถือครองหรือการโอนหลักทรัพย์โทเคน การให้บริการผ่าน Wallet หรือการดำเนินการในกรณีที่ผู้ถือหลักทรัพย์ไม่สามารถเข้าถึงหลักทรัพย์โทเคนของตนได้ ทั้งนี้ การดำเนินการในกรณีดังกล่าวให้เป็นไปตามกระบวนการและหลักเกณฑ์ที่เกี่ยวข้อง

ข้อเสนอแนะ : ผู้ให้บริการควรจัดให้มีกระบวนการจัดการข้อร้องเรียนและข้อพิพาท โดยควรดำเนินการอย่างน้อยดังต่อไปนี้

(1) ช่องทางและการรับเรื่องร้องเรียน : ผู้ให้บริการควรกำหนดช่องทางและวิธีการรับเรื่องร้องเรียนที่ชัดเจนและเหมาะสมกับลักษณะการให้บริการ รวมถึงข้อมูลที่ผู้ร้องเรียนควรจัดส่งเพื่อประกอบการพิจารณา และควรแจ้งให้ผู้ใช้บริการทราบช่องทางดังกล่าวอย่างเหมาะสม

(2) การพิจารณาและดำเนินการ : ผู้ให้บริการควรกำหนดผู้รับผิดชอบและกระบวนการในการตรวจสอบ พิจารณา และดำเนินการเกี่ยวกับข้อร้องเรียนอย่างเหมาะสม รวมถึงกำหนดระยะเวลาในการดำเนินการและการแจ้งความคืบหน้าหรือผลการพิจารณาแก่ผู้ร้องเรียนตามความเหมาะสม

ในกรณีที่ข้อร้องเรียนเกี่ยวข้องกับการดำเนินการที่มีผลต่อสิทธิหรือสถานะของหลักทรัพย์โทเคน ผู้ให้บริการควรพิจารณาข้อมูลและหลักฐานที่เกี่ยวข้องอย่างเหมาะสม และควรดำเนินการโดยคำนึงถึงความถูกต้องของข้อมูลและสถานะของหลักทรัพย์โทเคน รวมถึงสิทธิของผู้ใช้บริการและผู้ถือหลักทรัพย์ที่เกี่ยวข้อง

(3) การจัดการข้อพิพาทและการยกระดับ : ผู้ให้บริการควรกำหนดหลักเกณฑ์ในการยกระดับข้อร้องเรียนหรือข้อพิพาทที่มีความสำคัญหรือมีผลกระทบอย่างมีนัยสำคัญต่อผู้ใช้บริการหรือผู้ถือหลักทรัพย์โทเคนไปยังผู้บริหารหรือผู้มีอำนาจพิจารณาในระดับที่เหมาะสม รวมถึงกำหนดแนวทางในการประสานงานกับหน่วยงานหรือบุคคลที่เกี่ยวข้องตามความเหมาะสม

(4) การบันทึกและติดตามข้อร้องเรียน : ผู้ให้บริการควรจัดให้มีการบันทึกข้อมูลและหลักฐานเกี่ยวกับข้อร้องเรียนและผลการดำเนินการอย่างเหมาะสม เพื่อให้สามารถติดตาม ตรวจสอบ

และวิเคราะห์แนวโน้มของข้อร้องเรียน รวมถึงนำข้อมูลดังกล่าวไปใช้ในการปรับปรุงกระบวนการให้บริการและการควบคุมที่เกี่ยวข้อง

5.4 แนวทางการดำเนินงานตามขอบเขตของผู้ให้บริการสนับสนุนการออกและเสนอขายหลักทรัพย์โทเคน (Operational Guidelines)

ผู้ให้บริการสนับสนุนการออกและเสนอขายหลักทรัพย์โทเคน (Securities Tokenizer) อาจมีขอบเขตการดำเนินงานและความรับผิดชอบที่แตกต่างกันตามรูปแบบการประกอบธุรกิจและบริการที่ให้แก่ผู้ใช้บริการ โดยอาจรับผิดชอบงานบางส่วนหรือหลายส่วนที่เกี่ยวข้องกับวงจรชีวิตของหลักทรัพย์โทเคน ทั้งนี้ ผู้ให้บริการควรจัดให้มีระบบ กระบวนการ และกลไกที่เหมาะสมกับลักษณะและขอบเขตของงานที่อยู่ในความรับผิดชอบ เพื่อให้การดำเนินงานเป็นไปอย่างถูกต้อง มีประสิทธิภาพ และสามารถควบคุมความเสี่ยงที่เกี่ยวข้องได้อย่างเหมาะสม

แนวทางการดำเนินงานในส่วนนี้จึงกำหนดหลักการและแนวทางสำหรับงานหลักที่ผู้ให้บริการอาจรับผิดชอบ โดยคำนึงถึงลักษณะของแต่ละงาน ความเชื่อมโยงระหว่างกระบวนการ และผลกระทบที่อาจเกิดขึ้นต่อสิทธิของผู้ถือหลักทรัพย์โทเคนและผู้ที่เกี่ยวข้อง เพื่อให้การดำเนินงานในแต่ละขอบเขตเป็นไปอย่างถูกต้อง มีประสิทธิภาพ และสามารถรองรับและจัดการความเสี่ยงที่เกี่ยวข้องได้อย่างเหมาะสม

5.4.1 งานด้านการออก การบันทึก การทำรายการ และการดูแลหลักทรัพย์โทเคน

หลักการทั่วไป

ผู้ให้บริการสนับสนุนการออกและเสนอขายหลักทรัพย์โทเคน (Securities Tokenizer) ที่รับผิดชอบงานด้านการออก การบันทึก หรือการดำเนินการเกี่ยวกับหลักทรัพย์โทเคน ควรจัดให้มีกระบวนการและระบบงานที่เหมาะสมกับลักษณะ ขอบเขต และความซับซ้อนของงานที่ตนรับผิดชอบ เพื่อให้การดำเนินการเกี่ยวกับหลักทรัพย์โทเคนเป็นไปอย่างถูกต้อง ครบถ้วน และสอดคล้องกับสิทธิและเงื่อนไขของหลักทรัพย์โทเคนตลอดวงจรชีวิตของหลักทรัพย์

แนวทางในข้อนี้ครอบคลุมระบบงานที่เกี่ยวข้องกับการออกหลักทรัพย์โทเคน การจัดทำและบันทึกข้อมูลหลักทรัพย์โทเคน การส่งมอบและรับมอบ การโอนและรับโอน การใช้หลักทรัพย์โทเคนเป็นหลักประกัน และการให้บริการด้านสิทธิประโยชน์และการดำเนินการตามสิทธิของผู้ถือหลักทรัพย์ โดยส่วนหนึ่งอ้างอิงหลักการของ UNCITRAL Model Law on Electronic Transferable Records (MLETR) และมาตรฐานว่าด้วยแนวทางการใช้งานตราสารอิเล็กทรอนิกส์ (Electronic Transferable Records: ETR) ของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA) ซึ่งให้ความสำคัญกับการจัดทำข้อมูลอิเล็กทรอนิกส์ที่ครบถ้วนและสามารถเข้าถึงและนำกลับมาใช้ได้

การมีหนึ่งเดียวของตราสาร (Singularity) การบริหารจัดการสิทธิควบคุม (Exclusive Control) และการรักษาความถูกต้องครบถ้วนของข้อมูล (Integrity) ทั้งนี้ เพื่อให้ข้อมูลและสิทธิในหลักทรัพย์โทเคนมีความถูกต้อง น่าเชื่อถือ และสามารถใช้และโอนสิทธิได้อย่างต่อเนื่องตลอดวงจรชีวิตของหลักทรัพย์

ทั้งนี้ ผู้ให้บริการอาจรับผิดชอบงานเพียงบางส่วนหรือหลายส่วนของวงจรชีวิตหลักทรัพย์โทเคนตามขอบเขตการให้บริการของตน ระบบงานที่ผู้ให้บริการจัดให้มีจึงควรครอบคลุมงานที่รับผิดชอบได้อย่างชัดเจน และควรสามารถประสานงานกับผู้ออกหลักทรัพย์ นายทะเบียน ผู้รับฝากทรัพย์สิน ผู้ให้บริการเก็บหลักทรัพย์โทเคนหรือผู้ให้บริการและผู้ที่เกี่ยวข้องอื่นได้อย่างเหมาะสม เพื่อให้การดำเนินงานในส่วนที่เชื่อมโยงกันเป็นไปอย่างถูกต้อง ต่อเนื่อง และมีความสอดคล้องกันของข้อมูลหรือสิทธิในหลักทรัพย์โทเคน

ข้อเสนอแนะ : ผู้ให้บริการควรจัดให้มีระบบงานและกระบวนการที่เหมาะสมกับขอบเขตหน้าที่ของตน โดยอย่างน้อยควรครอบคลุมระบบงานที่เกี่ยวข้องกับวงจรชีวิตของหลักทรัพย์โทเคนดังต่อไปนี้

(1) การออกหลักทรัพย์โทเคน (Token Issuance) : ผู้ให้บริการควรจัดให้มีกลไกหรือกระบวนการทางอิเล็กทรอนิกส์ที่ใช้วิธีการที่เชื่อถือได้ สำหรับการสร้างและออกหลักทรัพย์โทเคน เพื่อให้ข้อมูล รายการ หรือข้อความที่เกี่ยวข้องกับหลักทรัพย์โทเคนมีความถูกต้อง ครบถ้วน และสามารถแสดงและใช้สิทธิในหลักทรัพย์โทเคนได้อย่างถูกต้องตามกฎหมาย โดยควรดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

- **การจัดทำข้อมูลของหลักทรัพย์โทเคน** : ผู้ให้บริการควรจัดให้ข้อมูล รายการ หรือข้อความที่เกี่ยวข้องกับหลักทรัพย์โทเคนอยู่ในรูปข้อมูลอิเล็กทรอนิกส์ที่มีความถูกต้อง (Integrity) และครบถ้วน (Completeness) รวมทั้งสามารถเข้าถึงได้ (Accessible) และสามารถนำข้อมูลกลับมาใช้ได้ (Usable) ในภายหลัง เพื่อให้สามารถแสดงสิทธิและข้อมูลที่เกี่ยวข้องกับหลักทรัพย์โทเคนได้อย่างเหมาะสม

ตัวอย่าง : ผู้ให้บริการอาจกำหนดโครงสร้างข้อมูลของหลักทรัพย์โทเคนให้มีข้อมูลที่จำเป็นต่อการระบุและแสดงสิทธิในหลักทรัพย์โทเคน เช่น Token Identifier, Issuer Identifier ประเภทและจำนวนหลักทรัพย์, วันที่ออก, วันครบกำหนด, สิทธิของผู้ถือ, เงื่อนไขของหลักทรัพย์ และสถานะของหลักทรัพย์โทเคน โดยข้อมูลดังกล่าวอาจถูกจัดทำในรูปแบบข้อมูลที่มีโครงสร้าง (Structured Data) และกำหนดรูปแบบและความหมายของข้อมูลแต่ละรายการไว้อย่างชัดเจน เพื่อให้ระบบที่เกี่ยวข้องสามารถตีความและนำข้อมูลไปใช้ได้อย่างสอดคล้องกัน ในการจัดเก็บข้อมูล ผู้ให้บริการอาจใช้ Cryptographic Hash, Digital Signature หรือกลไกทางเทคนิคอื่นที่เหมาะสม เพื่อช่วยยืนยัน

ความถูกต้องและความครบถ้วนของข้อมูล (Integrity) และสามารถตรวจสอบได้ว่าข้อมูลที่ถูกนำมาแสดงหรือใช้งานภายหลังเป็นข้อมูลเดียวกับที่ได้รับการจัดทำหรือรับรองไว้ในขณะที่มีการออกหลักทรัพย์โทเคน ทั้งนี้ หากข้อมูลของหลักทรัพย์โทเคนมีการจัดเก็บในหลายระบบหรือมีข้อมูลบางส่วนจัดเก็บนอกระบบ DLT ผู้ให้บริการควรกำหนด Unique Identifier หรือกลไกอ้างอิงที่สามารถเชื่อมโยงข้อมูลระหว่างระบบ เพื่อป้องกันการเกิดข้อมูลที่ไม่ตรงกันหรือไม่สามารถระบุได้ว่าเป็นข้อมูลของหลักทรัพย์โทเคนรายการเดียวกัน

นอกจากนี้ ผู้ให้บริการอาจจัดให้มีวิธีการจัดเก็บและสำรองข้อมูลที่ทำให้ข้อมูลสามารถเข้าถึงได้ (Accessible) และนำกลับมาใช้ได้ (Usable) ภายหลังการออกหลักทรัพย์โทเคน โดยไม่จำกัดเฉพาะการที่ข้อมูลยังคงอยู่บนระบบ DLT แต่ควรคำนึงถึงความสามารถในการ ค้นหา เรียกคืน ตรวจสอบ และแสดงข้อมูลในรูปแบบที่สามารถนำไปใช้ในการปฏิบัติงานหรือพิสูจน์สิทธิได้ตลอดระยะเวลาที่จำเป็นตามกฎหมาย หลักเกณฑ์ หรือวัตถุประสงค์ที่เกี่ยวข้อง เช่น เมื่อมีการโอนหลักทรัพย์ การใช้สิทธิ การตรวจสอบย้อนหลัง หรือการตรวจสอบโดยหน่วยงานที่เกี่ยวข้อง

- **การเชื่อมโยงข้อมูลที่เกี่ยวข้อง** : ในกรณีที่มีการเพิ่มเติมข้อมูล รายการ หรือข้อความที่เกี่ยวข้องกับหลักทรัพย์โทเคนภายหลังการออก ผู้ให้บริการควรจัดให้มีกลไกที่ทำให้ข้อมูลดังกล่าวสามารถเชื่อมโยงกับข้อมูลอิเล็กทรอนิกส์เดิมได้ (Logically Associated) เพื่อให้สามารถตรวจสอบความสัมพันธ์และลำดับของข้อมูลที่เกี่ยวข้องกับหลักทรัพย์โทเคนได้

ตัวอย่าง : ผู้ให้บริการอาจกำหนด Unique Identifier หรือข้อมูลอ้างอิง เช่น Token ID, Transaction ID หรือ Event ID เพื่อเชื่อมโยงข้อมูลที่เกิดขึ้นภายหลังกับข้อมูลเดิมของหลักทรัพย์โทเคน เช่น เชื่อมโยงรายการโอนหรือการเปลี่ยนแปลงสถานะกลับไปยัง Token ID เดิม และอาจใช้ Timestamp, Sequence Number หรือ Transaction Hash เพื่อแสดงลำดับและความสัมพันธ์ของข้อมูลแต่ละรายการ ทำให้สามารถตรวจสอบได้ว่าข้อมูลที่เพิ่มเติมหรือเปลี่ยนแปลงนั้นเกี่ยวข้องกับหลักทรัพย์โทเคนรายการใดและเกิดขึ้นต่อเนื่องจากข้อมูลเดิมอย่างไร (Logically Associated) ทั้งนี้ แม้ข้อมูลจะจัดเก็บอยู่ต่างระบบหรือบางส่วนอยู่นอกระบบ DLT ก็ควรมีกลไกอ้างอิงที่ทำให้สามารถเชื่อมโยงข้อมูลดังกล่าวเข้าด้วยกันได้อย่างถูกต้อง

- **การมีหนึ่งเดียวของหลักทรัพย์โทเคน** : ผู้ให้บริการควรจัดให้มีกลไกที่ทำให้หลักทรัพย์โทเคนแต่ละรายการมีสถานะหนึ่งเดียว (Singularity) และสามารถระบุหลักทรัพย์โทเคนแต่ละรายการได้อย่างชัดเจนและตรวจสอบได้ รวมทั้งควรมีมาตรการป้องกันการทำซ้ำหลักทรัพย์โทเคนโดยมิชอบ (Unauthorized Replication) และการเรียกร้องสิทธิซ้ำซ้อน (Multiple Claims) ที่อาจเกิดขึ้นจากการสร้างหรือบันทึกหลักทรัพย์โทเคนซ้ำซ้อน

ตัวอย่าง : ผู้ให้บริการอาจกำหนดให้หลักทรัพย์โทเคนแต่ละรายการมี Unique Identifier (Token ID) และจัดให้มีระบบหรือกลไกที่สามารถยืนยันได้ว่า Token ID ดังกล่าวอ้างถึงหลักทรัพย์โทเคนเพียงรายการเดียว และมีสถานะการถือครองหรือสิทธิควบคุมที่สามารถระบุได้ ณ เวลาใดเวลาหนึ่ง โดยควรกำหนดให้มีแหล่งข้อมูลหรือระบบที่เป็นข้อมูลอ้างอิงหลัก (Authoritative Record) สำหรับตรวจสอบสถานะของหลักทรัพย์โทเคนแต่ละรายการ และมีกลไกควบคุมการสร้าง ออก โอน หรือยกเลิกหลักทรัพย์โทเคน เพื่อไม่ให้เกิดหลักทรัพย์โทเคนที่มีสิทธิหรือสถานะเดียวกันซ้ำขึ้นมา เช่น ก่อนการออกหลักทรัพย์โทเคน ระบบควรตรวจสอบว่า Token ID ยังไม่ถูกใช้และจำนวนหลักทรัพย์ที่สามารถออกได้สอดคล้องกับข้อมูลที่ได้รับอนุมัติ รวมทั้งกำหนดให้การสร้างหรือออก Token สามารถดำเนินการได้เฉพาะผ่านกลไกที่ได้รับอนุญาต และเมื่อมีการโอนหรือยกเลิกหลักทรัพย์โทเคน ควรมีการปรับสถานะของรายการเดิมให้สอดคล้องกันเพื่อป้องกัน **Unauthorized Replication** และการเกิด **Multiple Claims** ต่อหลักทรัพย์โทเคนรายการเดียวกัน ทั้งนี้ หากมีการเก็บข้อมูลหรือสำเนาข้อมูลของหลักทรัพย์โทเคนไว้ในหลายระบบ ข้อมูลดังกล่าวควรสามารถตรวจสอบกลับมายังหลักทรัพย์โทเคนรายการเดียวกันได้ และไม่ควรถือว่าสำเนาดังกล่าวเป็นหลักทรัพย์โทเคนหรือสิทธิในหลักทรัพย์โทเคนอีกชุดหนึ่ง

- **การกำหนดสิทธิควบคุมหลักทรัพย์โทเคน** : ผู้ให้บริการควรจัดให้มีกลไกหรือกระบวนการที่เชื่อถือได้เพื่อให้สามารถระบุผู้มีสิทธิควบคุมหลักทรัพย์โทเคน (Person in Control) และรับรองการควบคุมหลักทรัพย์โทเคนแต่ละรายการได้อย่างชัดเจน โดยหลักทรัพย์โทเคนควรอยู่ภายใต้การควบคุมแต่เพียงผู้เดียว (**Exclusive Control**) ของผู้มีสิทธิควบคุมตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง ทั้งนี้ การระบุผู้มีสิทธิควบคุมอาจใช้ชื่อบุคคล รหัสประจำตัว (**ID/Identifier**) หรือข้อมูลอ้างอิงอื่นที่สามารถเชื่อมโยงกลับไปยังบุคคลที่เกี่ยวข้องได้ตามระบบที่กำหนด เช่น **Pseudonym หรือ Wallet Address** แต่การระบุดังกล่าวต้องไม่กระทบต่อการระบุผู้ถือหลักทรัพย์โทเคนตามทะเบียนหรือการรับรองสิทธิในหลักทรัพย์โทเคนตามกฎหมายที่เกี่ยวข้อง และการที่บุคคลอื่นสามารถดำเนินการหรือใช้สิทธิควบคุมทางเทคนิคแทนผู้มีสิทธิ เช่น ผู้รับฝากทรัพย์สินหรือผู้ให้บริการที่เกี่ยวข้อง ไม่ทำให้บุคคลดังกล่าวเป็นผู้มีสิทธิควบคุมในทางกฎหมายโดยอัตโนมัติ

ตัวอย่าง : ผู้ให้บริการควรจัดให้มีกระบวนการในการระบุตัวบุคคลที่มีสิทธิในหลักทรัพย์โทเคน และเชื่อมโยงบุคคลดังกล่าวกับหลักทรัพย์โทเคนที่ตนมีสิทธิตามทะเบียน จากนั้นควรนำสิทธิของบุคคลดังกล่าวไปกำหนดและควบคุมในระบบอิเล็กทรอนิกส์ (Implementation of Legal Rights) เพื่อให้สิทธิทางกฎหมายสามารถถูกใช้ได้จริงผ่านช่องทางที่ผู้ให้บริการกำหนด เช่น บัญชีผู้ใช้ (Account) Application หรือ Wallet โดยระบบควรกำหนดสิทธิในการดำเนินการให้สอดคล้องกับสิทธิของผู้ถือหลักทรัพย์ตามกฎหมายและเงื่อนไขของหลักทรัพย์โทเคน เช่น หากผู้ถือมีสิทธิในการโอนหลักทรัพย์ ระบบควรสามารถรองรับการส่งคำสั่งโอนโดยผู้มีสิทธิ หากมีสิทธิในการรับ

ผลประโยชน์หรือใช้สิทธิอื่นที่เกี่ยวข้อง ระบบควรสามารถรองรับการใช้หรือรับสิทธิดังกล่าวได้ตามขอบเขตที่กำหนด และไม่ควรเปิดให้ผู้ใช้สามารถดำเนินการเกินกว่าสิทธิที่ตนมีตามกฎหมาย

ทั้งนี้ ระบบควรสามารถตรวจสอบได้ว่า ณ เวลาใดเวลาหนึ่ง บุคคลใดเป็นผู้มีสิทธิและสามารถดำเนินการเกี่ยวกับหลักทรัพย์โทเคนแต่ละรายการได้ และเมื่อมีการเปลี่ยนแปลงสิทธิ เช่น การโอนหลักทรัพย์ การเปลี่ยนแปลงผู้ถือ หรือการเปลี่ยนแปลงเงื่อนไขของสิทธิ ระบบควรปรับปรุงสิทธิในการดำเนินการให้สอดคล้องกับข้อมูลและสิทธิที่เปลี่ยนแปลงไป

- **การตรวจสอบข้อมูลและหลักฐานการออกหลักทรัพย์โทเคน** : ผู้ให้บริการควรจัดให้มีกระบวนการตรวจสอบข้อมูล รายการ และเงื่อนไขที่เกี่ยวข้องก่อนหรือในขณะที่ออกหลักทรัพย์โทเคน เพื่อให้มั่นใจว่าหลักทรัพย์โทเคนที่สร้างขึ้นมีข้อมูลและเงื่อนไขสอดคล้องกับหลักทรัพย์ที่ออก และสามารถเชื่อมโยงกับข้อมูลในทะเบียนผู้ถือหลักทรัพย์โทเคนหรือระบบงานที่เกี่ยวข้องได้อย่างถูกต้อง รวมทั้งควรจัดให้มีข้อมูลหรือหลักฐานที่สามารถแสดงและตรวจสอบได้ว่าหลักทรัพย์โทเคนดังกล่าวได้ถูกออกโดยผู้มีอำนาจและตามเงื่อนไขที่กำหนด

(2) การจัดทำและบันทึกข้อมูลหลักทรัพย์โทเคน (Registration / Record) : ผู้ให้บริการควรจัดให้มีกลไกหรือกระบวนการสำหรับการจัดทำ บันทึก และปรับปรุงข้อมูลที่เกี่ยวข้องกับหลักทรัพย์โทเคน เพื่อให้ข้อมูลและสถานะของหลักทรัพย์โทเคนมีความถูกต้อง ครบถ้วน เป็นปัจจุบัน และสามารถตรวจสอบย้อนหลังได้ โดยข้อมูลดังกล่าวควรสามารถใช้เป็นข้อมูลอ้างอิงในการดำเนินงานที่เกี่ยวข้องกับหลักทรัพย์โทเคน และสนับสนุนการดำเนินงานของนายทะเบียนหลักทรัพย์หรือผู้ที่เกี่ยวข้องได้อย่างเหมาะสม โดยควรดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

- **การบันทึกและรักษาสถานะของหลักทรัพย์โทเคน** : ผู้ให้บริการควรจัดให้มีระบบสำหรับบันทึกและรักษาข้อมูลสถานะ (**State Record**) ของหลักทรัพย์โทเคนตลอดระยะเวลาที่หลักทรัพย์มีอยู่ โดยสามารถระบุได้ว่าหลักทรัพย์โทเคนแต่ละรายการมีสถานะและข้อมูลที่เกี่ยวข้อง ณ ปัจจุบันอย่างไร เช่น จำนวนหลักทรัพย์ที่มีอยู่ ผู้ถือหรือผู้มีสิทธิที่เกี่ยวข้อง และสถานะหรือข้อจำกัดที่มีผลต่อหลักทรัพย์ รวมทั้งควรสามารถบันทึกและติดตามการเปลี่ยนแปลงของข้อมูลหรือสถานะดังกล่าวได้ตลอดวงจรชีวิตของหลักทรัพย์ โดยสามารถระบุได้ว่าข้อมูลส่วนใดมีการเปลี่ยนแปลง และเชื่อมโยงการเปลี่ยนแปลงแต่ละครั้งกับรายการหรือเหตุการณ์ที่เกี่ยวข้องได้ ทั้งนี้ ควรกำหนดแหล่งข้อมูลอ้างอิงหลัก (**Authoritative Record**) สำหรับข้อมูลดังกล่าว เพื่อให้สามารถนำข้อมูลไปใช้เป็นฐานในการดำเนินงานเกี่ยวกับหลักทรัพย์โทเคนในขั้นตอนอื่นได้อย่างสอดคล้องกัน

ตัวอย่าง : State Record อาจอยู่บนระบบ DLT หรือจัดเก็บในระบบงานอื่นที่เชื่อมโยงกับระบบ DLT ก็ได้ ขึ้นอยู่กับการออกแบบระบบและบทบาทของผู้ให้บริการ โดยในกรณีที่

ข้อมูลสถานะบางส่วนปรากฏอยู่บนระบบ DLT เช่น จำนวน Token ที่ยังมีอยู่และสถานะของ Token ผู้ให้บริการอาจใช้ข้อมูลดังกล่าวเป็นส่วนหนึ่งของ State Record และเชื่อมโยงกับข้อมูลที่จัดเก็บในระบบอื่น เช่น ข้อมูลผู้ถือครองหรือข้อมูลที่อยู่ภายใต้ความรับผิดชอบของนายทะเบียน ทั้งนี้ ไม่จำเป็นต้องจัดเก็บข้อมูลทุกประเภทไว้บนระบบ DLT แต่ควรสามารถระบุแหล่งข้อมูลอ้างอิงของข้อมูลแต่ละประเภท และเชื่อมโยงข้อมูลดังกล่าวกลับมายังหลักทรัพย์โทเคนรายการเดียวกันได้อย่างถูกต้องและติดตามการเปลี่ยนแปลงของสถานะได้อย่างต่อเนื่อง

- **การเชื่อมโยงข้อมูลกับระบบทะเบียนหลักทรัพย์** : ผู้ให้บริการควรจัดให้มีกลไกสำหรับเชื่อมโยงหรือแลกเปลี่ยนข้อมูลระหว่างระบบที่ใช้บันทึกข้อมูลหลักทรัพย์โทเคนกับระบบที่ใช้จัดทำหรือดูแลทะเบียนหลักทรัพย์ เช่น ระบบของนายทะเบียนหลักทรัพย์ หรือระบบของผู้ออกหลักทรัพย์ในกรณีที่ผู้ออกหลักทรัพย์เป็นผู้จัดทำทะเบียนเอง เพื่อให้ข้อมูลเกี่ยวกับหลักทรัพย์โทเคนและข้อมูลผู้ถือหรือผู้มีสิทธิที่เกี่ยวข้องมีความสอดคล้องกัน โดยควรมีกระบวนการตรวจสอบและกระทบยอดข้อมูล (Reconciliation) ตามความถี่ที่เหมาะสมกับลักษณะและความเสี่ยงของระบบ **และในกรณีที่ระบบดังกล่าวทำหน้าที่บันทึกหรือดูแลข้อมูลหลักทรัพย์โทเคนที่มีผลต่อสิทธิของผู้ถือ ควรดำเนินการกระทบยอดอย่างน้อยเป็นรายวัน** เพื่อให้สามารถตรวจพบและแก้ไขความคลาดเคลื่อนระหว่างระบบได้อย่างทันท่วงที

(3) การส่งมอบและการรับมอบหลักทรัพย์โทเคน (Delivery) : ผู้ให้บริการควรจัดให้มีกลไกหรือกระบวนการสำหรับการส่งมอบและรับมอบหลักทรัพย์โทเคน เพื่อให้การส่งมอบหลักทรัพย์โทเคนเป็นไปอย่างถูกต้อง ครบถ้วน และสามารถยืนยันได้ว่าหลักทรัพย์โทเคนได้ถูกส่งมอบและผู้รับมอบได้รับหลักทรัพย์โทเคนตามเงื่อนไขที่กำหนด โดยควรดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

- **การระบุหลักทรัพย์และผู้รับมอบ** : ผู้ให้บริการควรจัดให้มีกระบวนการสำหรับตรวจสอบและระบุหลักทรัพย์โทเคนที่จะส่งมอบ จำนวนหลักทรัพย์ ผู้ส่งมอบ และผู้รับมอบให้ถูกต้อง รวมทั้งตรวจสอบข้อมูลของบัญชีหรือ Wallet ที่เกี่ยวข้องกับการส่งมอบ เพื่อให้มั่นใจว่าหลักทรัพย์โทเคนดังกล่าวสามารถส่งมอบให้แก่ผู้รับมอบที่ระบุไว้ได้ตามสิทธิและเงื่อนไขที่กำหนด และควรสามารถเชื่อมโยงข้อมูลของหลักทรัพย์โทเคนกับข้อมูลของผู้ส่งมอบและผู้รับมอบได้อย่างถูกต้องตลอดกระบวนการส่งมอบ ทั้งนี้ ควรตรวจสอบเงื่อนไขหรือข้อจำกัดที่อาจมีผลต่อการส่งมอบก่อนดำเนินการเพื่อป้องกันการส่งมอบหลักทรัพย์โทเคนที่ไม่สามารถส่งมอบได้หรือส่งมอบให้แก่ผู้รับที่ไม่ถูกต้อง

ตัวอย่าง : กลไกดังกล่าวอาจใช้การตรวจสอบ Token ID หรือ Identifier ของหลักทรัพย์โทเคน จำนวนหลักทรัพย์ ผู้ส่งมอบ และผู้รับมอบ รวมถึงการตรวจสอบบัญชีหรือ Wallet ที่เกี่ยวข้องว่าเชื่อมโยงกับผู้รับมอบที่ถูกต้องและสามารถรับหลักทรัพย์โทเคนได้ตามเงื่อนไขที่กำหนด ทั้งนี้ ระบบอาจใช้ Smart Contract, Transaction Rules, Whitelist หรือกลไกการตรวจสอบสิทธิ

และข้อจำกัดของผู้รับมอบ เพื่อป้องกันหรือปฏิเสธการส่งมอบที่ไม่เป็นไปตามเงื่อนไข เช่น การส่งมอบให้แก่ผู้รับที่ไม่มีสิทธิรับหลักทรัพย์ การส่งมอบเกินจำนวนที่กำหนด หรือการส่งมอบหลักทรัพย์ที่อยู่ภายใต้ข้อจำกัดในการส่งมอบ

- **การดำเนินการส่งมอบและรับมอบ** : ผู้ให้บริการควรจัดให้มีกลไกหรือกระบวนการสำหรับดำเนินการส่งมอบและรับมอบหลักทรัพย์โทเคนตามคำสั่งและเงื่อนไขที่กำหนด โดยควรสามารถยืนยันได้ว่าหลักทรัพย์โทเคนที่ส่งมอบเป็นรายการที่ถูกต้องและการส่งมอบเป็นไปยังผู้รับมอบที่ระบุไว้ ทั้งนี้ เมื่อการส่งมอบเสร็จสมบูรณ์ ผู้รับมอบควรสามารถได้รับและควบคุมหลักทรัพย์โทเคนดังกล่าวได้ตามสิทธิและเงื่อนไขที่กำหนด โดยหลักทรัพย์โทเคนควรอยู่ภายใต้การควบคุมแต่เพียงผู้เดียว (**Exclusive Control**) ของผู้มีสิทธิควบคุมตามผลของการส่งมอบ และไม่ควรเปิดให้ผู้ส่งมอบหรือบุคคลอื่นสามารถควบคุมหรือดำเนินการเกี่ยวกับหลักทรัพย์โทเคนดังกล่าวในลักษณะที่ขัดกับผลของการส่งมอบได้

นอกจากนี้ ควรสามารถระบุได้อย่างชัดเจนว่าเมื่อใดการส่งมอบถือว่าเสร็จสมบูรณ์ และควรบันทึกหรือปรับปรุงสถานะของหลักทรัพย์โทเคนให้สอดคล้องกับผลของการส่งมอบ โดยในกรณีที่การส่งมอบไม่สามารถดำเนินการให้เสร็จสมบูรณ์ได้ เช่น รายการถูกปฏิเสธจากการตรวจสอบเงื่อนไขของระบบหรือธุรกรรมบนระบบ DLT ไม่ได้รับการยืนยัน ควรมีกลไกที่ทำให้สถานะของหลักทรัพย์โทเคนไม่ขัดแย้งกับผลของรายการ และไม่ทำให้เกิดการส่งมอบหรือการควบคุมหลักทรัพย์โทเคนซ้ำซ้อน

- **การจัดให้มีและจัดเก็บหลักฐานการส่งมอบ** : ผู้ให้บริการควรจัดให้มีกลไกหรือกระบวนการสำหรับจัดให้มีและจัดเก็บข้อมูลหรือหลักฐานที่สามารถยืนยันการส่งมอบและรับมอบหลักทรัพย์โทเคนได้อย่างเหมาะสม โดยหลักฐานดังกล่าวควรมีความน่าเชื่อถือ สามารถระบุหลักทรัพย์โทเคนที่เกี่ยวข้อง จำนวน ผู้ส่งมอบ ผู้รับมอบ วันและเวลาของรายการ รวมถึงผลและสถานะของการส่งมอบ และควรสามารถเชื่อมโยงกับรายการที่เกิดขึ้นในระบบที่เกี่ยวข้องได้อย่างถูกต้อง ทั้งนี้ ควรจัดเก็บหลักฐานในลักษณะที่สามารถรักษาความถูกต้องครบถ้วนของข้อมูล และสามารถตรวจสอบหรือเรียกดูย้อนหลังได้ตลอดระยะเวลาที่กำหนดตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง ในกรณีที่การส่งมอบดำเนินการผ่านระบบ DLT ข้อมูลการทำรายการและข้อมูลที่ใช้ยืนยันผลของรายการบนระบบดังกล่าวอาจใช้เป็นส่วนหนึ่งของหลักฐานการส่งมอบได้

(4) การโอนและรับโอนหลักทรัพย์โทเคน (Transfer) : ผู้ให้บริการควรจัดให้มีกลไกหรือกระบวนการสำหรับการโอนและรับโอนหลักทรัพย์โทเคน เพื่อให้การโอนหลักทรัพย์โทเคนและการเปลี่ยนแปลงสิทธิในหลักทรัพย์โทเคนเป็นไปอย่างถูกต้อง ครบถ้วน และสอดคล้องกับสิทธิและเงื่อนไขที่กำหนด โดยควรดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

- **การตรวจสอบสิทธิและเงื่อนไขก่อนการโอน** : ผู้ให้บริการควรจัดให้มีกลไกสำหรับตรวจสอบข้อมูลที่เกี่ยวข้องกับการโอน เช่น ผู้โอน ผู้รับโอน หลักทรัพย์โทเคน และจำนวนหลักทรัพย์ ให้สอดคล้องกับข้อมูลและสิทธิที่เกี่ยวข้อง รวมทั้งตรวจสอบว่าคำสั่งโอนมาจากหรือได้รับอนุญาตโดยผู้มีสิทธิในการดำเนินการเกี่ยวกับหลักทรัพย์โทเคนดังกล่าว และควรสามารถตรวจสอบเงื่อนไขหรือข้อจำกัดที่มีผลต่อการโอน เพื่อให้การดำเนินการโอนเป็นไปตามข้อมูลและเงื่อนไขที่กำหนด ทั้งนี้ การตรวจสอบดังกล่าวควรเป็นส่วนหนึ่งของกระบวนการดำเนินการโอนตามที่กำหนด และไม่ควรหมายความว่าผู้ให้บริการต้องพิจารณาหรืออนุมัติการโอนแต่ละรายการด้วยดุลพินิจ เว้นแต่เป็นหน้าที่ของผู้ให้บริการตามกฎหมายหรือหลักเกณฑ์ที่เกี่ยวข้อง

ตัวอย่าง : ระบบอาจกำหนดเงื่อนไขการโอนใน Smart Contract หรือ Transaction Rules ให้ตรวจสอบว่าคำสั่งโอนมาจากผู้มีสิทธิหรือผู้ที่ได้รับมอบอำนาจจากผู้มีสิทธิ และตรวจสอบข้อมูลของผู้โอน ผู้รับโอน และหลักทรัพย์โทเคนก่อนดำเนินการ เช่น ตรวจสอบว่า Wallet หรือ Account ที่ใช้ส่งคำสั่งมีความเชื่อมโยงกับผู้มีสิทธิหรือผู้ได้รับอนุญาต มีจำนวนหลักทรัพย์เพียงพอ หลักทรัพย์ไม่อยู่ในสถานะที่ห้ามโอน และผู้รับโอนมีคุณสมบัติหรืออยู่ใน Whitelist ตามที่กำหนด หากเงื่อนไขครบถ้วน ระบบจึงดำเนินการโอน แต่หากไม่เป็นไปตามเงื่อนไข ระบบจะปฏิเสธธุรกรรมโดยอัตโนมัติ

- **การดำเนินการโอนและการบันทึกผล** : ผู้ให้บริการควรจัดให้มีกลไกหรือกระบวนการสำหรับดำเนินการโอนและรับโอนหลักทรัพย์โทเคนตามคำสั่งและเงื่อนไขที่กำหนด โดยเมื่อการโอนเสร็จสมบูรณ์ สิทธิในหลักทรัพย์โทเคนควรเปลี่ยนจากผู้โอนไปยังผู้รับโอน และการควบคุมหลักทรัพย์โทเคนควรเปลี่ยนไปอยู่ภายใต้การควบคุมแต่เพียงผู้เดียว (Exclusive Control) ของผู้รับโอนตามสิทธิที่ได้รับ โดยไม่ควรเปิดให้ผู้โอนหรือบุคคลอื่นสามารถควบคุมหรือดำเนินการเกี่ยวกับหลักทรัพย์โทเคนดังกล่าวในลักษณะที่ขัดกับผลของการโอนได้ ทั้งนี้ ควรมีการบันทึกหรือปรับปรุงข้อมูลและสถานะของหลักทรัพย์โทเคนให้สอดคล้องกับผลของการโอน และสามารถระบุและตรวจสอบได้ว่าการเปลี่ยนแปลงสิทธิและการควบคุมดังกล่าวเกิดขึ้นจากรายการใด หากการโอนไม่สำเร็จ ถูกปฏิเสธ หรือเกิดความผิดพลาดในการดำเนินการ ควรมีกลไกสำหรับบริหารจัดการกรณีดังกล่าว และปรับปรุงข้อมูลหรือสถานะที่เกี่ยวข้องให้สอดคล้องกับผลของรายการ เพื่อป้องกันไม่ให้เกิดกรณีที่หลักทรัพย์โทเคนถูกหักจากผู้โอนแล้ว แต่ยังไม่ถูกโอนไปยังผู้รับโอน หรือเกิดการโอนซ้ำ

ตัวอย่าง : ในกรณีที่หลักทรัพย์โทเคนถูกควบคุมผ่าน Wallet ระบบอาจกำหนดให้การโอนสำเร็จต่อเมื่อธุรกรรมได้รับการยืนยันตามเงื่อนไขที่กำหนด และทำให้สิทธิในการควบคุมหลักทรัพย์โทเคนเปลี่ยนจาก Wallet ของผู้โอน ไปยัง Wallet ของผู้รับโอน เช่น Smart Contract จะลดจำนวนหลักทรัพย์โทเคนที่อยู่ภายใต้การควบคุมของผู้โอน และเพิ่มจำนวนดังกล่าวให้แก่ผู้รับโอน พร้อมทั้งปรับปรุงสถานะหรือข้อมูลที่ใช้ระบุผู้มีสิทธิให้สอดคล้องกัน เมื่อรายการเสร็จสมบูรณ์ ผู้โอนไม่

ควรสามารถใช้ Key หรือกลไกเดิมเพื่อโอนหรือดำเนินการกับหลักทรัพย์โทเคนที่โอนไปแล้วได้อีก ขณะที่ผู้รับโอนสามารถใช้กลไกการควบคุมที่กำหนดสำหรับ Wallet ของตนในการดำเนินการกับหลักทรัพย์โทเคนดังกล่าวได้ตามสิทธิ

(5) การใช้หลักทรัพย์โทเคนเป็นหลักประกัน (Pledge) : ผู้ให้บริการควรจัดให้มีกลไกหรือกระบวนการที่สามารถรองรับการสร้าง บันทึก และเปลี่ยนแปลงสถานะของสิทธิหรือข้อจำกัดที่เกิดจากการนำหลักทรัพย์โทเคนไปเป็นหลักประกัน เพื่อให้ข้อมูลและสถานะของหลักทรัพย์โทเคนสอดคล้องกับสิทธิของผู้ที่เกี่ยวข้องและหลักเกณฑ์ตามกฎหมาย ทั้งนี้ การดำเนินการของผู้ให้บริการควรเป็นไปตามบทบาทและหน้าที่ที่ได้รับมอบหมาย และควรสามารถเชื่อมโยงหรือแลกเปลี่ยนข้อมูลกับระบบทะเบียนหลักทรัพย์หรือระบบงานที่เกี่ยวข้องได้ตามความเหมาะสม

- **การตรวจสอบข้อมูลและเงื่อนไขก่อนการสร้างหลักประกัน** : ผู้ให้บริการควรจัดให้มีกลไกสำหรับตรวจสอบข้อมูล สิทธิ และเงื่อนไขที่เกี่ยวข้องกับการนำหลักทรัพย์โทเคนไปเป็นหลักประกันในขอบเขตที่ระบบและหน้าที่ของผู้ให้บริการกำหนด เช่น หลักทรัพย์โทเคนที่นำไปเป็นหลักประกัน จำนวนหลักทรัพย์ ผู้จำนำ ผู้รับจำนำ และสถานะหรือข้อจำกัดของหลักทรัพย์ เพื่อให้สามารถระบุได้ว่ารายการดังกล่าวเป็นไปตามเงื่อนไขที่กำหนดก่อนดำเนินการสร้างหรือบันทึกหลักประกัน ทั้งนี้ การตรวจสอบดังกล่าวเป็นการตรวจสอบข้อมูลและเงื่อนไขตามที่กำหนดในระบบ และไม่รวมถึงการวินิจฉัยความมีผลหรือข้อผูกพันทางกฎหมายของการจำนำ เว้นแต่เป็นหน้าที่ของผู้ให้บริการตามกฎหมายหรือหลักเกณฑ์ที่เกี่ยวข้อง

ตัวอย่าง : กรณีผู้ถือหลักทรัพย์โทเคนประสงค์จะนำหลักทรัพย์จำนวน 100 หน่วยไปเป็นหลักประกัน ระบบอาจตรวจสอบว่า Token ที่ระบุเป็นหลักทรัพย์ของผู้จำนำจริง มีจำนวนเพียงพอ และไม่ได้อยู่ในสถานะที่ห้ามหรือจำกัดการนำไปเป็นหลักประกัน รวมทั้งตรวจสอบว่าผู้รับจำนำและคำสั่งที่เกี่ยวข้องเป็นไปตามเงื่อนไขที่ระบบกำหนด เช่น ผู้สั่งรายการเป็นผู้มีสิทธิหรือผู้ที่ได้รับมอบอำนาจจากผู้มีสิทธิ ทั้งนี้ ระบบไม่จำเป็นต้องวินิจฉัยเองว่าข้อตกลงจำนำระหว่างคู่สัญญามีผลสมบูรณ์ตามกฎหมายหรือไม่ หากเรื่องดังกล่าวไม่ได้อยู่ในหน้าที่ของผู้ให้บริการ

- **การบันทึกและจัดการสถานะของหลักทรัพย์โทเคนที่เป็นหลักประกัน** : ผู้ให้บริการควรจัดให้มีกลไกสำหรับบันทึกและปรับปรุงสถานะของหลักทรัพย์โทเคนที่ถูกนำไปเป็นหลักประกันให้สอดคล้องกับผลของการสร้างหลักประกัน รวมทั้งควรสามารถระบุได้ว่าหลักทรัพย์โทเคนดังกล่าวอยู่ภายใต้สิทธิหรือข้อจำกัดใดจากการเป็นหลักประกัน และบุคคลใดเป็นผู้มีสิทธิที่เกี่ยวข้องกับหลักประกันดังกล่าว ทั้งนี้ ควรจัดให้มีกลไกที่สามารถกำหนดหรือบังคับใช้การควบคุมหรือข้อจำกัดในการดำเนินการเกี่ยวกับหลักทรัพย์โทเคนตามสิทธิของผู้รับจำนำและผู้จำนำที่กำหนดไว้

เช่น การจำกัดการโอนหรือการดำเนินการอื่นที่อาจกระทบต่อสิทธิของผู้รับจำนำ เพื่อให้สามารถรักษาสถานะและสิทธิที่เกี่ยวข้องกับหลักประกันของผู้รับจำนำได้ตามกฎหมายและเงื่อนไขที่เกี่ยวข้อง

ทั้งนี้ การบันทึกและจัดการสถานะของหลักทรัพย์โทเคนที่เป็นหลักประกันควรดำเนินการให้สอดคล้องกับข้อมูลในระบบทะเบียนหลักทรัพย์หรือระบบงานที่เกี่ยวข้องตามบทบาทและหน้าที่ของผู้ให้บริการ และการกำหนดข้อจำกัดหรือการควบคุมทางระบบเพื่อรักษาสิทธิของผู้รับจำนำไม่ควรทำให้เกิดการเปลี่ยนแปลงผู้ถือหรือการโอนสิทธิในหลักทรัพย์โทเคนไปยังผู้รับจำนำโดยอัตโนมัติ เว้นแต่เป็นผลตามกฎหมายหรือเงื่อนไขของหลักประกัน

ตัวอย่าง : กรณีผู้ถือหลักทรัพย์โทเคนจำนวน 100 หน่วยนำหลักทรัพย์ดังกล่าวไปเป็นหลักประกัน ระบบควรสามารถบันทึกสถานะของหลักทรัพย์โทเคนดังกล่าวว่า **“Pledged”** และเชื่อมโยงข้อมูลกับผู้จำนำ ผู้รับจำนำ จำนวนหลักทรัพย์ และเงื่อนไขหรือข้อจำกัดที่เกี่ยวข้อง นอกจากนี้ ระบบอาจกำหนดกลไกในการควบคุมหลักทรัพย์โทเคนได้หลายรูปแบบตามโครงสร้างของระบบ เช่น **(1) การ Lock หลักทรัพย์โทเคนไว้ใน Wallet ของผู้จำนำ** โดยระบบหรือ Smart Contract กำหนดสถานะหรือเงื่อนไขที่ไม่ให้หลักทรัพย์โทเคนดังกล่าวถูกโอนหรือดำเนินการอื่นที่ขัดต่อสิทธิของผู้รับจำนำในระหว่างที่มีการเป็นหลักประกัน หรือ **(2) การโอนหลักทรัพย์โทเคนไปยัง Wallet กลางหรือ Smart Contract ที่จัดไว้สำหรับการเป็นหลักประกัน (Escrow / Pledge Smart Contract)** เพื่อให้หลักทรัพย์โทเคนถูกแยกและอยู่ภายใต้กลไกการควบคุมที่กำหนด โดยอาจกำหนดให้สามารถโอนหลักทรัพย์โทเคนออกจาก Wallet หรือ Smart Contract ดังกล่าวได้เฉพาะเมื่อเป็นไปตามเงื่อนไขที่กำหนด เช่น การปลดหลักประกันหรือการบังคับหลักประกัน

ในทั้งสองกรณี ระบบควรสามารถเชื่อมโยงหลักทรัพย์โทเคนกับข้อมูลของผู้จำนำ ผู้รับจำนำ และสถานะการเป็นหลักประกัน และกำหนดกลไกเพื่อป้องกันการดำเนินการที่อาจกระทบต่อสิทธิของผู้รับจำนำโดยไม่เป็นไปตามเงื่อนไขที่กำหนด ทั้งนี้ การที่หลักทรัพย์โทเคนถูก Lock หรืออยู่ภายใต้การควบคุมของ Wallet หรือ Smart Contract กลาง **ไม่ควรทำให้ผู้รับจำนำเป็นผู้ถือหลักทรัพย์โทเคนหรือเป็นผู้มีสิทธิได้รับดอกผลหรือสิทธิประโยชน์จากหลักทรัพย์โดยอัตโนมัติ** โดยการจัดสรรดอกผลหรือสิทธิประโยชน์ควรเป็นไปตามสิทธิของผู้ถือและเงื่อนไขของหลักประกันที่เกี่ยวข้อง

- **การเปลี่ยนแปลง การปลด และการบังคับหลักประกัน** : ผู้ให้บริการควรจัดให้มีกลไกสำหรับรองรับการเปลี่ยนแปลง การปลด หรือการบังคับหลักประกันที่เกี่ยวข้องกับหลักทรัพย์โทเคนให้สอดคล้องกับสิทธิและเงื่อนไขของหลักประกัน รวมทั้งควรสามารถปรับปรุงสถานะ จำนวน หรือข้อจำกัดของหลักทรัพย์โทเคนให้สอดคล้องกับผลของการเปลี่ยนแปลงดังกล่าว โดยการดำเนินการควรอาศัยข้อมูล คำสั่ง หรือหลักฐานจากผู้มีอำนาจตามกฎหมายหรือเงื่อนไขของหลักประกัน และควรมีกลไก

ตรวจสอบเพื่อป้องกันการเปลี่ยนแปลง การปลดข้อจำกัด หรือการดำเนินการกับหลักทรัพย์โทเคนโดยไม่ได้รับอนุญาต

ทั้งนี้ เมื่อมีการปลดหลักประกัน ผู้ให้บริการควรสามารถปรับปรุงสถานะของหลักทรัพย์โทเคนจากสถานะที่อยู่ภายใต้หลักประกัน และยกเลิกหรือปรับลดข้อจำกัดในการโอนหรือการดำเนินการเกี่ยวกับหลักทรัพย์โทเคนให้สอดคล้องกับส่วนของหลักประกันที่ได้รับการปลด และในกรณีที่มีการบังคับหลักประกัน ผู้ให้บริการควรสามารถดำเนินการกับหลักทรัพย์โทเคนให้สอดคล้องกับผลของการบังคับหลักประกัน เช่น การเปลี่ยนแปลงผู้มีสิทธิ การเปลี่ยนแปลงการควบคุมหลักทรัพย์โทเคน และการโอนหรือส่งมอบหลักทรัพย์โทเคนไปยังผู้รับจำนำหรือบุคคลอื่นที่มีสิทธิตามกฎหมายหรือเงื่อนไขของหลักประกัน แล้วแต่กรณี ทั้งนี้ การดำเนินการดังกล่าวควรทำให้ข้อมูลและสถานะของหลักทรัพย์โทเคนในระบบที่เกี่ยวข้องสอดคล้องกับข้อมูลในระบบทะเบียนหลักทรัพย์ และควรสามารถจัดเก็บหลักฐานและตรวจสอบย้อนหลังได้ว่า การเปลี่ยนแปลง การปลด หรือการบังคับหลักประกันเกิดขึ้นจากเหตุหรือคำสั่งใด และมีผลต่อหลักทรัพย์โทเคนรายการใดบ้าง

ตัวอย่าง : สมมติว่า A นำหลักทรัพย์โทเคนจำนวน 100 หน่วยไปเป็นหลักประกันกับ B ระบบอาจบันทึกสถานะของ Token ทั้ง 100 หน่วยเป็น Pledged และกำหนดข้อจำกัดไม่ให้โอนออกจาก Wallet ของ A ในระหว่างที่หลักประกันมีผล หากต่อมามีการเปลี่ยนแปลงหลักประกัน เช่น ลดจำนวนหลักประกันจาก 100 หน่วยเหลือ 60 หน่วย ระบบควรสามารถปรับสถานะของ Token จำนวน 40 หน่วยให้พ้นจากสถานะ Pledged และยกเลิกข้อจำกัดในการโอนของ Token จำนวนดังกล่าว ขณะที่ Token อีก 60 หน่วยยังคงอยู่ภายใต้สถานะ Pledged และข้อจำกัดเดิม

ในกรณีที่มีการปลดหลักประกันทั้งหมด ระบบอาจเปลี่ยนสถานะ Token จาก Pledged กลับเป็นสถานะที่สามารถโอนได้ตามปกติ และยกเลิกกลไกที่ใช้ Lock Token หรือข้อจำกัดใน Smart Contract หรือ Transaction Rules เพื่อให้ A สามารถควบคุมและดำเนินการกับ Token ได้ตามสิทธิของตนอีกครั้ง ทั้งนี้ ระบบควรบันทึกเหตุการณ์การปลดหลักประกันและเชื่อมโยงกับคำสั่งหรือหลักฐานที่เกี่ยวข้อง โดยในในทางกลับกัน หากเกิดการบังคับหลักประกันตามเงื่อนไขที่กำหนด ระบบอาจเปลี่ยนสถานะของ Token จาก Pledged เป็นสถานะที่สามารถดำเนินการตามผลของการบังคับหลักประกัน และดำเนินการโอน Token จาก Wallet ของ A ไปยัง Wallet ของ B หรือบุคคลอื่นที่มีสิทธิตามกฎหมายหรือเงื่อนไขของหลักประกัน โดย Smart Contract อาจกำหนดให้การโอนดังกล่าวสามารถเกิดขึ้นได้เมื่อมีข้อมูลหรือคำสั่งที่ผ่านการตรวจสอบตามเงื่อนไขที่กำหนด และเมื่อการโอนเสร็จสมบูรณ์ ระบบควรปรับปรุงข้อมูลผู้มีสิทธิและการควบคุม Token ให้สอดคล้องกับผลของการบังคับหลักประกัน

กรณีที่ใช้ **Pledge / Escrow Smart Contract** แทนการ Lock Token ใน Wallet ของ A ก็สามารถใช้หลักการเดียวกันได้ โดยเมื่อมีการเปลี่ยนแปลงหรือปลดหลักประกัน Smart Contract อาจปล่อย Token กลับไปยัง A ตามจำนวนที่เกี่ยวข้อง หรือเมื่อมีการบังคับหลักประกัน อาจโอน Token ไปยัง B หรือผู้มีสิทธิตามเงื่อนไขที่กำหนด ทั้งนี้ การเปลี่ยนแปลงสถานะทางเทคนิคดังกล่าวควรเกิดขึ้นตามผลทางกฎหมายของหลักประกัน ไม่ใช่ทำให้การเปลี่ยนแปลงทางเทคนิคเป็นเหตุให้เกิดสิทธิในหลักทรัพย์ขึ้นเอง

(6) การให้บริการด้านสิทธิประโยชน์และการดำเนินการตามสิทธิของผู้ถือหลักทรัพย์ (Asset Servicing / Corporate Actions) : ผู้ให้บริการควรจัดให้มีกลไกหรือกระบวนการสำหรับรองรับการดำเนินการเกี่ยวกับสิทธิประโยชน์และสิทธิของผู้ถือหลักทรัพย์โทเคนตลอดอายุของหลักทรัพย์ เพื่อให้การระบุผู้มีสิทธิ การคำนวณและจัดสรรสิทธิประโยชน์ ตลอดจนการใช้หรือดำเนินการตามสิทธิของผู้ถือหลักทรัพย์เป็นไปอย่างถูกต้อง ครบถ้วน และสอดคล้องกับเงื่อนไขของหลักทรัพย์โทเคนและข้อมูลในระบบทะเบียนหลักทรัพย์หรือระบบงานที่เกี่ยวข้อง ทั้งนี้ การดำเนินการของผู้ให้บริการควรเป็นไปตามบทบาทและหน้าที่ที่ได้รับมอบหมายและไม่ควรทำให้เกิดการเปลี่ยนแปลงสิทธิของผู้ถือหลักทรัพย์นอกเหนือจากที่กำหนดตามกฎหมายหรือเงื่อนไขของหลักทรัพย์

ผู้ให้บริการควรจัดให้มีกระบวนการสำหรับระบุและตรวจสอบเหตุการณ์ที่ก่อให้เกิดสิทธิหรือการดำเนินการเกี่ยวกับหลักทรัพย์โทเคน เช่น การจ่ายเงินปันผลหรือดอกเบี้ย การไถ่ถอน การแบ่งหรือรวมหรือเปลี่ยนแปลงจำนวนหลักทรัพย์ การใช้สิทธิของผู้ถือ หรือการดำเนินการอื่นที่มีผลต่อสิทธิของผู้ถือหลักทรัพย์ รวมทั้งควรสามารถกำหนด วันและเวลาที่ใช้เป็นเกณฑ์ในการระบุผู้มีสิทธิ (Record Date / Entitlement Date) และข้อมูลที่ใช้ในการคำนวณหรือจัดสรรสิทธิให้สอดคล้องกับข้อมูลผู้ถือหลักทรัพย์ที่เกี่ยวข้อง

เมื่อมีการดำเนินการตามสิทธิ ผู้ให้บริการควรสามารถปรับปรุงข้อมูลหรือสถานะของหลักทรัพย์โทเคนและดำเนินการจัดสรรหรือส่งมอบสิทธิประโยชน์ให้แก่ผู้มีสิทธิตามที่กำหนด โดยควรสามารถเชื่อมโยงการดำเนินการดังกล่าวกับหลักทรัพย์โทเคน ผู้มีสิทธิ และเหตุการณ์ที่เกี่ยวข้อง และควรจัดให้มีหลักฐานที่สามารถตรวจสอบย้อนหลังได้ ทั้งนี้ ในกรณีที่การดำเนินการเกี่ยวข้องกับการเปลี่ยนแปลงสิทธิหรือจำนวนหลักทรัพย์โทเคน ระบบควรสามารถทำให้ข้อมูลและสถานะของหลักทรัพย์โทเคนภายหลังการดำเนินการสอดคล้องกับสิทธิที่เกิดขึ้นจริง

ในกรณีที่หลักทรัพย์โทเคนสิ้นสภาพตามกฎหมายหรือเงื่อนไขของหลักทรัพย์ เช่น การไถ่ถอนครบจำนวนหรือการครบกำหนดที่ทำให้สิทธิในหลักทรัพย์สิ้นสุดลง ผู้ให้บริการควรจัดให้มีกลไกในการปรับปรุงสถานะของหลักทรัพย์โทเคนให้สะท้อนการสิ้นสภาพดังกล่าว

และป้องกันมิให้หลักทรัพย์โทเคนที่สิ้นสภาพแล้วถูกนำกลับมาโอนหรือใช้สิทธิซ้ำ ทั้งนี้ ควรจัดให้มีข้อมูลหรือหลักฐานที่สามารถตรวจสอบย้อนหลังเกี่ยวกับการสิ้นสภาพดังกล่าวได้อย่างเหมาะสมและครบถ้วน

5.4.2 งานด้านการถือครองและการดูแลหลักทรัพย์โทเคน

หลักการทั่วไป

ผู้ให้บริการควรจัดให้มีกระบวนการและระบบงานที่เหมาะสมกับลักษณะ ขอบเขต และความซับซ้อนของบริการที่ตนรับผิดชอบ เพื่อให้สามารถระบุผู้มีสิทธิและสถานะการควบคุมหลักทรัพย์โทเคนได้อย่างถูกต้อง และเพื่อให้หลักทรัพย์โทเคนของลูกค้าได้รับการดูแลและคุ้มครองตามสิทธิและเงื่อนไขที่เกี่ยวข้องตลอดระยะเวลาที่อยู่ภายใต้การให้บริการ

การให้บริการด้านการถือครองหรือการดูแลหลักทรัพย์โทเคนอาจครอบคลุมทั้ง **การจัดให้มีหรือให้บริการเกี่ยวกับกระเป๋าอิเล็กทรอนิกส์ที่ลูกค้าเป็นผู้ควบคุมหลักทรัพย์โทเคนด้วยตนเอง (Non-Custodial Wallet) และการรับฝากหรือเก็บรักษาหลักทรัพย์โทเคนโดยผู้ให้บริการเป็นผู้ควบคุมหลักทรัพย์โทเคนหรือกลไกที่ใช้ในการควบคุมแทนลูกค้า (Custodial Service)** ทั้งนี้ ผู้ให้บริการควรดำเนินการเฉพาะในขอบเขตของบริการที่ตนรับผิดชอบ และจัดให้มีระบบงานที่สอดคล้องกับลักษณะและระดับความเสี่ยงของบริการดังกล่าว

ในการดำเนินงาน ผู้ให้บริการควรคำนึงถึงการรักษาความเป็นหนึ่งเดียวของหลักทรัพย์โทเคน (Singularity) ความถูกต้องครบถ้วนของข้อมูล (Integrity) และการควบคุมหลักทรัพย์โทเคน (Control) รวมทั้งควรสามารถระบุความสัมพันธ์ระหว่างหลักทรัพย์โทเคน ผู้ถือหรือผู้มีสิทธิ และบัญชีหรือกระเป๋าที่ใช้ในการถือครองหรือควบคุมหลักทรัพย์โทเคนได้อย่างเหมาะสม ทั้งนี้ การควบคุมหลักทรัพย์โทเคนในทางเทคนิคของผู้ให้บริการหรือบุคคลที่เกี่ยวข้องไม่ควรทำให้เกิดการเปลี่ยนแปลงผู้ถือหรือสิทธิในหลักทรัพย์โทเคน เว้นแต่เป็นไปตามกฎหมายหรือเงื่อนไขของหลักทรัพย์โทเคน

ข้อเสนอแนะ : ผู้ให้บริการควรจัดให้มีระบบงานและกระบวนการที่เหมาะสมกับขอบเขตหน้าที่และประเภทของบริการที่ตนให้บริการ โดยควรดำเนินการเฉพาะในส่วนที่เกี่ยวข้องกับบริการที่ตนรับผิดชอบ ดังต่อไปนี้

(1) การจัดให้มีหรือให้บริการเกี่ยวกับ Non-Custodial Wallet : ในกรณีที่ผู้ให้บริการจัดให้มีหรือให้บริการเกี่ยวกับ Non-Custodial Wallet ผู้ให้บริการควรจัดให้มีระบบงานที่เหมาะสมดังต่อไปนี้

- **การออกแบบและพัฒนา Wallet :** ควรออกแบบและพัฒนา Wallet ให้เหมาะสมกับลักษณะของหลักทรัพย์โทเคนและรูปแบบการให้บริการ โดยคำนึงถึงความมั่นคงปลอดภัยการควบคุมหลักทรัพย์โทเคนโดยผู้มีสิทธิ ความถูกต้องและครบถ้วนของข้อมูล ความสามารถในการตรวจสอบและติดตามการทำรายการ ตลอดจนการรองรับการเปลี่ยนแปลงและการยุติการใช้งาน

Wallet ทั้งนี้ ในกรณีที่ใช้ Wallet ที่จัดให้โดยผู้ให้บริการรายอื่น ควรพิจารณาความเหมาะสมและความเสี่ยงของ Wallet และการเชื่อมต่อดังกล่าวในส่วนที่เกี่ยวข้องกับบริการของตน

- **การจัดการ Credential และการควบคุม Wallet :** ควรมีกระบวนการสำหรับการจัดให้มีหรือสร้าง Credential หรือกลไกที่ใช้ในการควบคุม Wallet โดยควรเลือกใช้รูปแบบของ Credential และกลไกการควบคุมที่เหมาะสมกับลักษณะและ architecture ของ Wallet รวมถึงลักษณะของหลักทรัพย์โทเคนและความเสี่ยงที่เกี่ยวข้อง เช่น ในกรณีที่ Wallet ใช้ Private Key หรือ Seed Phrase ควรมีกระบวนการที่ทำให้ลูกค้าสามารถสร้างหรือได้รับและเก็บรักษา Credential ดังกล่าวด้วยตนเอง ขณะที่ในกรณีที่ Wallet ใช้ Multi-Party Computation (MPC)[6] หรือ Smart Contract Wallet ควรกำหนดการควบคุมและการอนุมัติการทำรายการให้เหมาะสมกับarchitecture ของ Wallet ทั้งนี้ ควรจัดให้ลูกค้าหรือผู้มีสิทธิสามารถควบคุม Wallet ได้ตามสิทธิที่กำหนด และควรป้องกันไม่ให้ผู้ให้บริการหรือบุคคลอื่นสามารถควบคุมหลักทรัพย์โทเคนของลูกค้าโดยลำพัง

- **การทดสอบและประเมินความพร้อม :** ควรจัดให้มีกระบวนการทดสอบและประเมินความพร้อมของ Wallet และระบบที่เกี่ยวข้องก่อนให้บริการแก่ลูกค้า เพื่อให้มั่นใจว่าสามารถทำงานได้อย่างถูกต้องและสามารถรองรับการทำรายการและกรณีผิดพลาดที่อาจเกิดขึ้นได้อย่างเหมาะสม ทั้งนี้ ในกรณีที่ใช้ Wallet ที่จัดให้โดยผู้ให้บริการรายอื่น ควรทดสอบและประเมินความพร้อมในส่วนของการเชื่อมต่อและการทำงานร่วมกันตามขอบเขตหน้าที่ของผู้ให้บริการ

- **การจัดให้มี เปิดใช้งาน และเชื่อมโยง Wallet :** ควรจัดให้มีกระบวนการสำหรับการจัดให้มีหรือเปิดใช้งาน Wallet และการเชื่อมโยง Wallet กับลูกค้าที่ได้รับอนุญาตและหลักทรัพย์โทเคนที่เกี่ยวข้อง เพื่อให้สามารถระบุและตรวจสอบความสัมพันธ์ระหว่างลูกค้า Wallet และหลักทรัพย์โทเคนได้อย่างถูกต้อง และสามารถตรวจสอบข้อมูลดังกล่าวได้ตลอดระยะเวลาที่ให้บริการ ทั้งนี้ ในกรณีที่เป็น Wallet ที่จัดให้โดยผู้ให้บริการรายอื่น ควรมีกระบวนการสำหรับการเชื่อมต่อและตรวจสอบข้อมูลตามขอบเขตหน้าที่ของผู้ให้บริการ

- **การตรวจสอบสิทธิและเงื่อนไขในการทำรายการ :** ควรมีกระบวนการสำหรับตรวจสอบว่าการทำรายการผ่าน Wallet ดำเนินการโดยลูกค้าหรือผู้มีสิทธิ หรือบุคคลที่ได้รับมอบอำนาจหรือได้รับอนุญาตจากผู้มีสิทธิ และเป็นไปตามสิทธิและเงื่อนไขของหลักทรัพย์โทเคน รวมทั้งควร

[6] Multi-party Computation (MPC) หมายถึง เทคนิคทางการเข้ารหัสที่ช่วยให้หลายฝ่ายร่วมกันดำเนินการทางคริปโทกราฟีได้โดยไม่ต้องเปิดเผยข้อมูลลับของแต่ละฝ่าย โดยในการจัดการกุญแจเข้ารหัส หลายฝ่ายสามารถร่วมกันใช้งานกุญแจส่วนตัว (Private Key) โดยไม่ต้องเปิดเผยกุญแจฉบับสมบูรณ์แก่ฝ่ายใดฝ่ายหนึ่ง ช่วยลดความเสี่ยงจากการรั่วไหล การโจรกรรม และการพึ่งพาจุดควบคุมเพียงจุดเดียว

คำนึงถึงข้อจำกัดที่เกี่ยวข้องกับ Wallet หรือหลักทรัพย์โทเคนก่อนการทำรายการ เพื่อป้องกันการทำรายการโดยไม่ได้รับอนุญาตหรือไม่เป็นไปตามเงื่อนไขที่กำหนด

- **การรองรับการทำรายการและการแสดงสถานะ :** ควรมีกระบวนการสำหรับรองรับการรับ การส่งมอบ การโอน และการดำเนินการอื่นเกี่ยวกับหลักทรัพย์โทเคนผ่าน Wallet และควรสามารถแสดงหรือยืนยันผลและสถานะของรายการ รวมทั้งข้อมูลเกี่ยวกับหลักทรัพย์โทเคนที่อยู่ภายใต้ Wallet ได้อย่างถูกต้อง ครบถ้วน และเป็นปัจจุบัน โดยควรสามารถเชื่อมโยงข้อมูลดังกล่าวกับระบบที่เกี่ยวข้องและจัดเก็บหลักฐานเพื่อให้สามารถตรวจสอบย้อนหลังได้

- **การบริหารจัดการ Wallet และ Credential ตลอดวงจรชีวิต :** ควรมีกระบวนการรองรับการเปลี่ยนแปลง การระงับ การสูญเสียการเข้าถึง การเปลี่ยนหรือย้าย Wallet และการยุติการใช้งาน Wallet รวมทั้งควรมีกลไกที่เหมาะสมสำหรับการเปลี่ยนแปลงหรือกู้คืนการควบคุม Wallet ตามรูปแบบที่กำหนด โดยกลไกดังกล่าวไม่ควรทำให้ผู้ให้บริการสามารถควบคุมหรือโอนหลักทรัพย์โทเคนของลูกค้าโดยลำพัง ทั้งนี้ เมื่อมีการเปลี่ยนแปลง Wallet หรือ Credential ที่ใช้ในการควบคุม Wallet ควรสามารถปรับปรุงความเชื่อมโยงระหว่างลูกค้า Wallet และหลักทรัพย์โทเคนให้ถูกต้องและเป็นปัจจุบัน และไม่ทำให้เกิดความไม่สอดคล้องกันเกี่ยวกับผู้มีสิทธิหรือการควบคุมหลักทรัพย์โทเคน เช่น ในกรณีที่ลูกค้าเปลี่ยน Wallet หรือเปลี่ยน Credential ควรสามารถยกเลิกหรือปรับปรุงความเชื่อมโยงกับ Wallet หรือ Credential เดิม และกำหนดความเชื่อมโยงกับ Wallet หรือ Credential ใหม่ให้สอดคล้องกัน

(2) การรับฝากและเก็บรักษาหลักทรัพย์โทเคน (Custodial Service) : ในกรณีที่ผู้ให้บริการให้บริการรับฝากหรือเก็บรักษาหลักทรัพย์โทเคน หรือควบคุม Credential, Private Key หรือกลไกที่ใช้ในการควบคุมหลักทรัพย์โทเคนแทนลูกค้า ผู้ให้บริการควรจัดให้มีระบบงานและกระบวนการที่เหมาะสม เพื่อคุ้มครองหลักทรัพย์โทเคนและสิทธิของลูกค้า และสามารถติดตามสถานะของหลักทรัพย์โทเคนได้ตลอดระยะเวลาที่อยู่ภายใต้การรับฝากหรือเก็บรักษา โดยควรคำนึงถึงอย่างน้อยในเรื่องดังต่อไปนี้

- **การรับฝาก การส่งคืน และการโอนหลักทรัพย์โทเคน :** ควรมีกระบวนการสำหรับการรับฝาก การส่งคืน และการโอนหลักทรัพย์โทเคนออกจากการรับฝากที่สามารถตรวจสอบได้ โดยก่อนรับฝากควรตรวจสอบหลักทรัพย์โทเคน จำนวน สถานะ และสิทธิที่เกี่ยวข้อง รวมถึงตรวจสอบว่าการรับฝากหรือการโอนเป็นไปตามคำสั่งและเงื่อนไขที่กำหนด ทั้งนี้ ควรสามารถระบุได้อย่างชัดเจนว่าหลักทรัพย์โทเคนใดอยู่ภายใต้การดูแลของผู้ให้บริการ และเมื่อมีการส่งคืนหรือโอนออก ควรสามารถยืนยันได้ว่าหลักทรัพย์โทเคนถูกส่งมอบให้แก่บุคคลหรือ Wallet ที่ถูกต้อง

- **การจัดทำบัญชีและการแยกทรัพย์สินของลูกค้า (Client Asset Segregation) :** ควรจัดทำและรักษาข้อมูลหลักทรัพย์โทเคนของลูกค้าให้ถูกต้อง ครบถ้วน และเป็นปัจจุบัน และสามารถระบุได้ว่าหลักทรัพย์โทเคนจำนวนใดเป็นของลูกค้ารายใด รวมทั้งควรมีการแยกทรัพย์สินของลูกค้าออกจากทรัพย์สินของผู้ให้บริการและของลูกค้ารายอื่นในลักษณะที่สามารถระบุและคุ้มครองสิทธิของลูกค้าได้ ทั้งนี้ รูปแบบการแยกทรัพย์สินอาจแตกต่างกันตามรูปแบบการให้บริการ แต่ไม่ควรทำให้เกิดความไม่ชัดเจนเกี่ยวกับสิทธิในหลักทรัพย์โทเคนของลูกค้า

- **การบริหารจัดการ Wallet และ Credential/Key และการควบคุมหลักทรัพย์โทเคน :** ควรมีกระบวนการบริหารจัดการ Wallet และ Credential หรือกลไกที่ใช้ควบคุมหลักทรัพย์โทเคนตลอดวงจรชีวิต ตั้งแต่การจัดให้มี การเก็บรักษา การใช้งาน การเปลี่ยนแปลง การสำรองและกู้คืน ตลอดจนการยกเลิกหรือเลิกใช้งาน โดยควรกำหนดให้เฉพาะบุคคลหรือกระบวนการที่ได้รับอนุญาตเท่านั้นที่สามารถควบคุมหรือดำเนินการกับหลักทรัพย์โทเคนของลูกค้า และควรมีมาตรการป้องกันการสูญหาย การเข้าถึงโดยไม่ได้รับอนุญาต หรือการนำหลักทรัพย์โทเคนของลูกค้าไปใช้โดยไม่ชอบ

- **การอนุมัติและการดำเนินการทำรายการ :** ควรมีกระบวนการตรวจสอบคำสั่งและการอนุมัติการทำรายการกับหลักทรัพย์โทเคนของลูกค้า เพื่อให้มั่นใจว่ารายการนั้นมาจากผู้มีสิทธิหรือผู้ที่ได้รับมอบอำนาจ และเป็นไปตามเงื่อนไขที่เกี่ยวข้อง เช่น จำนวนหลักทรัพย์ ผู้รับโอน และข้อจำกัดในการทำรายการ รวมทั้งควรมีการแบ่งแยกหน้าที่และอำนาจในการอนุมัติ การควบคุม Credential/Key และการดำเนินการโอนอย่างเหมาะสม เพื่อป้องกันไม่ให้บุคคลใดบุคคลหนึ่งสามารถดำเนินการกับทรัพย์สินของลูกค้าได้โดยลำพังโดยไม่มีการควบคุมที่เหมาะสม

- **การบันทึกข้อมูลและการรักษาความถูกต้องของหลักทรัพย์โทเคน :** ควรสามารถบันทึกและติดตามสถานะของหลักทรัพย์โทเคนที่อยู่ภายใต้การรับฝาก รวมถึงการเปลี่ยนแปลงการควบคุม การโอน การอายัดหรือข้อจำกัดต่าง ๆ ได้อย่างต่อเนื่อง โดยข้อมูลดังกล่าวควรมีความถูกต้องครบถ้วน และสามารถตรวจสอบย้อนหลังได้ และควรมีกลไกที่ช่วยรักษา **Singularity, Control และ Integrity** ของหลักทรัพย์โทเคน เพื่อป้องกันการเกิดหลักทรัพย์โทเคนซ้ำซ้อน การบันทึกสถานะไม่ตรงกับสภาพจริง หรือการทำรายการที่ขัดกับสิทธิของลูกค้า

- **การกระทบยอดและการตรวจสอบ (Reconciliation and Verification) :** ควรมีกระบวนการตรวจสอบและกระทบยอดข้อมูลระหว่างบัญชีหรือระบบบันทึกหลักทรัพย์ของลูกค้ากับข้อมูลใน Wallet, ระบบ DLT หรือระบบงานอื่นที่เกี่ยวข้องตามความเหมาะสม เพื่อให้สามารถตรวจพบความแตกต่างระหว่างข้อมูลได้อย่างทันท่วงที และสามารถตรวจสอบหาสาเหตุและดำเนินการแก้ไขได้ ทั้งนี้ ควรมีการตรวจสอบหลักทรัพย์และสถานะที่เกี่ยวข้องทั้งในช่วงรับฝากและระหว่างที่อยู่ภายใต้การดูแลตามระดับความเสี่ยงและลักษณะของบริการ

- **การควบคุมภายในและการแบ่งแยกหน้าที่ :** ควรจัดให้มีการแบ่งแยกหน้าที่และสิทธิในการเข้าถึงระบบที่เหมาะสมระหว่างผู้ที่ทำหน้าที่ดูแลทรัพย์สิน ผู้อนุมัติรายการ ผู้ควบคุม Credential/Key และผู้ตรวจสอบหรือกระทบยอดข้อมูล เพื่อให้มีการถ่วงดุลและลดความเสี่ยงจากการทุจริตหรือการดำเนินการโดยไม่ได้รับอนุญาต รวมทั้งควรมีการบันทึกหลักฐานการดำเนินการที่สามารถตรวจสอบย้อนหลังได้

ทั้งนี้ การรับฝากหรือเก็บรักษาหลักทรัพย์โทเคน หรือการที่ผู้ให้บริการเป็นผู้ควบคุม Wallet, Credential, Private Key หรือกลไกที่ใช้ในการควบคุมหลักทรัพย์โทเคนแทนลูกค้า ไม่ทำให้ผู้ให้บริการเป็นผู้ถือหรือผู้มีสิทธิในหลักทรัพย์โทเคนดังกล่าว เว้นแต่จะเป็นไปตามสิทธิหรือผลทางกฎหมายที่เกี่ยวข้อง โดยผู้ให้บริการควรสามารถแยกแยะและรักษาความแตกต่างระหว่างการควบคุมหลักทรัพย์โทเคนในทางเทคนิคกับสิทธิในหลักทรัพย์โทเคนของลูกค้าได้อย่างชัดเจน

5.4.3 งานด้านการชำระราคาและการส่งมอบหลักทรัพย์โทเคน

หลักการทั่วไป

ผู้ให้บริการที่ให้บริการด้านการชำระราคาและการส่งมอบหลักทรัพย์โทเคน ควรจัดให้มีกระบวนการและระบบงานที่เหมาะสมกับลักษณะ ขอบเขต และความซับซ้อนของบริการที่ตนรับผิดชอบ เพื่อให้การชำระราคาและการส่งมอบหลักทรัพย์โทเคนเป็นไปอย่างถูกต้อง ครบถ้วน และสามารถระบุผลและสถานะของการชำระราคาและการส่งมอบได้อย่างชัดเจน ทั้งนี้ ผู้ให้บริการอาจรับผิดชอบกระบวนการชำระราคาและการส่งมอบทั้งหมดหรือเพียงบางส่วน ตามรูปแบบการให้บริการและบทบาทหน้าที่ที่กำหนด

การให้บริการดังกล่าวอาจครอบคลุมการรับและประมวลผลรายการเพื่อการชำระราคา (Settlement Processing) การเชื่อมโยงการชำระราคาและการส่งมอบหลักทรัพย์โทเคนกับการชำระเงินหรือการส่งมอบสินทรัพย์อื่น (Exchange-of-Value Settlement) การกำหนดและติดตามสถานะและความเป็นที่สุดของการชำระราคา (Settlement Finality) ตลอดจนการบันทึก ตรวจสอบและกระทบยอดข้อมูลที่เกี่ยวข้อง (Settlement Record and Reconciliation) ทั้งนี้ ผู้ให้บริการควรจัดให้มีกลไกที่เหมาะสมกับลักษณะของธุรกรรมเพื่อป้องกันความเสี่ยงจากการที่คู่สัญญาฝ่ายหนึ่งปฏิบัติตามภาระผูกพันแล้ว แต่อีกฝ่ายหนึ่งยังไม่ได้ปฏิบัติตาม (Principal Risk) และเพื่อให้ผลของการชำระราคาและการส่งมอบสอดคล้องกับสิทธิและสถานะของหลักทรัพย์โทเคน

ในการดำเนินงาน ผู้ให้บริการควรสามารถกำหนดและระบุได้อย่างชัดเจนว่า เมื่อใดการชำระราคาและการส่งมอบถือว่าเสร็จสมบูรณ์และเป็นที่สุด (Final Settlement) รวมทั้งควรสามารถรักษาความเป็นหนึ่งเดียวของหลักทรัพย์โทเคน (Singularity) และความถูกต้องครบถ้วนของข้อมูล (Integrity) ตลอดกระบวนการชำระราคาและการส่งมอบ โดยระบบอาจใช้กลไกอัตโนมัติ เช่น Smart

Contract หรือกลไกการชำระราคาแบบ Atomic Settlement เพื่อดำเนินการตามเงื่อนไขที่กำหนด ทั้งนี้ ควรคำนึงถึงความสอดคล้องระหว่างผลการทำรายการบนระบบที่เกี่ยวข้อง และสามารถตรวจสอบย้อนหลังถึงรายการ สถานะ และผลของการชำระราคาและการส่งมอบได้

ข้อเสนอแนะ: ผู้ให้บริการควรจัดให้มีระบบงานและกระบวนการที่เหมาะสมกับขอบเขตหน้าที่และประเภทของบริการที่ตนให้บริการ โดยควรดำเนินการเฉพาะในส่วนที่เกี่ยวข้องกับบริการที่ตนรับผิดชอบ ดังต่อไปนี้

(1) การรับและประมวลผลรายการเพื่อการชำระราคาและส่งมอบ (Settlement Processing) : ผู้ให้บริการควรจัดให้มีกลไกหรือกระบวนการสำหรับรับ ตรวจสอบ และประมวลผลข้อมูลหรือคำสั่งที่เกี่ยวข้องกับการชำระราคาและการส่งมอบหลักทรัพย์โทเคน เพื่อให้สามารถดำเนินการชำระราคาและส่งมอบได้ตามเงื่อนไขที่กำหนด และสามารถระบุสถานะของรายการได้อย่างถูกต้อง โดยควรดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

- **การรับและตรวจสอบข้อมูลหรือคำสั่งเพื่อการชำระราคา :** ผู้ให้บริการควรจัดให้มีกลไกสำหรับรับและตรวจสอบข้อมูลหรือคำสั่งที่เกี่ยวข้องกับการชำระราคาและการส่งมอบ เช่น หลักทรัพย์โทเคน จำนวน ผู้ส่งมอบ ผู้รับมอบ สินทรัพย์หรือเงินที่ใช้ชำระราคา และวันที่หรือเวลาที่กำหนดให้ชำระราคา เพื่อให้มั่นใจว่าข้อมูลดังกล่าวมีความถูกต้อง ครบถ้วน และสอดคล้องกันก่อนนำรายการเข้าสู่กระบวนการชำระราคา ทั้งนี้ ควรสามารถตรวจสอบได้ว่าผู้สั่งหรือผู้ที่เกี่ยวข้องมีสิทธิหรือได้รับมอบอำนาจให้ดำเนินการดังกล่าว และรายการเป็นไปตามเงื่อนไขหรือข้อจำกัดที่เกี่ยวข้อง

- **การตรวจสอบความพร้อมและเงื่อนไขก่อนการชำระราคา :** ผู้ให้บริการควรมีกลไกสำหรับตรวจสอบว่าหลักทรัพย์โทเคนและสินทรัพย์ที่ใช้ในการชำระราคามีความพร้อมและสามารถนำมาชำระตามเงื่อนไขที่กำหนด เช่น มีจำนวนเพียงพอ อยู่ในสถานะที่สามารถโอนหรือส่งมอบได้ และไม่อยู่ภายใต้ข้อจำกัดที่ขัดกับการชำระราคา รวมทั้งควรสามารถตรวจสอบเงื่อนไขที่เกี่ยวข้องกับคู่สัญญาและรายการก่อนดำเนินการ เพื่อป้องกันการนำหลักทรัพย์โทเคนหรือสินทรัพย์เดียวกันไปใช้เพื่อการชำระภาระผูกพันซ้ำซ้อน

- **การประมวลผลและติดตามสถานะของรายการ :** ผู้ให้บริการควรมีกลไกสำหรับจัดลำดับและประมวลผลรายการตามเงื่อนไขและเวลาที่กำหนด และสามารถติดตามสถานะของรายการได้ตั้งแต่การรับคำสั่งจนถึงการชำระราคาและส่งมอบแล้วเสร็จ เช่น รายการที่อยู่ระหว่างรอการดำเนินการ (Pending) รายการที่อยู่ระหว่างการประมวลผล (Processing) รายการที่ชำระราคาและส่งมอบแล้ว (Settled) หรือรายการที่ไม่สามารถดำเนินการได้ (Failed) ทั้งนี้ ควรสามารถระบุสาเหตุหรือเงื่อนไขที่ทำให้รายการไม่สามารถดำเนินการได้ และดำเนินการกับรายการดังกล่าวตามหลักเกณฑ์และกระบวนการที่กำหนด

- **การควบคุมความสอดคล้องของรายการและป้องกันการดำเนินการซ้ำซ้อน :** ผู้ให้บริการควรมีกลไกที่ช่วยให้ข้อมูลของรายการที่นำเข้าสู่การชำระราคาและผลการดำเนินการมีความสอดคล้องกัน และสามารถป้องกันการนำรายการเดียวกันมาดำเนินการซ้ำหรือทำให้เกิดการส่งมอบหรือชำระภาระผูกพันซ้ำซ้อน ทั้งนี้ ในกรณีที่ใช้ระบบ DLT หรือ Smart Contract กลไกดังกล่าวอาจดำเนินการโดยอัตโนมัติตามเงื่อนไขที่กำหนดในระบบ

(2) การเชื่อมโยงการชำระราคาและการส่งมอบ (Exchange-of-Value Settlement) : ผู้ให้บริการควรจัดให้มีกลไกหรือกระบวนการสำหรับเชื่อมโยงการชำระราคาและการส่งมอบหลักทรัพย์โทเคนกับการชำระเงินหรือการส่งมอบสินทรัพย์อื่นที่เป็นภาระผูกพันของคู่สัญญา เพื่อให้การดำเนินการในแต่ละด้านเป็นไปตามเงื่อนไขที่กำหนด และลดความเสี่ยงจากการที่คู่สัญญาฝ่ายหนึ่งปฏิบัติตามภาระผูกพันแล้ว แต่อีกฝ่ายหนึ่งยังไม่ได้ปฏิบัติตาม โดยควรดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

- **การเชื่อมโยงภาระผูกพันที่เกี่ยวข้อง :** ผู้ให้บริการควรมีกลไกสำหรับระบุและเชื่อมโยงการส่งมอบหลักทรัพย์โทเคนกับการชำระเงิน เพื่อให้สามารถตรวจสอบได้ว่าภาระผูกพันที่เกี่ยวข้องกันเป็นรายการใด และเงื่อนไขใดที่ต้องดำเนินการให้สำเร็จก่อนหรือพร้อมกัน ทั้งนี้ กลไกดังกล่าวควรสามารถรองรับรูปแบบการชำระราคาที่เหมาะสมกับลักษณะของธุรกรรม เช่น Delivery versus Payment (DvP), Delivery versus Delivery (DvD) หรือ Payment versus Payment (PvP)[7]
- **การดำเนินการชำระราคาและส่งมอบที่เชื่อมโยงกัน :** ผู้ให้บริการควรจัดให้มีกลไกหรือกระบวนการที่ทำให้การส่งมอบหลักทรัพย์โทเคนและการชำระเงินหรือการส่งมอบสินทรัพย์ที่ใช้ในการชำระราคาที่เกี่ยวข้องกัน ดำเนินการตามเงื่อนไขที่กำหนดและมีความเชื่อมโยงกันอย่างเหมาะสม เพื่อป้องกันความเสี่ยงที่คู่สัญญาฝ่ายหนึ่งจะปฏิบัติตามภาระผูกพันของตนแล้ว แต่อีกฝ่ายหนึ่งยังไม่ได้ปฏิบัติตามภาระผูกพันที่เกี่ยวข้อง (Principal Risk) โดยควรกำหนดเงื่อนไขที่ชัดเจนว่าเมื่อใดการส่งมอบหลักทรัพย์โทเคนและการชำระเงินหรือการส่งมอบสินทรัพย์ที่ใช้ในการชำระราคา แต่ละด้านถือว่าเสร็จสมบูรณ์ และควรสามารถตรวจสอบสถานะของภาระผูกพันแต่ละด้านได้ ในกรณีที่การชำระราคาและการส่งมอบดำเนินการผ่านกลไกอัตโนมัติ ผู้ให้บริการควรจัดให้มีกลไกที่ทำให้การดำเนินการของภาระผูกพันทั้งสองด้านเป็นไปตามเงื่อนไขที่กำหนด และไม่ทำให้การส่งมอบหลักทรัพย์โทเคนหรือการชำระเงินหรือส่งมอบสินทรัพย์ที่ใช้ในการชำระราคาด้านใดด้านหนึ่งเสร็จสมบูรณ์โดยที่ภาระผูกพันอีกด้านหนึ่งยังไม่เป็นไปตามเงื่อนไขที่กำหนด ทั้งนี้ อาจใช้กลไกทางเทคโนโลยี

[7] **Delivery versus Delivery (DvD)** คือกลไกที่กำหนดให้การโอนหรือส่งมอบหลักทรัพย์โทเคนรายการหนึ่งเกิดขึ้นต่อเมื่อมีการโอนหรือส่งมอบหลักทรัพย์โทเคนอีกรายการหนึ่งที่เกี่ยวข้อง

Payment versus Payment (PvP) คือกลไกการชำระเงินที่กำหนดให้การชำระเงินรายการหนึ่งเกิดขึ้นก็ต่อเมื่อมีการชำระเงินอีกรายการหนึ่งที่เกี่ยวข้อง โดยทั่วไปใช้กับการแลกเปลี่ยนเงินต่างประเทศ

เช่น **Smart Contract, Atomic Settlement หรือ Atomic Swap** เพื่อสนับสนุนการดำเนินการดังกล่าว โดยกลไกที่ใช้ควรสามารถระบุได้อย่างชัดเจนว่ารายการชำระราคาและส่งมอบเสร็จสมบูรณ์หรือไม่สำเร็จ หรืออยู่ระหว่างดำเนินการ และสามารถบันทึกผลของรายการแต่ละด้านให้สอดคล้องกัน

- **การจัดการกรณีภาระผูกพันด้านใดด้านหนึ่งไม่สำเร็จ** : ผู้ให้บริการควรมีกระบวนการสำหรับจัดการกรณีที่การชำระเงิน การส่งมอบหลักทรัพย์โทเคน หรือการส่งมอบสินทรัพย์ที่ใช้ในการชำระราคา ไม่สามารถดำเนินการได้ตามเงื่อนไขที่กำหนด เพื่อไม่ให้เกิดการเปลี่ยนแปลงสิทธิหรือการควบคุมหลักทรัพย์โทเคนโดยไม่สอดคล้องกับผลของการชำระราคา รวมทั้งควรสามารถบันทึกและตรวจสอบได้ว่ารายการดังกล่าวไม่สำเร็จเนื่องจากเหตุใด และสถานะของภาระผูกพันแต่ละด้านภายหลังจากนั้นเป็นอย่างไร

(3) การจัดการสินทรัพย์ที่ใช้ในการชำระราคาและการเชื่อมโยงกับระบบที่เกี่ยวข้อง (Settlement Asset and Settlement Infrastructure) : ผู้ให้บริการควรจัดให้มีกลไกหรือกระบวนการสำหรับรองรับและเชื่อมโยงการชำระราคาในส่วนที่เกี่ยวข้องกับเงินหรือสินทรัพย์ที่ใช้ในการชำระราคา (Settlement Asset) เพื่อให้สามารถตรวจสอบสถานะของการชำระราคาและเชื่อมโยงกับการส่งมอบหลักทรัพย์โทเคนได้อย่างถูกต้อง โดยควรคำนึงถึงอย่างน้อยในเรื่องดังต่อไปนี้

- **การกำหนดและรองรับ Settlement Asset :** ผู้ให้บริการควรกำหนดหรือรองรับประเภทของเงินหรือสินทรัพย์ที่สามารถใช้ในการชำระราคาตามลักษณะของธุรกรรมและหลักเกณฑ์ที่เกี่ยวข้อง และควรสามารถระบุได้อย่างชัดเจนว่าสินทรัพย์ใดเป็นสินทรัพย์ที่ใช้ในการชำระราคาของรายการ รวมทั้งควรตรวจสอบว่าสินทรัพย์ดังกล่าวสามารถใช้ชำระราคาได้ตามเงื่อนไขที่กำหนด

- **การเชื่อมโยงกับระบบหรือผู้ให้บริการที่เกี่ยวข้อง :** ในกรณีที่การชำระราคาด้านเงินหรือสินทรัพย์ที่ใช้ในการชำระราคา ดำเนินการผ่านระบบหรือผู้ให้บริการอื่น ผู้ให้บริการควรมีกลไกสำหรับเชื่อมโยงและรับข้อมูลผลการชำระราคาจากระบบดังกล่าว เพื่อให้สามารถนำผลการชำระราคามาประกอบการดำเนินการส่งมอบหลักทรัพย์โทเคนได้อย่างถูกต้อง ทั้งนี้ ควรสามารถระบุได้ว่าผลการชำระราคาที่ได้รับนั้นเกี่ยวข้องกับรายการใด และมีสถานะอย่างไร

- **การพิจารณาความเสี่ยงของ Settlement Asset และผู้ให้บริการที่เกี่ยวข้อง :** ผู้ให้บริการควรประเมินความเหมาะสมและความเสี่ยงของ Settlement Asset และระบบหรือผู้ให้บริการที่เกี่ยวข้องกับการชำระราคา โดยคำนึงถึงความสามารถของ Settlement Asset ในการใช้ชำระราคาได้ตามจำนวน เวลา และเงื่อนไขที่กำหนด รวมทั้งความเสี่ยงที่อาจทำให้การชำระราคาไม่สามารถดำเนินการได้ตามกำหนด เช่น ความเสี่ยงด้านเครดิต (Credit Risk) ความเสี่ยงด้านสภาพคล่อง (Liquidity Risk) และความเสี่ยงด้านการดำเนินงาน (Operational Risk) ทั้งนี้ ผู้ให้บริการควรจัด

ให้มีกระบวนการรองรับกรณีที่ Settlement Asset หรือระบบหรือผู้ให้บริการที่เกี่ยวข้องไม่สามารถดำเนินการชำระราคาได้ตามกำหนด เพื่อให้สามารถระบุสถานะของรายการและดำเนินการตามแนวทางที่กำหนดได้ โดยไม่ทำให้ผลของการชำระราคาและการส่งมอบหลักทรัพย์โทเคนไม่สอดคล้องกัน

ตัวอย่าง : หากการชำระราคาหลักทรัพย์โทเคนสามารถใช้เงินฝากธนาคารพาณิชย์หรือ Tokenized Deposit เป็น Settlement Asset ผู้ให้บริการควรพิจารณาว่า Settlement Asset ดังกล่าวสามารถใช้ชำระราคาได้ครบถ้วนและภายในเวลาที่กำหนดหรือไม่ รวมทั้งพิจารณาความเสี่ยงกรณีธนาคารหรือผู้ให้บริการที่เกี่ยวข้องไม่สามารถให้บริการ ระบบขัดข้อง หรือไม่สามารถยืนยันผลการชำระเงินได้ตามกำหนด และควรมีกระบวนการรองรับเพื่อไม่ให้เกิดกรณีที่หลักทรัพย์โทเคนถูกส่งมอบหรือเปลี่ยนแปลงการควบคุมแล้ว แต่การชำระเงินยังไม่เสร็จสมบูรณ์

(4) การกำหนดและยืนยันความสมบูรณ์ของการชำระราคาและการส่งมอบ (Settlement Finality) : ผู้ให้บริการควรจัดให้มีกลไกหรือกระบวนการที่สามารถกำหนดและยืนยันได้อย่างชัดเจนว่าเมื่อใดการชำระราคาและการส่งมอบหลักทรัพย์โทเคนถือว่าเสร็จสมบูรณ์และเป็นที่สุด (Final Settlement) เพื่อให้ผู้ที่เกี่ยวข้องสามารถทราบสถานะและผลทางการทำรายการได้อย่างแน่นอน และควรดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

- **การกำหนดจุดที่การชำระราคาถือว่าเป็นที่สุด (Point of Finality) :** ผู้ให้บริการควรกำหนดหลักเกณฑ์และเงื่อนไขที่ชัดเจนสำหรับระบุว่าเมื่อใดการชำระราคาและการส่งมอบหลักทรัพย์โทเคนถือว่าเสร็จสมบูรณ์และเป็นที่สุด (Final Settlement) รวมทั้งควรกำหนดผลของการเป็นที่สุดดังกล่าว โดยเมื่อการชำระราคาถึงจุดที่กำหนดแล้ว ไม่ควรเปิดให้ผู้เข้าร่วมรายการสามารถเพิกถอนหรือยกเลิกรายการได้ฝ่ายเดียว เว้นแต่เป็นกรณีที่กฎหมาย หลักเกณฑ์ หรือเงื่อนไขของระบบกำหนดไว้ และควรสามารถระบุและตรวจสอบได้ว่ารายการใดได้ถึงจุดของความเป็นที่สุดแล้ว
- **การกำหนดเวลาและการดำเนินการให้เสร็จตามกำหนด (Settlement Timing) :** ผู้ให้บริการควรจัดให้การชำระราคาและการส่งมอบหลักทรัพย์ โทเคนสามารถดำเนินการให้เสร็จสิ้นภายในระยะเวลาที่กำหนด และไม่ช้ากว่าวันที่กำหนดชำระราคา (Value Date) ทั้งนี้ หากลักษณะของธุรกรรมและระบบเอื้ออำนวย ผู้ให้บริการควรพิจารณารองรับการชำระราคาแบบระหว่างวัน (Intraday) หรือแบบทันที (Real-time) ตามความเหมาะสม เพื่อลดระยะเวลาที่เกิดความเสี่ยงจากการชำระราคา
- **การแสดงและบันทึกผลของ Final Settlement :** ผู้ให้บริการควรสามารถแสดงและบันทึกผลของการชำระราคาและการส่งมอบได้อย่างชัดเจน รวมถึงสามารถระบุวันและเวลาที่รายการถือว่าเป็นที่สุด หลักทรัพย์โทเคนและสินทรัพย์ที่เกี่ยวข้อง และสถานะหรือผู้มีสิทธิหรือผู้มีอำนาจ

ควบคุมภายหลังการชำระราคาและการส่งมอบ เพื่อให้สามารถตรวจสอบและยืนยันผลของรายการย้อนหลังได้

(5) การบันทึก ตรวจสอบ และกระทบยอดผลการชำระราคาและการส่งมอบ (Settlement Record and Reconciliation) : ผู้ให้บริการควรจัดให้มีกลไกหรือกระบวนการสำหรับบันทึก ตรวจสอบ และกระทบยอดข้อมูลที่เกี่ยวข้องกับการชำระราคาและการส่งมอบหลักทรัพย์โทเคน เพื่อให้ข้อมูลเกี่ยวกับรายการ สถานะ และผลของการชำระราคาและการส่งมอบมีความถูกต้อง ครบถ้วน และสอดคล้องกันระหว่างระบบที่เกี่ยวข้อง และสามารถตรวจสอบย้อนหลังได้ โดยควรดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

- **การบันทึกข้อมูลและหลักฐานการชำระราคาและการส่งมอบ :** ผู้ให้บริการควรจัดให้มีการบันทึกข้อมูลและหลักฐานที่เกี่ยวข้องกับการชำระราคาและการส่งมอบอย่างเหมาะสม โดยอย่างน้อยควรสามารถระบุรายการหรือคำสั่งที่เกี่ยวข้อง หลักทรัพย์โทเคนและจำนวนหลักทรัพย์ ผู้ส่งมอบและผู้รับมอบ สินทรัพย์ที่ใช้ในการชำระราคา วันและเวลาที่เกี่ยวข้อง รวมถึงสถานะและผลของการชำระราคาและการส่งมอบ ทั้งนี้ ข้อมูลดังกล่าวควรสามารถเชื่อมโยงกันได้ตลอดกระบวนการ และสามารถตรวจสอบย้อนหลังได้ตามระยะเวลาที่กำหนดตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง
- **การรักษาความสอดคล้องของข้อมูลและสถานะของหลักทรัพย์โทเคน :** ผู้ให้บริการควรจัดให้มีกลไกสำหรับตรวจสอบว่าข้อมูลและสถานะของหลักทรัพย์โทเคนภายหลังการชำระราคาและการส่งมอบสอดคล้องกับผลของรายการ และไม่ก่อให้เกิดการสร้างหรือส่งมอบหลักทรัพย์โทเคนซ้ำซ้อน หรือทำให้เกิดความไม่สอดคล้องระหว่างสิทธิและการควบคุมหลักทรัพย์โทเคน ทั้งนี้ ควรมีกลไกสำหรับตรวจพบรายการหรือสถานะที่ผิดปกติหรือไม่สอดคล้องกันได้อย่างเหมาะสม
- **การตรวจสอบและกระทบยอดข้อมูล (Reconciliation) :** ผู้ให้บริการควรจัดให้มีกระบวนการกระทบยอดข้อมูลระหว่างระบบที่เกี่ยวข้องกับการชำระราคาและการส่งมอบ เช่น ระบบบันทึกสถานะของหลักทรัพย์โทเคน ระบบประมวลผลการชำระราคา และระบบหรือผู้ให้บริการที่เกี่ยวข้องกับสินทรัพย์ที่ใช้ในการชำระราคา เพื่อให้สามารถตรวจพบความแตกต่างของข้อมูลหรือสถานะระหว่างระบบได้ ทั้งนี้ ความถี่และวิธีการกระทบยอดควรกำหนดให้เหมาะสมกับลักษณะ ปริมาณ และความเสี่ยงของการให้บริการ และอาจใช้กระบวนการอัตโนมัติหรือระบบ DLT ในการสนับสนุนการกระทบยอดได้
- **การจัดการความคลาดเคลื่อนและข้อผิดพลาด :** เมื่อพบว่าข้อมูลหรือสถานะของรายการระหว่างระบบไม่สอดคล้องกัน ผู้ให้บริการควรมีกระบวนการสำหรับระบุสาเหตุ ตรวจสอบผลกระทบ และดำเนินการแก้ไขตามอำนาจหน้าที่และเงื่อนไขที่กำหนด โดยควรสามารถระบุได้ว่าความคลาดเคลื่อนเกี่ยวข้องกับรายการหรือเหตุการณ์ใด และควรจัดเก็บหลักฐานของการตรวจสอบ

และการแก้ไขเพื่อให้สามารถตรวจสอบย้อนหลังได้ ทั้งนี้ การแก้ไขข้อมูลไม่ควรทำให้เกิดการเปลี่ยนแปลงสิทธิหรือสถานะของหลักทรัพย์โทเคนโดยไม่สอดคล้องกับผลของรายการหรือสิทธิที่เกี่ยวข้อง

- **การเชื่อมโยงข้อมูลกับระบบทะเบียนหรือระบบงานที่เกี่ยวข้อง :** ในกรณีที่ระบบที่ใช้ดำเนินการชำระราคาและส่งมอบแยกจากระบบที่ใช้บันทึกหรือจัดทำทะเบียนหลักทรัพย์โทเคน ผู้ให้บริการควรจัดให้มีกลไกสำหรับเชื่อมโยงหรือแลกเปลี่ยนข้อมูลระหว่างระบบดังกล่าวเพื่อให้ผลของการชำระราคาและการส่งมอบสามารถนำไปปรับปรุงข้อมูลหรือสถานะของหลักทรัพย์โทเคนและข้อมูลที่เกี่ยวข้องได้อย่างถูกต้อง และควรสามารถตรวจสอบความสอดคล้องของข้อมูลระหว่างระบบได้ตามบทบาทและหน้าที่ของแต่ละฝ่าย

6. ความมั่นคงปลอดภัยทางไซเบอร์ ความเสี่ยงด้านเทคโนโลยี และความพร้อมในการดำเนินงาน (Cybersecurity, Technology Risk and Operational Resilience)

ผู้ออกหลักทรัพย์โทเคนและผู้ให้บริการที่เกี่ยวข้องควรจัดให้มีการกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยี ความมั่นคงปลอดภัยทางไซเบอร์ ความสามารถในการตรวจสอบย้อนหลัง และความพร้อมในการดำเนินงานที่เหมาะสมกับลักษณะ ขนาด ความซับซ้อน และระดับความเสี่ยงของการให้บริการ ทั้งนี้ เพื่อรักษาความมั่นคงปลอดภัย ความน่าเชื่อถือ ความถูกต้องครบถ้วน และความพร้อมใช้งานของระบบและข้อมูล รวมถึงสนับสนุนการคุ้มครองผู้ลงทุน ความสามารถในการพิสูจน์และตรวจสอบยืนยันบันทึกการถือครองและสิทธิในหลักทรัพย์โทเคน ความต่อเนื่องในการให้บริการ และความเชื่อมั่นต่อระบบตลาดทุน นอกจากนี้ ในการดำเนินการดังกล่าว ผู้ออกหลักทรัพย์โทเคนและผู้ให้บริการที่เกี่ยวข้องควรคำนึงถึงผลกระทบที่อาจเกิดขึ้นต่อผู้ลงทุน ผู้ใช้บริการ ระบบงานที่เกี่ยวข้อง ผู้มีส่วนได้เสีย และตลาดทุนโดยรวม ตลอดจนกำหนดมาตรการควบคุมที่เหมาะสมกับระดับความเสี่ยงของระบบและการให้บริการ

หมวดนี้ครอบคลุมมาตรการด้านความมั่นคงปลอดภัยทางไซเบอร์ ความเสี่ยงด้านเทคโนโลยี และความพร้อมในการดำเนินงานตลอดวงจรชีวิตของระบบและหลักทรัพย์โทเคน ตั้งแต่การออก การถือครอง การโอน การบันทึกข้อมูล การพิสูจน์ตัวตนและการควบคุมสิทธิการเข้าถึง การบริหารจัดการกุญแจเข้ารหัสและการดำเนินการที่มีสิทธิพิเศษ การเปลี่ยนแปลงระบบและ Smart Contract การบำรุงรักษา การติดตามและตรวจจับเหตุการณ์ การบริหารจัดการช่องโหว่ การทดสอบและประเมินความมั่นคงปลอดภัย การตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัย การรักษาความต่อเนื่องในการดำเนินงานและการกู้คืนระบบหรือการให้บริการเมื่อเกิดเหตุขัดข้องหรือเหตุการณ์ไม่พึงประสงค์

นอกจากนี้ ยังครอบคลุมองค์ประกอบทางเทคโนโลยีทั้งหมดที่เกี่ยวข้องกับการออกหรือการให้บริการเกี่ยวกับหลักทรัพย์โทเคน ทั้งองค์ประกอบบนระบบ DLT หรือ Blockchain และองค์ประกอบภายนอกระบบดังกล่าว ตัวอย่างเช่น Smart Contract, Validator Node, Consensus Mechanism และองค์ประกอบอื่นของโครงสร้างพื้นฐาน DLT รวมถึงระบบบริหารจัดการผู้ลงทุน ระบบพิสูจน์และยืนยันตัวตน ระบบรับคำสั่ง ระบบรับฝากและดูแลทรัพย์สิน ระบบฐานข้อมูล ระบบเชื่อมต่อผ่าน API ระบบเชื่อมโยงข้อมูลภายนอก (Oracle System[8]) ระบบเชื่อมโยงระหว่างเครือข่ายหรือระบบ (Bridge System[9]) ระบบติดตามและเฝ้าระวังเหตุการณ์ ระบบบริหารจัดการกุญแจ

[8] Oracle System คือ กลไกที่เชื่อมโยงบล็อกเชนกับข้อมูลหรือระบบภายนอก เพื่อให้สัญญาอัจฉริยะนำข้อมูลมาใช้หรือทำงานร่วมกับระบบภายนอกได้

[9] Bridge System คือ กลไกที่เชื่อมต่อบล็อกเชนต่างเครือข่าย เพื่อให้สามารถโอนสินทรัพย์หรือส่งข้อมูลระหว่างกันได้

เข้ารหัส ระบบที่ใช้ในการดำเนินการหรืออนุมัติการดำเนินการที่มีสิทธิพิเศษ และองค์ประกอบอื่นใดที่อาจส่งผลต่อความมั่นคงปลอดภัย ความถูกต้องครบถ้วน ความพร้อมใช้งาน หรือความน่าเชื่อถือของระบบและข้อมูลที่เกี่ยวข้องกับหลักทรัพย์โทเคน

ผู้ออกหลักทรัพย์โทเคนและผู้ให้บริการที่เกี่ยวข้องต้องสามารถแสดงให้เห็นได้ว่ามีมาตรการควบคุมที่เหมาะสมและเพียงพอในการรักษาความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานของระบบและข้อมูล รวมทั้งสามารถตรวจสอบย้อนหลังเหตุการณ์และการดำเนินการที่มีนัยสำคัญต่อระบบ ข้อมูล และหลักทรัพย์โทเคนได้อย่างเพียงพอและน่าเชื่อถือ ตลอดจนสามารถป้องกัน ตรวจจับ ตอบสนอง และฟื้นฟูการดำเนินงานจากเหตุการณ์ด้านความมั่นคงปลอดภัยหรือเหตุการณ์หยุดชะงักได้อย่างมีประสิทธิภาพ

6.1 การกำกับดูแลด้านความมั่นคงปลอดภัยและความเสี่ยงด้านเทคโนโลยี (Security and Technology Risk Governance)

การออกแบบ การพัฒนา การให้บริการ และการบริหารจัดการหลักทรัพย์โทเคนควรอยู่ภายใต้การกำกับดูแลด้านความมั่นคงปลอดภัยทางไซเบอร์และความเสี่ยงด้านเทคโนโลยีที่เหมาะสม โดยคำนึงถึงลักษณะของผลิตภัณฑ์ โครงสร้างทางเทคนิค รูปแบบการให้บริการ บทบาทของผู้เกี่ยวข้อง และระดับความเสี่ยงที่อาจเกิดขึ้นต่อผู้ลงทุน ตลาดทุน และระบบที่เกี่ยวข้อง

การกำกับดูแลตามหัวข้อนี้ครอบคลุมการกำหนดโครงสร้างการกำกับดูแลและการบริหารจัดการด้านความมั่นคงปลอดภัย บทบาทและความรับผิดชอบของผู้เกี่ยวข้อง นโยบายและมาตรฐานภายในการบริหารจัดการความเสี่ยง การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัย การบริหารจัดการการเปลี่ยนแปลงระบบ ตลอดจนการบริหารจัดการความเสี่ยงจากผู้ให้บริการภายนอกหรือระบบที่ต้องพึ่งพาบุคคลภายนอก เพื่อให้การดำเนินงานเกี่ยวกับหลักทรัพย์โทเคนมีความมั่นคงปลอดภัย สามารถตรวจสอบย้อนหลังได้ มีความต่อเนื่องในการให้บริการ และสามารถรองรับเหตุการณ์หรือการเปลี่ยนแปลงที่อาจส่งผลกระทบต่อระบบ ข้อมูล หรือสิทธิของผู้ถือหลักทรัพย์โทเคนได้อย่างเหมาะสม

การกำหนดมาตรการภายใต้หัวข้อนี้ควรยึดหลัก Risk-based และ Proportionate Approach โดยพิจารณาให้สอดคล้องกับระดับความสำคัญ ลักษณะ และระดับความเสี่ยงของระบบหรือบริการที่เกี่ยวข้อง รวมถึงผลกระทบที่อาจเกิดขึ้นต่อผู้ลงทุน ความถูกต้องครบถ้วนและความน่าเชื่อถือของข้อมูล สิทธิของผู้ถือหลักทรัพย์โทเคน ความต่อเนื่องในการให้บริการ และการปฏิบัติตามกฎหมายหรือข้อกำหนดด้านการกำกับดูแลที่เกี่ยวข้อง

6.1.1. การกำกับดูแลและการบริหารจัดการความมั่นคงปลอดภัย (Security Governance and Management)

หลักการทั่วไป

ผู้เกี่ยวข้องกับการออกแบบ การพัฒนา การให้บริการ หรือการบริหารจัดการหลักทรัพย์โทเคนควรกำหนดกรอบการกำกับดูแลและการบริหารจัดการด้านความมั่นคงปลอดภัยและความเสี่ยงด้านเทคโนโลยีที่ชัดเจน เพื่อกำหนดทิศทาง กำกับ ควบคุม ติดตาม และทบทวนมาตรการด้านความมั่นคงปลอดภัยให้มีความเหมาะสมและสอดคล้องกับระดับความเสี่ยงของระบบอย่างต่อเนื่อง

กรอบการกำกับดูแลดังกล่าวควรครอบคลุมระบบ องค์ประกอบ และกระบวนการที่มีนัยสำคัญต่อการดำเนินงานเกี่ยวกับหลักทรัพย์โทเคน ทั้งองค์ประกอบบนระบบ DLT หรือ Blockchain และองค์ประกอบภายนอกระบบดังกล่าว เช่น Smart Contract, ระบบบริหารจัดการตัวตนและสิทธิการเข้าถึง (Identity and Access Management), ระบบบริหารจัดการกุญแจเข้ารหัส (Key Management System), ระบบฐานข้อมูล, ระบบเชื่อมต่อผ่าน API, Oracle System, Bridge System หรือระบบงานสนับสนุนอื่นที่เกี่ยวข้อง

การบริหารจัดการด้านความมั่นคงปลอดภัยไม่ควรจำกัดอยู่เพียงมาตรการทางเทคนิค แต่ควรครอบคลุมการกำหนดบทบาทและความรับผิดชอบ การกำหนดนโยบายและมาตรฐานภายใน การประเมินและบริหารจัดการความเสี่ยง การติดตามและทบทวนประสิทธิผลของมาตรการควบคุม ตลอดจนการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยแก่บุคลากรและผู้เกี่ยวข้อง ทั้งนี้ เพื่อให้มาตรการควบคุมสามารถนำไปปฏิบัติได้อย่างมีประสิทธิผล มีผู้รับผิดชอบที่ชัดเจน และสามารถตรวจสอบย้อนหลังได้

ข้อเสนอแนะขั้นต่ำ

ผู้ออกหลักทรัพย์โทเคนและผู้ให้บริการที่เกี่ยวข้องควรดำเนินการอย่างน้อย ดังต่อไปนี้

(1) **การกำหนดกรอบการกำกับดูแล (Governance Framework)** : ควรจัดให้มีกรอบการกำกับดูแลด้านความมั่นคงปลอดภัยและความเสี่ยงด้านเทคโนโลยีที่เหมาะสมกับลักษณะของผลิตภัณฑ์ บริการ ระบบ และระดับความเสี่ยงที่เกี่ยวข้อง รวมทั้งกำหนดนโยบาย และแนวปฏิบัติด้านความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร ซึ่งครอบคลุมระบบ กระบวนการ และองค์ประกอบสำคัญที่เกี่ยวข้องกับหลักทรัพย์โทเคน นอกจากนี้ **ควรจัดให้มีการทบทวนกรอบการกำกับดูแล นโยบาย และแนวปฏิบัติด้านความมั่นคงปลอดภัยโดยคณะกรรมการบริษัทหรือคณะบุคคลที่ได้รับมอบหมาย อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ** เพื่อให้มั่นใจว่ากรอบการกำกับดูแล นโยบาย และ

แนวปฏิบัติดังกล่าวยังคงเหมาะสม สอดคล้องกับระดับความเสี่ยง และรองรับการเปลี่ยนแปลงของเทคโนโลยี ภัยคุกคาม และกฎหมายหรือข้อกำหนดที่เกี่ยวข้อง

(2) **การกำหนดบทบาทและความรับผิดชอบ (Roles and Responsibilities) :** ควรกำหนดบทบาทหน้าที่ และความรับผิดชอบของผู้เกี่ยวข้องอย่างชัดเจน โดยครอบคลุมอย่างน้อย ได้แก่ คณะกรรมการบริษัทและกลุ่มผู้บริหาร ผู้พัฒนาและผู้ดูแลระบบ ผู้รับผิดชอบงานด้านการบริหารจัดการความเสี่ยงและความมั่นคงปลอดภัยทางไซเบอร์ ผู้รับผิดชอบงานด้านการกำกับดูแลและการปฏิบัติตามกฎหมาย และผู้ให้บริการภายนอกที่มีบทบาทสำคัญต่อการให้บริการเกี่ยวกับหลักทรัพย์โทเคน ทั้งนี้ ควรจัดให้มีการแบ่งแยกหน้าที่ (Segregation of Duties) ที่เหมาะสมสำหรับการดำเนินงานที่มีความสำคัญหรือมีความเสี่ยงสูง เพื่อลดความเสี่ยงจากความผิดพลาด การใช้อำนาจโดยมิชอบ หรือความขัดแย้งทางผลประโยชน์

(3) **การบริหารจัดการความเสี่ยง (Risk Management) :** ควรจัดให้มีกระบวนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยและความเสี่ยงด้านเทคโนโลยีที่เหมาะสม โดยอย่างน้อยควรครอบคลุม

- **การระบุและจำแนก (Identify & Classify)** ระบบ ข้อมูล และองค์ประกอบสำคัญที่เกี่ยวข้องกับการให้บริการหลักทรัพย์โทเคน รวมถึงการจำแนกระดับความสำคัญตามความเสี่ยงและผลกระทบ
- **การประเมิน (Assess)** ความเสี่ยงด้านความมั่นคงปลอดภัยและความเสี่ยงด้านเทคโนโลยี ก่อนเริ่มให้บริการ เมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ และเป็นระยะตามความเหมาะสม
- **การจัดการ (Treat)** ความเสี่ยงที่พบจากการประเมิน โดยอาจดำเนินการในรูปแบบการลด การหลีกเลี่ยง การถ่ายโอน หรือการยอมรับความเสี่ยง ทั้งนี้ การยอมรับความเสี่ยงควรได้รับอนุมัติจากผู้มีอำนาจตามที่องค์กรกำหนด
- **การติดตามและทบทวน (Monitor and Review)** ความเสี่ยงและมาตรการควบคุมอย่างต่อเนื่อง พร้อมปรับปรุงมาตรการด้านความมั่นคงปลอดภัยให้สอดคล้องกับภัยคุกคาม ช่องโหว่ เทคโนโลยี และข้อกำหนดที่เปลี่ยนแปลง

(4) การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัย (Security Awareness and Training) : ควรจัดให้มีการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยแก่คณะกรรมการบริษัท กลุ่มผู้บริหาร บุคลากร และผู้เกี่ยวข้อง ให้เหมาะสมกับบทบาท หน้าที่ และระดับความรับผิดชอบ เพื่อให้มีความรู้ความเข้าใจ และความสามารถที่เพียงพอในการปฏิบัติงาน ตระหนักถึงความเสี่ยงด้านความมั่นคงปลอดภัยและความเสี่ยงด้านเทคโนโลยี รวมทั้งสามารถปฏิบัติตามนโยบาย แนวปฏิบัติ และมาตรการด้านความมั่นคงปลอดภัยขององค์กรได้อย่างถูกต้องและเหมาะสม

6.1.2 การบริหารจัดการการเปลี่ยนแปลงระบบ (Change Management)

หลักการทั่วไป

การเปลี่ยนแปลงระบบหรือองค์ประกอบที่เกี่ยวข้องกับหลักทรัพย์โทเคนอาจส่งผลกระทบต่อความมั่นคงปลอดภัย ความถูกต้องครบถ้วนและความน่าเชื่อถือของข้อมูล ความต่อเนื่องในการให้บริการ การทำงานของ Smart Contract สิทธิของผู้ถือหลักทรัพย์โทเคน หรือการปฏิบัติตามกฎหมายและข้อกำหนดด้านการกำกับดูแลที่เกี่ยวข้อง ดังนั้น การเปลี่ยนแปลงควรอยู่ภายใต้กระบวนการบริหารจัดการการเปลี่ยนแปลงที่เหมาะสมกับลักษณะและระดับความเสี่ยงของการเปลี่ยนแปลง โดยควรมีการประเมิน อนุมัติ ทดสอบ นำขึ้นใช้งาน ติดตามผล และจัดเก็บหลักฐานอย่างเหมาะสม

กระบวนการบริหารจัดการการเปลี่ยนแปลงควรครอบคลุมระบบและองค์ประกอบทางเทคโนโลยีที่เกี่ยวข้องกับหลักทรัพย์โทเคน ทั้งองค์ประกอบบนระบบ DLT เช่น Smart Contract และระบบโครงสร้างพื้นฐานของ DLT องค์ประกอบภายนอกระบบ DLT เช่น ระบบฐานข้อมูลและระบบบริหารจัดการกุญแจเข้ารหัส และองค์ประกอบที่ใช้เชื่อมโยงระหว่างระบบ เช่น API, Oracle และ Bridge รวมถึงการเปลี่ยนแปลงที่เกี่ยวข้องกับระบบหรือองค์ประกอบอื่นซึ่งอาจส่งผลกระทบต่อการทำงานของระบบ ความมั่นคงปลอดภัย ข้อมูล หรือสิทธิของผู้ถือหลักทรัพย์โทเคน

การบริหารจัดการการเปลี่ยนแปลงควรคำนึงถึงการประเมินและควบคุมความเสี่ยง การแบ่งแยกหน้าที่ การทดสอบก่อนนำไปใช้งานจริง การตรวจสอบความถูกต้องของการเปลี่ยนแปลง ความสามารถในการย้อนกลับ แก้ไข หรือจำกัดผลกระทบตามความเหมาะสม การสื่อสารต่อผู้เกี่ยวข้อง และการจัดเก็บหลักฐานเพื่อให้สามารถตรวจสอบย้อนหลังได้ โดยเฉพาะการเปลี่ยนแปลงที่อาจส่งผลกระทบต่อธุรกรรมที่ยังไม่สิ้นสุด (Transactions in progress) สถานะของโทเคน สิทธิของผู้ถือหลักทรัพย์โทเคน หรือความต่อเนื่องของบริการที่มีนัยสำคัญ

ข้อเสนอแนะขั้นต่ำ

ผู้ออกหลักทรัพย์โทเคนและผู้ให้บริการที่เกี่ยวข้องควรดำเนินการอย่างน้อย ดังต่อไปนี้

(1) การกำหนดกระบวนการบริหารจัดการการเปลี่ยนแปลง (Change Management Process) : ควรจัดให้มีกระบวนการบริหารจัดการการเปลี่ยนแปลงที่เป็นลายลักษณ์อักษร โดยกำหนดประเภทและระดับความสำคัญของการเปลี่ยนแปลง ผู้รับผิดชอบ ผู้มีอำนาจอนุมัติ และขั้นตอนที่เกี่ยวข้องกับการประเมิน การทดสอบ การนำขึ้นใช้งานจริง การติดตามผล และการจัดเก็บหลักฐาน ทั้งนี้ ควรกำหนดกระบวนการและระดับการควบคุมให้เหมาะสมกับลักษณะ ความสำคัญ และระดับความเสี่ยงของการเปลี่ยนแปลง รวมถึงแยกแนวทางการบริหารจัดการสำหรับการเปลี่ยนแปลงทั่วไป การเปลี่ยนแปลงที่มีนัยสำคัญ และการเปลี่ยนแปลงกรณีฉุกเฉินตามความเหมาะสม

(2) การประเมินผลกระทบ การอนุมัติ และการแบ่งแยกหน้าที่ (Impact Assessment, Approval and Segregation of Duties) : ก่อนดำเนินการเปลี่ยนแปลงที่มีนัยสำคัญ ควรประเมินผลกระทบและความเสี่ยงที่อาจเกิดขึ้นต่อความมั่นคงปลอดภัย ความถูกต้องครบถ้วนและความน่าเชื่อถือของข้อมูล ความต่อเนื่องของบริการ การปฏิบัติตามข้อกำหนด และสิทธิของผู้ถือหลักทรัพย์โทเคน รวมถึงพิจารณาผลกระทบต่อธุรกรรมหรือสถานะของโทเคนที่อยู่ระหว่างการดำเนินการตามความเหมาะสม ทั้งนี้ การเปลี่ยนแปลงที่มีนัยสำคัญควรได้รับการอนุมัติจากผู้มีอำนาจก่อนนำไปใช้งานจริง และควรแบ่งแยกหน้าที่ระหว่างผู้พัฒนา ผู้ทดสอบ ผู้อนุมัติ และผู้ดำเนินการนำขึ้นใช้งานตามความเหมาะสม

(3) การทดสอบและการนำการเปลี่ยนแปลงขึ้นใช้งาน (Testing and Deployment) : ควรทดสอบการเปลี่ยนแปลงในสภาพแวดล้อมที่เหมาะสมก่อนนำขึ้นใช้งานจริง โดยขอบเขตและวิธีการทดสอบควรสอดคล้องกับลักษณะ ความสำคัญ และระดับความเสี่ยงของการเปลี่ยนแปลง รวมถึงควรมีการบริหารจัดการการนำการเปลี่ยนแปลงขึ้นใช้งานอย่างเป็นระบบ โดยกำหนดแผนการนำขึ้นใช้งาน ผู้รับผิดชอบ และขั้นตอนการตรวจสอบก่อนและหลังการดำเนินการ ตลอดจนมีแนวทางในการยกเลิก ย้อนกลับ หรือจำกัดผลกระทบเมื่อเกิดปัญหา ทั้งนี้ สำหรับการเปลี่ยนแปลงที่เกี่ยวข้องกับ Smart Contract เช่น การปรับรุ่น การย้ายระบบ

หรือการเปลี่ยนแปลง Logic ควรมีกลไกควบคุมและการบันทึกหลักฐานที่สามารถตรวจสอบย้อนหลังได้

(4) การเปลี่ยนแปลงกรณีฉุกเฉิน การติดตามผล และการจัดเก็บหลักฐาน (Emergency Change, Post-implementation Review and Record Keeping) : ควรจัดให้มีกระบวนการรองรับการเปลี่ยนแปลงกรณีฉุกเฉิน เช่น กรณีเกิดช่องโหว่ด้านความมั่นคงปลอดภัย เหตุโจมตี หรือเหตุขัดข้องที่มีนัยสำคัญ เป็นต้น โดยต้องบันทึกเหตุผล รายละเอียด และการอนุมัติที่เกี่ยวข้อง และควรทบทวนการดำเนินการย้อนหลังภายในระยะเวลาที่เหมาะสม ทั้งนี้ ภายหลังการเปลี่ยนแปลงที่มีนัยสำคัญ ควรมีการติดตามและทบทวนผลการนำไปใช้งานจริง เพื่อประเมินผลกระทบ ปัญหาที่เกิดขึ้น และประเด็นที่ต้องปรับปรุง รวมทั้งจัดเก็บหลักฐานที่เกี่ยวข้องกับการเปลี่ยนแปลงให้ครบถ้วนและสามารถตรวจสอบย้อนหลังได้

6.1.3. การบริหารจัดการผู้ให้บริการภายนอก (Third-Party Risk Management)

หลักการทั่วไป

การออกแบบ พัฒนา ให้บริการ หรือบริหารจัดการหลักทรัพย์โทเคนอาจมีการพึ่งพาผู้ให้บริการภายนอกหรือโครงสร้างพื้นฐานของบุคคลภายนอก หรือผู้ให้บริการระบบอื่นที่เกี่ยวข้อง การพึ่งพาผู้ให้บริการดังกล่าวอาจก่อให้เกิดความเสี่ยงต่อความมั่นคงปลอดภัย ความต่อเนื่องในการให้บริการ ความถูกต้องของข้อมูล การคุ้มครองข้อมูล และการปฏิบัติตามข้อกำหนดด้านกฎหมายหรือการกำกับดูแล

ดังนั้น ผู้เกี่ยวข้องควรมีแนวทางบริหารจัดการความเสี่ยงจากผู้ให้บริการภายนอกตลอดวงจรชีวิตของการใช้บริการ ตั้งแต่การคัดเลือกและตรวจสอบก่อนใช้บริการ การกำหนดเงื่อนไขในสัญญา การติดตามผลการให้บริการ การจัดการเหตุการณ์ การเปลี่ยนแปลงหรือยุติการใช้บริการ ตลอดจนการประเมินความเสี่ยงจากการพึ่งพาผู้ให้บริการรายใดรายหนึ่งหรือบริการใดบริการหนึ่งมากเกินสมควร

การบริหารจัดการผู้ให้บริการภายนอกควรเป็นไปตามระดับความสำคัญของบริการและผลกระทบที่อาจเกิดขึ้น หากผู้ให้บริการไม่สามารถให้บริการได้ ถูกโจมตี มีข้อบกพร่องด้านความมั่นคงปลอดภัย หรือไม่สามารถปฏิบัติตามข้อกำหนดที่เกี่ยวข้อง โดยเฉพาะบริการที่มีผลต่อการออก โอน ถือครอง ตรวจสอบสิทธิ เก็บรักษากุญแจเข้ารหัส ตรวจสอบตัวตน บังคับใช้ compliance หรือรักษาความต่อเนื่องของระบบหลักทรัพย์โทเคน

ข้อเสนอแนะขั้นต่ำ

ผู้ออกหลักทรัพย์โทเคนและผู้ให้บริการที่เกี่ยวข้องควรดำเนินการอย่างน้อย ดังต่อไปนี้

(1) **การกำหนดกระบวนการบริหารจัดการผู้ให้บริการภายนอก (Third-Party Risk Management Process) :** ควรจัดให้มีกระบวนการบริหารจัดการผู้ให้บริการภายนอกที่เป็นลายลักษณ์อักษร โดยครอบคลุมการจำแนกประเภทและระดับความสำคัญของบริการ การคัดเลือกและประเมินผู้ให้บริการ การจัดทำสัญญาหรือข้อตกลง การติดตามผลการให้บริการ การจัดการเหตุการณ์ และการเปลี่ยนแปลงหรือยุติการใช้บริการ ทั้งนี้ ระดับของการควบคุมควรสอดคล้องกับความเสี่ยงและผลกระทบของบริการนั้น

(2) **การประเมินและคัดเลือกผู้ให้บริการ (Due Diligence and Selection) :** ก่อนใช้บริการจากผู้ให้บริการภายนอกที่มีนัยสำคัญ ควรประเมินความเหมาะสม ความพร้อม และความเสี่ยงของผู้ให้บริการอย่างเพียงพอ โดยพิจารณาอย่างน้อยด้านความมั่นคงปลอดภัย ความต่อเนื่องในการให้บริการ การคุ้มครองข้อมูล ความสามารถในการปฏิบัติตามกฎหมายหรือข้อกำหนดด้านการกำกับดูแล และการพึ่งพาผู้ให้บริการช่วงต่อ ทั้งนี้ ควรทบทวนผลการประเมินเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญหรือเมื่อมีเหตุอันควรให้ทบทวนความเหมาะสมและความเสี่ยงของผู้ให้บริการ

(3) **การกำหนดข้อตกลงและการติดตามการให้บริการ (Contractual Controls and Ongoing Monitoring) :** ควรกำหนดสัญญาหรือข้อตกลงกับผู้ให้บริการภายนอกให้ชัดเจนและเหมาะสมกับความสำคัญของบริการ โดยครอบคลุมขอบเขตและระดับการให้บริการ มาตรการด้านความมั่นคงปลอดภัยและการคุ้มครองข้อมูล การแจ้งเหตุการณ์หรือเหตุขัดข้องที่อาจส่งผลกระทบต่อระบบหรือผู้ถือหลักทรัพย์โทเคน สิทธิในการเข้าถึงข้อมูลหรือประเมินการควบคุม ตลอดจนเงื่อนไขเกี่ยวกับการเปลี่ยนแปลงและยุติบริการ ทั้งนี้ ควรติดตามผลการให้บริการ การปฏิบัติตามเงื่อนไขหรือระดับการให้บริการที่กำหนด เหตุการณ์ผิดปกติ และการเปลี่ยนแปลงที่อาจส่งผลกระทบต่อการให้บริการอย่างต่อเนื่องตามระดับความเสี่ยง

(4) **การบริหารความต่อเนื่อง การกระจุกตัว และการยุติบริการ (Continuity, Concentration and Exit Management) :** ควรประเมินและบริหารจัดการความเสี่ยงจากการพึ่งพาผู้ให้บริการรายใดรายหนึ่งหรือบริการสำคัญมากเกินสมควร โดยเฉพาะผู้ให้บริการที่มีบทบาทสำคัญต่อโครงสร้างพื้นฐานหรือการให้บริการเกี่ยวกับหลักทรัพย์โทเคน เช่น ผู้ให้บริการ Cloud, Custodian, Wallet หรือ Oracle รวมทั้งจัดให้มีแผนรองรับกรณีผู้ให้บริการไม่สามารถให้บริการได้หรือจำเป็นต้องยุติการใช้บริการ โดยอาจครอบคลุมการกู้คืนหรือย้ายบริการ การใช้ผู้ให้บริการทดแทน การถ่ายโอนข้อมูลและทรัพย์สินที่เกี่ยวข้อง และการตรวจสอบความครบถ้วนภายหลังการยุติบริการ ทั้งนี้ควรจัดเก็บหลักฐานเกี่ยวกับการประเมิน การอนุมัติ การติดตาม เหตุการณ์สำคัญ และการดำเนินการตามแผนให้สามารถตรวจสอบย้อนหลังได้

6.2 ความมั่นคงปลอดภัยของระบบ แอปพลิเคชัน และโครงสร้างพื้นฐาน DLT (System, Application and DLT Infrastructure Security)

ระบบ แอปพลิเคชัน และโครงสร้างพื้นฐานที่ใช้ในการออก ให้บริการ หรือบริหารจัดการหลักทรัพย์โทเคนต้องได้รับการออกแบบ พัฒนา ทดสอบ นำขึ้นใช้งาน และดูแลรักษาโดยคำนึงถึงความมั่นคงปลอดภัยอย่างเหมาะสม เนื่องจากข้อผิดพลาดของระบบ ช่องโหว่ หรือการตั้งค่าที่ไม่เหมาะสมอาจส่งผลต่อความถูกต้องของธุรกรรม สถานะของโทเคน สิทธิของผู้ถือหลักทรัพย์โทเคน ความต่อเนื่องในการให้บริการ และความน่าเชื่อถือของระบบโดยรวม

หัวข้อนี้ครอบคลุมระบบและองค์ประกอบที่เกี่ยวข้องกับหลักทรัพย์โทเคน ทั้งส่วนที่อยู่บน DLT และระบบสนับสนุนอื่นที่เกี่ยวข้อง เช่น API, Oracle, Bridge, ระบบรับฝากหรือดูแลสินทรัพย์ ระบบบริหารจัดการตัวตน ฐานข้อมูล และระบบงานสนับสนุนอื่น โดยแยกประเด็นความเสี่ยงเฉพาะของ Smart Contract หรือ Logic ที่ทำงานบน DLT ไว้เป็นหัวข้อเฉพาะ

การกำหนดมาตรการภายใต้หัวข้อนี้ยึดหลัก technology-neutral และ risk-based approach โดยไม่ผูกกับเทคโนโลยีหรือรูปแบบ DLT ใดเป็นการเฉพาะ แต่ต้องสามารถแสดงได้ว่าระบบหรือองค์ประกอบที่เลือกใช้มีมาตรการด้านความมั่นคงปลอดภัย การควบคุมการเปลี่ยนแปลง การตรวจสอบ และการรองรับเหตุขัดข้องที่เหมาะสมกับลักษณะของผลิตภัณฑ์ ระดับความเสี่ยง และผลกระทบที่อาจเกิดขึ้นต่อผู้ลงทุนหรือผู้เกี่ยวข้อง

6.2.1. การออกแบบและพัฒนาระบบอย่างมั่นคงปลอดภัย (Secure System Development)

หลักการทั่วไป

ระบบและองค์ประกอบที่เกี่ยวข้องกับหลักทรัพย์โทเคนควรได้รับการออกแบบและพัฒนาโดยคำนึงถึงความมั่นคงปลอดภัยตั้งแต่ระยะเริ่มต้น เพื่อลดความเสี่ยงจากข้อผิดพลาดของซอฟต์แวร์ การตั้งค่าระบบที่ไม่ปลอดภัย การใช้ส่วนประกอบภายนอกที่มีช่องโหว่ และความเสี่ยงจากการเชื่อมต่อกับระบบอื่น

หลักการตามหัวข้อนี้ครอบคลุมระบบสนับสนุนที่เกี่ยวข้องกับการทำงานของหลักทรัพย์โทเคน เช่น API, Oracle, Bridge, ระบบรับฝากหรือดูแลสินทรัพย์ ระบบบริหารจัดการตัวตน ฐานข้อมูล ระบบสำหรับผู้ดูแลระบบ และระบบงานสนับสนุนอื่น ทั้งนี้ ความเสี่ยงเฉพาะของ Smart Contract หรือ Logic ที่ทำงานบน DLT ให้พิจารณาเพิ่มเติมตามหัวข้อ 6.2.2

การพัฒนาระบบควรมีขั้นตอนที่ชัดเจนตั้งแต่การกำหนดความต้องการด้านความมั่นคงปลอดภัย การออกแบบ การพัฒนา การทดสอบ การนำขึ้นใช้งานจริง และการบำรุงรักษา เพื่อให้ระบบสามารถทำงานได้อย่างถูกต้องปลอดภัย และลดความเสี่ยงต่อผู้ถือหลักทรัพย์โทเคนหรือผู้เกี่ยวข้อง

ข้อเสนอแนะขั้นต่ำ

ผู้ออกหลักทรัพย์โทเคนและผู้ให้บริการที่เกี่ยวข้องควรดำเนินการอย่างน้อย ดังต่อไปนี้

(1) กระบวนการพัฒนาระบบอย่างมั่นคงปลอดภัย (Secure Development Lifecycle) : ควรจัดให้มีกระบวนการพัฒนาระบบที่เป็นลายลักษณ์อักษรและคำนึงถึงความมั่นคงปลอดภัยตลอดวงจรชีวิตของระบบ ตั้งแต่การพิจารณาข้อกำหนดด้านความมั่นคงปลอดภัย การออกแบบ การพัฒนา การทดสอบ การนำขึ้นใช้งาน การบำรุงรักษา จนถึงการยุติการใช้งาน โดยความต้องการด้านความมั่นคงปลอดภัยควรครอบคลุมข้อมูล ธุรกรรม สิทธิของผู้ใช้งาน การเชื่อมต่อกับระบบอื่น และข้อกำหนดด้านกฎหมายหรือการกำกับดูแลที่เกี่ยวข้อง ทั้งนี้ ควรใช้แนวทางการเขียนโปรแกรม การกำหนดค่า และการดูแลระบบที่เหมาะสมกับเทคโนโลยี สถาปัตยกรรม และระดับความเสี่ยงของระบบ

(2) การควบคุมสภาพแวดล้อมและสิทธิในการพัฒนา (Development Environment and Access Controls) : ควรจำกัดการเข้าถึง Source Code, Repository, เครื่องมือ และระบบที่ใช้ในการพัฒนา ทดสอบ และนำระบบขึ้นใช้งานเฉพาะผู้ที่มีหน้าที่เกี่ยวข้อง พร้อมจัดให้มีการแบ่งแยกสภาพแวดล้อมสำหรับการพัฒนา (Development Environment) การทดสอบ (Test Environment)

และการใช้งานจริง (Production Environment) ตามความเหมาะสม รวมทั้งควบคุมการนำข้อมูลจริงมาใช้ในสภาพแวดล้อมที่ไม่ใช่ระบบใช้งานจริง และป้องกันข้อมูลสำคัญ เช่น Private Key, Credential, API Key หรือ Password ไม่ให้ถูกจัดเก็บ เปิดเผย หรือใช้งานในลักษณะที่ไม่ปลอดภัย

(3) การบริหารจัดการส่วนประกอบและระบบที่เชื่อมต่อ (Component and Integration Security) : ควรประเมินและควบคุมความเสี่ยงด้านความมั่นคงปลอดภัยของส่วนประกอบที่นำมาใช้ในการพัฒนาระบบ เช่น Open-source Component, Software Development Kit (SDK), API และส่วนประกอบภายนอกอื่น รวมทั้งกำหนดมาตรการด้านความมั่นคงปลอดภัยสำหรับระบบหรือส่วนประกอบที่เชื่อมต่อหรือสนับสนุนการทำงานของหลักทรัพย์โทเคนให้เหมาะสมกับระดับความสำคัญและความเสี่ยง โดยควรมีการติดตามช่องโหว่ การปรับปรุงรุ่น (Version Update) และการยกเลิกใช้ส่วนประกอบที่ไม่ได้รับการสนับสนุนหรือมีความเสี่ยงด้านความมั่นคงปลอดภัยตามความเหมาะสม

(4) การทดสอบและการจัดทำเอกสาร (Security Testing and Documentation) : ควรจัดให้มีการทดสอบด้านความมั่นคงปลอดภัยก่อนนำระบบขึ้นใช้งานจริง และเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ โดยขอบเขตและระดับของการทดสอบควรสอดคล้องกับความสำคัญและระดับความเสี่ยงของระบบ รวมทั้งควรจัดทำและเก็บรักษาเอกสารที่จำเป็นเกี่ยวกับการออกแบบ การพัฒนา การตั้งค่า การทดสอบ การนำขึ้นใช้งาน และการบำรุงรักษาระบบ เพื่อให้สามารถตรวจสอบย้อนหลัง ถ่ายทอดความรู้และดูแลระบบได้อย่างต่อเนื่อง

6.2.2 ความมั่นคงปลอดภัยและการควบคุมการเปลี่ยนแปลงของสมาร์ตคอนแทรกต์ (Smart Contract Security and Change Management)

หลักการทั่วไป

Smart Contract หรือ Logic ที่ทำงานบน DLT อาจมีบทบาทสำคัญต่อการทำงานของหลักทรัพย์โทเคน โดยอาจกำหนดหรือควบคุมการออก การถือครอง การโอน การจำกัดหรือระงับสิทธิ การบังคับใช้เงื่อนไข และการดำเนินการอื่นที่เกี่ยวข้องกับหลักทรัพย์โทเคน ดังนั้น Smart Contract หรือ Logic ดังกล่าวควรได้รับการออกแบบ พัฒนา ทดสอบ และนำขึ้นใช้งานโดยคำนึงถึงความมั่นคงปลอดภัย

ความถูกต้องของ Logic และผลกระทบที่อาจเกิดขึ้นต่อสิทธิของผู้ถือหลักทรัพย์โทเคนและการทำงานของระบบ

ความเสี่ยงที่ควรพิจารณา ได้แก่ ความเสี่ยงจาก Logic ที่ไม่สอดคล้องกับเงื่อนไขของผลิตภัณฑ์หรือข้อกำหนดที่เกี่ยวข้อง ช่องโหว่ของ Smart Contract การตั้งค่าที่ไม่เหมาะสม การเปลี่ยนแปลงหรือการอัปเกรด Smart Contract ตลอดจนการใช้ฟังก์ชันที่มีสิทธิหรืออำนาจสูง เช่น การหยุดการทำงานชั่วคราว การบังคับโอน การระงับหรือจำกัดการโอน หรือการเปลี่ยนแปลงค่าที่มีนัยสำคัญต่อการทำงานของระบบ

การควบคุม Smart Contract จึงควรครอบคลุมตลอดวงจรชีวิต ตั้งแต่การออกแบบและพัฒนา การตรวจสอบและทดสอบ การควบคุม Version และการนำขึ้นใช้งาน ไปจนถึงการเปลี่ยนแปลงหรือการอัปเกรดภายหลังการนำขึ้นใช้งาน โดยควรมีกระบวนการอนุมัติและควบคุมการเปลี่ยนแปลงที่เหมาะสม รวมถึงมีแนวทางรองรับกรณีเกิดข้อผิดพลาดหรือเหตุการณ์ที่อาจกระทบต่อการทำงานของ Smart Contract และจัดเก็บหลักฐานที่เกี่ยวข้องให้สามารถตรวจสอบย้อนหลังได้

หลักการตามหัวข้อนี้ให้ใช้โดยอนุโลมกับระบบหรือกลไกทางเทคโนโลยีอื่นที่ไม่ได้ใช้ Smart Contract แต่มี Logic อัตโนมัติซึ่งอาจส่งผลต่อสิทธิ สถานะ หรือธุรกรรมของหลักทรัพย์โทเคนในลักษณะเดียวกัน

ข้อเสนอแนะขั้นต่ำ

ผู้ออกหลักทรัพย์โทเคนและผู้ให้บริการที่เกี่ยวข้องควรดำเนินการอย่างน้อย ดังต่อไปนี้

(1) การออกแบบและกำหนดการทำงานของสมาร์ตคอนแทรกต์ (Smart Contract Design and Specification) : ควรกำหนดขอบเขต หน้าที่ รูปแบบการทำงาน ข้อจำกัด และเงื่อนไขของ Smart Contract ให้ชัดเจนก่อนการพัฒนา โดย Logic ที่เกี่ยวข้องกับการออก การโอน การจำกัดหรือระงับสิทธิ และเหตุการณ์ตามวงจรชีวิตของหลักทรัพย์โทเคนควรสอดคล้องกับข้อกำหนดของผลิตภัณฑ์ หลักเกณฑ์ และเงื่อนไขที่เปิดเผยต่อผู้ลงทุน รวมทั้งควรพิจารณาความเสี่ยงและช่องโหว่ที่อาจเกิดขึ้นจากเทคโนโลยี สถาปัตยกรรม และรูปแบบการใช้งาน และกำหนดมาตรการควบคุมที่เหมาะสม

ในกรณีที่ Smart Contract รองรับการทำงานข้ามเครือข่าย (Cross-chain) ควรกำหนดและควบคุมเงื่อนไขในการส่ง รับ และยืนยันข้อมูลหรือธุรกรรมระหว่างเครือข่ายให้ชัดเจน โดยคำนึงถึงความถูกต้องและความสอดคล้องของสถานะธุรกรรมระหว่างเครือข่าย รวมถึงความเสี่ยงจากการส่งข้อมูลหรือธุรกรรมซ้ำ การส่งข้อมูลไม่ครบถ้วน หรือความไม่สอดคล้องระหว่างเครือข่าย

(2) การควบคุมสิทธิและการตั้งค่าที่เกี่ยวข้อง (Access and Configuration Controls) : ควรจำกัดสิทธิในการเข้าถึงและดำเนินการกับ Smart Contract เฉพาะผู้ที่ได้รับมอบหมาย โดยเฉพาะการดำเนินการที่สามารถเปลี่ยนแปลงการทำงานหรือสถานะของ Smart Contract เช่น การ Mint/Burn การ Pause/Unpause การ Freeze/Unfreeze การบังคับโอน (Force Transfer) การเปลี่ยนแปลงผู้มีสิทธิหรือบทบาทในการควบคุม (Role หรือ Admin) หรือการอัปเกรด Smart Contract เป็นต้น และควรจัดให้มีกลไกการอนุมัติและการแบ่งแยกหน้าที่ตามระดับความเสี่ยง ทั้งนี้ การควบคุมสิทธิพิเศษและการดำเนินการที่มีสิทธิพิเศษให้เป็นไปตามหลักเกณฑ์ในข้อ 6.3 และ 6.4

นอกจากนี้ ควรควบคุมค่าพารามิเตอร์ ข้อมูลอ้างอิง และข้อมูลที่นำเข้าจาก Oracle หรือระบบภายนอกที่มีผลต่อการทำงานของ Smart Contract ให้มีความถูกต้องน่าเชื่อถือ เป็นปัจจุบัน และสามารถตรวจสอบแหล่งที่มาและการเปลี่ยนแปลงได้ รวมทั้งควรมีมาตรการรองรับกรณีข้อมูลดังกล่าวไม่ถูกต้อง ไม่สอดคล้อง หรือไม่สามารถใช้งานได้ตามปกติ

(3) การตรวจสอบ การทดสอบ และการนำขึ้นใช้งาน (Review, Testing and Deployment) : ควรจัดให้มีการตรวจสอบและทดสอบ Smart Contract ก่อนนำขึ้นใช้งานจริง โดยครอบคลุมความถูกต้องของ Logic การทำงานของฟังก์ชันที่มีนัยสำคัญ และการควบคุมสิทธิหรือข้อจำกัดในการทำธุรกรรม เช่น การตรวจสอบ Source Code การทดสอบการทำงานตามเงื่อนไขและกรณีต่าง ๆ และการทดสอบการเรียกใช้ฟังก์ชันที่มีสิทธิพิเศษ ทั้งนี้ ควรมีกระบวนการควบคุมการนำ Smart Contract ขึ้นใช้งาน รวมถึงการเปลี่ยนแปลง การอัปเกรด หรือการย้าย Smart Contract (Migration) ภายหลังการนำขึ้นใช้งาน โดยมีการประเมินความเสี่ยง

การอนุมัติ การทดสอบ และการควบคุมการนำขึ้นใช้งานที่เหมาะสมกับระดับความเสี่ยง ตลอดจนจัดเก็บหลักฐานที่เกี่ยวข้องให้สามารถตรวจสอบย้อนหลังได้ นอกจากนี้ ควรจัดให้มีการควบคุมและจัดเก็บข้อมูลสำคัญของ Smart Contract ที่นำขึ้นใช้งานจริง เช่น Version แหล่งที่มาของ Source Code วันที่นำขึ้นใช้งาน ผู้ดำเนินการ และ Contract Address หรือข้อมูลอ้างอิงอื่นที่เกี่ยวข้อง เพื่อให้สามารถตรวจสอบและยืนยัน Smart Contract ที่ใช้งานอยู่ได้ ทั้งนี้ การตรวจสอบและทดสอบด้านความมั่นคงปลอดภัยให้เป็นไปตามหลักเกณฑ์ในข้อ 6.7

(4) การติดตาม การรองรับเหตุผิดปกติ และการตรวจสอบย้อนหลัง (Monitoring, Incident Response and Auditability) : ควรจัดให้มีการติดตามและตรวจจับการทำงานของ Smart Contract และการดำเนินการที่มีสิทธิพิเศษอย่างเหมาะสม เพื่อให้สามารถตรวจพบความผิดปกติหรือการดำเนินการที่ไม่ได้รับอนุญาตได้อย่างทันท่วงที เช่น การเปลี่ยนแปลงสถานะของ Smart Contract การเรียกใช้ฟังก์ชันที่มีสิทธิพิเศษ หรือการเปลี่ยนแปลงค่าพารามิเตอร์ที่มีนัยสำคัญ รวมทั้งควรจัดให้มีแนวทางรองรับกรณีเกิดข้อผิดพลาด ช่องโหว่ หรือเหตุการณ์ที่อาจส่งผลกระทบต่อการทำงานหรือสถานะของ Smart Contract เช่น การระงับการทำงาน การจำกัดผลกระทบ การกู้คืน การอัปเกรด หรือการย้าย Smart Contract (Migration) ตามความเหมาะสม และควรจัดให้มีการบันทึกข้อมูลและหลักฐานที่เกี่ยวข้องกับการดำเนินการดังกล่าวอย่างเพียงพอและสามารถตรวจสอบย้อนหลังได้ ทั้งนี้ การติดตาม การบันทึกข้อมูล การตอบสนองต่อเหตุการณ์ และการจัดการเหตุการณ์ที่เกี่ยวข้องกับ Smart Contract ให้เป็นไปตามหลักเกณฑ์ในข้อ 6.6 และ 6.8

6.2.3 ความมั่นคงปลอดภัยของโครงสร้างพื้นฐาน DLT (DLT Infrastructure Security)

หลักการทั่วไป

โครงสร้างพื้นฐาน DLT และองค์ประกอบที่เกี่ยวข้องควรได้รับการออกแบบ จัดให้มีมาตรการป้องกัน ดูแล และบริหารจัดการอย่างเหมาะสม เพื่อให้ระบบที่ใช้รองรับหลักทรัพย์โทเคนมีความมั่นคงปลอดภัย สามารถรักษาความถูกต้องของธุรกรรม มีความพร้อมใช้งาน และสามารถดำเนินงานได้อย่างต่อเนื่อง

หลักการตามหัวข้อนี้ให้ยึดแนวทาง Technology-neutral และ Principle-based โดยไม่กำหนดหรือผูกกับสถาปัตยกรรมหรือรูปแบบ DLT ประเภทใดประเภทหนึ่งเป็นการเฉพาะ ทั้งนี้

ผู้เกี่ยวข้องควรพิจารณาองค์ประกอบของโครงสร้างพื้นฐานที่มีบทบาทสำคัญต่อการทำงานของระบบ โดยคำนึงถึงองค์ประกอบที่เกี่ยวข้องกับการเข้าร่วมเครือข่าย การเชื่อมต่อ การยืนยัน การจัดลำดับ การบันทึก การตรวจสอบ และการเผยแพร่ธุรกรรม รวมถึง Node, Endpoint, API, Network Connection, Permissioning Mechanism และระบบสนับสนุนอื่นที่เกี่ยวข้อง

การบริหารจัดการความมั่นคงปลอดภัยของโครงสร้างพื้นฐาน DLT ควรครอบคลุมการระบุและประเมินองค์ประกอบที่เกี่ยวข้อง การตั้งค่าระบบอย่างมั่นคงปลอดภัย การควบคุมสิทธิการเข้าถึง การรักษาความมั่นคงปลอดภัยของเครือข่าย การติดตามและตรวจสอบสถานะการทำงาน การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับ DLT ตลอดจนการเตรียมความพร้อมเพื่อรองรับกรณีเกิดเหตุขัดข้องหรือเหตุการณ์ที่อาจส่งผลกระทบต่อสถานะของหลักทรัพย์โทเคนหรือธุรกรรมที่เกี่ยวข้อง

ข้อเสนอแนะขั้นต่ำ

ผู้ออกหลักทรัพย์โทเคนและผู้ให้บริการที่เกี่ยวข้องควรดำเนินการอย่างน้อย ดังต่อไปนี้

(1) การบริหารจัดการองค์ประกอบ การตั้งค่า และสิทธิการเข้าถึง (Infrastructure, Configuration and Access Management) : ควรระบุองค์ประกอบของโครงสร้างพื้นฐาน DLT และระบบสนับสนุนที่เกี่ยวข้องให้ชัดเจน เช่น Node, Endpoint, API ระบบที่ใช้ในการยืนยันหรือบันทึกธุรกรรม และระบบสนับสนุนอื่นที่มีความสำคัญต่อการให้บริการ รวมทั้งกำหนดมาตรการในการตั้งค่าและดูแลรักษาระบบอย่างมั่นคงปลอดภัย เช่น การปิดหรือจำกัดการใช้งาน Service และการเชื่อมต่อที่ไม่จำเป็น การปรับปรุง Software หรือ Version ที่เกี่ยวข้อง และการทบทวนการตั้งค่าเมื่อมีการเปลี่ยนแปลงหรือพบความเสี่ยงด้านความมั่นคงปลอดภัยให้เหมาะสมกับระดับความสำคัญและความเสี่ยง

นอกจากนี้ ควรประเมินและบริหารจัดการความเสี่ยงที่เกี่ยวข้องกับผู้เข้าร่วมเครือข่ายหรือผู้ทำหน้าที่ตรวจสอบและยืนยันธุรกรรม (Validator/Node Operator) และกลไกการบรรลุฉันทามติ (Consensus Mechanism) ให้สอดคล้องกับรูปแบบและลักษณะของ DLT ที่ใช้ โดยพิจารณาถึงรูปแบบและเงื่อนไขในการเข้าร่วมเครือข่าย (Network Participation/Permissioning) บทบาทในการตรวจสอบและยืนยันธุรกรรม (Transaction/Block Validation) การมีส่วนร่วมในกลไกการบรรลุฉันทามติ (Consensus Participation) และความเสี่ยงจากการกระจุกตัวของผู้เข้าร่วม (Validator Concentration) ตามความเหมาะสม

(2) ความมั่นคงปลอดภัยของเครือข่ายและความพร้อมใช้งาน (Network Security and Resilience) : ควรจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของเครือข่าย การเชื่อมต่อ การสื่อสาร และรับส่งข้อมูล (Traffic) ที่เกี่ยวข้องกับโครงสร้างพื้นฐาน DLT เช่น การจำกัดการเชื่อมต่อระหว่างองค์ประกอบของระบบเฉพาะที่จำเป็น การควบคุมช่องทางและปลายทางที่สามารถเชื่อมต่อกับ Node หรือระบบสำคัญ และการป้องกันการเข้าถึงหรือการรับส่งข้อมูลที่ไม่ได้รับอนุญาต รวมทั้งออกแบบระบบให้รองรับความพร้อมใช้งาน ความต่อเนื่อง และปริมาณการใช้งานตามความเหมาะสม โดยเฉพาะองค์ประกอบที่มีนัยสำคัญต่อการให้บริการ รวมถึงควรมีมาตรการหรือกลไกรองรับกรณีที่ระบบหรือองค์ประกอบดังกล่าวไม่สามารถให้บริการได้ตามปกติ เช่น การสำรองระบบหรือองค์ประกอบที่สำคัญ การกู้คืน การสลับไปใช้ระบบหรือองค์ประกอบสำรอง หรือการย้ายบริการไปยังระบบหรือผู้ให้บริการทดแทน เพื่อจำกัดผลกระทบต่อการให้บริการและธุรกรรมที่เกี่ยวข้อง

(3) การติดตามและบริหารจัดการเหตุการณ์ของ DLT (DLT Monitoring and Event Management) : ควรติดตามสถานะและประสิทธิภาพของโครงสร้างพื้นฐาน DLT อย่างเหมาะสม เช่น ความพร้อมใช้งาน ความล่าช้า สถานะการประมวลผลและความสมบูรณ์ของธุรกรรม รวมถึงเหตุผิดปกติที่อาจกระทบต่อการให้บริการ เช่น ความผิดปกติของการทำงานของ Node การเชื่อมต่อเครือข่ายขัดข้อง หรือความผิดปกติที่เกี่ยวข้องกับการยืนยันธุรกรรมและบรรลุฉันทามติ (Consensus Mechanism) ที่อาจกระทบต่อการยืนยัน การจัดลำดับ หรือความสิ้นสุดของธุรกรรม (Transaction Finality) รวมถึงควรติดตามความผิดปกติของข้อมูลที่นำเข้าจาก Oracle หรือระบบภายนอกที่มีผลต่อการทำงานของ DLT หรือ Smart Contract เช่น ข้อมูลไม่ถูกต้อง ไม่สอดคล้อง หรือไม่เป็นปัจจุบัน และในกรณีระบบรองรับการทำงานข้ามเครือข่าย (Cross-chain) ควรติดตามความผิดปกติ เช่น ความไม่สอดคล้องของสถานะธุรกรรมระหว่างเครือข่าย ธุรกรรมที่ดำเนินการไม่ครบถ้วน หรือธุรกรรมที่ไม่สามารถดำเนินการต่อได้ตามเงื่อนไขที่กำหนด

นอกจากนี้ ควรกำหนดแนวทางบริหารจัดการเหตุการณ์เฉพาะของ DLT และความขัดข้องของระบบที่พึงพา เช่น กรณีเครือข่ายหนาแน่น การเกิด Hard Fork หรือเหตุการณ์ที่ทำให้การประมวลผลหรือการยืนยันธุรกรรมของเครือข่ายไม่เป็นไป

ตามปกติ หรือความขัดข้องของ Endpoint, Oracle, Bridge หรือระบบที่พึ่งพาภายนอก เพื่อให้สามารถตรวจพบ ประเมินผลกระทบ และตอบสนองต่อเหตุการณ์ได้อย่างเหมาะสม รวมทั้งสามารถดำเนินการตามแผนรองรับเหตุหยุดชะงักและการกู้คืนระบบตามความเหมาะสม ทั้งนี้ การติดตาม การบันทึกข้อมูล การตอบสนองต่อเหตุการณ์ และการกู้คืนระบบ ให้เป็นไปตามหลักเกณฑ์ในข้อ 6.6 และ 6.8

ทั้งนี้ ควรจัดเก็บข้อมูลและหลักฐานที่เกี่ยวข้องกับสถาปัตยกรรม การตั้งค่า เวอร์ชัน สิทธิการเข้าถึง การเปลี่ยนแปลง สถานะการทำงาน และเหตุการณ์สำคัญของโครงสร้างพื้นฐาน DLT ให้ครบถ้วนและสามารถตรวจสอบย้อนหลังได้

6.3 การพิสูจน์ตัวตนและการควบคุมสิทธิการเข้าถึง (Identity and Access Control)

ระบบที่เกี่ยวข้องกับหลักทรัพย์โทเคนควรมีกลไกในการ **ระบุตัวตน พิสูจน์ตัวตน และควบคุมสิทธิการเข้าถึง** อย่างเหมาะสม เพื่อให้มั่นใจได้ว่าเฉพาะผู้ที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงระบบข้อมูล หรือฟังก์ชันที่เกี่ยวข้องได้ตามสิทธิและบทบาทหน้าที่ที่กำหนด

หัวข้อนี้ครอบคลุมการบริหารจัดการตัวตนและสิทธิการเข้าถึงของบุคลากร ผู้ดูแลระบบ ผู้พัฒนาระบบ ผู้ให้บริการภายนอก บัญชีระบบ และผู้เกี่ยวข้องอื่นที่สามารถเข้าถึงระบบทั้ง On-chain และ Off-chain รวมถึงระบบสนับสนุนที่เกี่ยวข้องกับการออก การถือครอง การโอน หรือการบริหารจัดการหลักทรัพย์โทเคน ทั้งนี้ การควบคุมสิทธิการเข้าถึงควรยึดหลัก **Least Privilege และ Need-to-Know** โดยกำหนดสิทธิตามหน้าที่และความจำเป็นในการปฏิบัติงาน และมีการแบ่งแยกหน้าที่ที่เหมาะสมกับลักษณะและระดับความเสี่ยงของการดำเนินงาน

6.3.1. การบริหารจัดการตัวตนและสิทธิการเข้าถึง (Identity and Access Management)

หลักการทั่วไป

ระบบที่เกี่ยวข้องกับหลักทรัพย์โทเคนควรมีกระบวนการบริหารจัดการตัวตนและสิทธิการเข้าถึงที่ชัดเจน ครอบคลุมทั้งผู้ใช้งานภายใน ผู้ดูแลระบบ ผู้พัฒนาระบบ ผู้ให้บริการภายนอก บัญชีระบบ และระบบเชื่อมต่ออื่นที่เกี่ยวข้อง เพื่อให้การกำหนดและบริหารจัดการสิทธิการเข้าถึงเป็นไปอย่างเหมาะสมและสอดคล้องกับบทบาทหน้าที่ของผู้ใช้งานหรือบัญชีที่เกี่ยวข้อง

การบริหารจัดการสิทธิควรครอบคลุมระบบทั้ง On-chain และ Off-chain รวมถึงระบบหรือองค์ประกอบทางเทคโนโลยีที่เกี่ยวข้องกับการออก การถือครอง การโอน หรือการบริหารจัดการหลักทรัพย์โทเคน เช่น Smart Contract, DLT Infrastructure, ระบบบริหารจัดการกุญแจเข้ารหัส (Key Management System), API, Oracle, Custody System, ฐานข้อมูล หรือระบบสนับสนุนอื่นตามที่มีการใช้งานและมีความเกี่ยวข้องกับการให้บริการ

การกำหนดสิทธิควรสอดคล้องกับบทบาทหน้าที่ ความจำเป็นในการปฏิบัติงาน และระดับความเสี่ยงของระบบหรือข้อมูลที่เข้าถึง โดยควรมีการบริหารจัดการสิทธิตลอดวงจรชีวิตของผู้ใช้งานหรือบัญชีที่เกี่ยวข้อง ตั้งแต่การให้สิทธิ การเปลี่ยนแปลงสิทธิ การทบทวนสิทธิ จนถึงการยกเลิกสิทธิอย่างเหมาะสม

ข้อเสนอแนะขั้นต่ำ

ผู้ออกหลักทรัพย์โทเคนและผู้ให้บริการที่เกี่ยวข้องควรดำเนินการอย่างน้อย ดังต่อไปนี้

(1) การบริหารจัดการตัวตนและการพิสูจน์ตัวตน (Identity and Authentication Management) : ควรจัดให้มีกระบวนการระบุและบริหารจัดการตัวตนสำหรับผู้ใช้งาน ผู้ดูแลระบบ ผู้ให้บริการภายนอก บัญชีระบบ และผู้เกี่ยวข้องอื่น โดยควรกำหนดให้แต่ละบัญชีสามารถเชื่อมโยงกับบุคคลหรือระบบที่รับผิดชอบได้อย่างชัดเจน และหลีกเลี่ยงการใช้บัญชีร่วมกัน เว้นแต่มีเหตุจำเป็นและมีมาตรการที่สามารถระบุผู้ใช้งานจริงได้ ทั้งนี้ ควรใช้วิธีการพิสูจน์ตัวตนที่เหมาะสมกับระดับความเสี่ยง และใช้ MFA[10] หรือมาตรการที่ให้ผลเทียบเท่าสำหรับการเข้าถึงระบบหรือฟังก์ชันสำคัญ

ควรจัดให้มีกระบวนการระบุและบริหารจัดการตัวตน ตลอดวงจรชีวิตของผู้ใช้งานหรือบัญชีที่เกี่ยวข้อง สำหรับผู้ใช้งาน ผู้ดูแลระบบ ผู้ให้บริการภายนอก บัญชีระบบและผู้เกี่ยวข้องอื่น โดยควรกำหนดให้แต่ละบัญชีสามารถเชื่อมโยงกับบุคคลหรือระบบที่รับผิดชอบได้อย่างชัดเจน และหลีกเลี่ยงการใช้บัญชีร่วมกัน เว้นแต่มีเหตุจำเป็นและมีมาตรการที่ทำให้สามารถระบุผู้ดำเนินการแต่ละรายได้ ทั้งนี้ ควรใช้วิธีการพิสูจน์ตัวตนที่เหมาะสมกับระดับความเสี่ยง และใช้ Multi-Factor Authentication (MFA) หรือมาตรการที่ให้ผลเทียบเท่าสำหรับการเข้าถึงระบบหรือฟังก์ชันสำคัญ

(2) การกำหนดและควบคุมสิทธิการเข้าถึง (Access Provisioning and Control) : ควรกำหนดสิทธิการเข้าถึงตามบทบาทหน้าที่และความจำเป็นในการปฏิบัติงาน โดยจำกัดสิทธิเท่าที่จำเป็นต่อการปฏิบัติงาน (Least Privilege / Need to Know) และจัดให้มีการแบ่งแยกหน้าที่ (Segregation of Duties) สำหรับการดำเนินการที่มีนัยสำคัญหรือมีความเสี่ยงสูงตามความเหมาะสม นอกจากนี้ ควรมีกระบวนการ

[10] Multi-factor Authentication (MFA) คือ การยืนยันตัวตนโดยใช้หลักฐานต่างประเภทกันอย่างน้อยสองประเภท เช่น รหัสผ่านร่วมกับอุปกรณ์ยืนยันตัวตนหรือลายนิ้วมือ

อนุมัติ การให้สิทธิ การเปลี่ยนแปลงสิทธิ และการยกเลิกสิทธิที่ชัดเจน โดยดำเนินการอย่างทันท่วงทีเมื่อมีการเข้าปฏิบัติงาน การเปลี่ยนแปลงบทบาทหน้าที่ การสิ้นสุดหน้าที่ หรือการยุติการให้บริการ

(3) การทบทวนสิทธิและการบริหารจัดการบัญชีระบบ (Access Review and System Account Management) : ควรทบทวนความเหมาะสมของสิทธิการเข้าถึง (Access Review) เป็นระยะและเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ รวมทั้งควรบริหารจัดการบัญชีระบบ (System Account), API Key, Credential และข้อมูลที่ใช้เชื่อมต่อระหว่างระบบให้มีการจำกัดสิทธิ การจัดเก็บอย่างปลอดภัย การเปลี่ยนแปลงหรือหมุนเวียน (Rotation) ตามความเหมาะสม และการยกเลิกเมื่อไม่มีความจำเป็นต้องใช้งาน

(4) การติดตามและตรวจสอบการเข้าถึง (Access Monitoring and Auditability) : ควรบันทึกและติดตามการเข้าถึงระบบ ข้อมูล และฟังก์ชันสำคัญ รวมถึงการเปลี่ยนแปลงสิทธิ เพื่อให้สามารถตรวจพบการเข้าถึงที่ผิดปกติ ระบุผู้ดำเนินการ และตรวจสอบย้อนหลังได้ ทั้งนี้ ควรป้องกันบันทึกข้อมูล (Logs) ดังกล่าวจากการแก้ไข ลบ หรือทำลายโดยไม่ได้รับอนุญาต และกำหนดระยะเวลาการจัดเก็บ (Retention Period) ให้เหมาะสมกับความสำคัญและความเสี่ยงของระบบ รวมถึงข้อกำหนดที่เกี่ยวข้อง ทั้งนี้ การบันทึก การติดตาม และการตรวจสอบการเข้าถึงให้เป็นไปตามหลักเกณฑ์ในข้อ 6.6

6.3.2 การบริหารจัดการสิทธิพิเศษ (Privileged Access Management)

หลักการทั่วไป

บัญชีหรือผู้ใช้งานที่มีสิทธิพิเศษสามารถเข้าถึงหรือดำเนินการที่มีผลกระทบสูงต่อระบบ ข้อมูล การตั้งค่า หรือการให้บริการหลักทรัพย์โทเคนได้ เช่น การเปลี่ยนแปลงการตั้งค่าระบบ การจัดการผู้ใช้งานหรือสิทธิการเข้าถึง การติดตั้งหรือปรับปรุงซอฟต์แวร์ การบริหารจัดการโครงสร้างพื้นฐาน หรือการเข้าถึงข้อมูลหรือระบบที่มีความสำคัญ จึงควรได้รับการควบคุมที่เข้มงวดกว่าบัญชีทั่วไป เพื่อลดความเสี่ยงจากการใช้งานโดยมิชอบ ความผิดพลาดของผู้ใช้งาน หรือการถูกโจมตี

สิทธิพิเศษตามหัวข้อนี้ครอบคลุมสิทธิของผู้ดูแลระบบ ผู้ดูแลโครงสร้างพื้นฐาน ผู้พัฒนาและผู้ที่นำระบบขึ้นใช้งานจริง ผู้ดูแลระบบฐานข้อมูล ผู้ดูแลระบบเชื่อมต่อ ผู้ดูแลระบบ DLT และผู้ที่สามารถเปลี่ยนแปลงการตั้งค่าหรือควบคุมระบบสำคัญ ทั้งนี้ ไม่รวมถึงการอนุมัติหรือการดำเนินการ

ที่เกี่ยวข้องกับกุญแจเข้ารหัส หรือการดำเนินการที่มีสิทธิพิเศษซึ่งมีผลโดยตรงต่อสถานะหรือสิทธิในหลักทรัพย์โทเคน เช่น mint, burn, freeze, unfreeze, force transfer หรือ privileged operation ซึ่งพิจารณาแยกในหัวข้อ 6.4

การบริหารจัดการสิทธิพิเศษควรครอบคลุมการระบุและจำแนกบัญชีหรือผู้ใช้งานที่มีสิทธิพิเศษ การควบคุมการให้และใช้สิทธิ การพิสูจน์ตัวตนและการควบคุมการเข้าถึงที่เหมาะสมกับระดับความเสี่ยง การแบ่งแยกหน้าที่ การติดตามและทบทวนการใช้สิทธิ ตลอดจนการรองรับกรณีฉุกเฉิน โดยระดับและรูปแบบของการควบคุมควรสอดคล้องกับความสำคัญและผลกระทบของสิทธิที่ได้รับ

ข้อเสนอแนะขั้นต่ำ

ผู้ออกหลักทรัพย์โทเคนและผู้ให้บริการที่เกี่ยวข้องควรดำเนินการอย่างน้อย ดังต่อไปนี้

(1) การระบุ อนุมัติ และจำกัดสิทธิพิเศษ (Privileged Access Identification and Authorization) : ควรระบุบัญชี บทบาท และฟังก์ชันที่มีสิทธิพิเศษให้ชัดเจน และจำกัดการให้สิทธิเฉพาะผู้ที่มีความจำเป็นตามบทบาทหน้าที่ โดยต้องได้รับอนุมัติจากผู้มีอำนาจก่อนใช้งาน ทั้งนี้ ควรแยกบัญชีสำหรับการปฏิบัติงานทั่วไปออกจากบัญชีสิทธิพิเศษ และกำหนดสิทธิในลักษณะจำกัดขอบเขต ระยะเวลา หรือภารกิจเท่าที่จำเป็นต่อการปฏิบัติงาน เพื่อลดการถือครองสิทธิถาวรเกินสมควร

(2) การพิสูจน์ตัวตนและการควบคุมการใช้งานสิทธิพิเศษ (Authentication and Privileged Operation Controls) : บัญชีสิทธิพิเศษควรใช้ Multi-factor Authentication (MFA) หรือมาตรการที่ให้ระดับความเชื่อมั่นเทียบเท่าในการเข้าถึงระบบหรือฟังก์ชันที่มีสิทธิพิเศษ และควรมีการควบคุมเพิ่มเติมตามระดับความเสี่ยงของการใช้งาน เช่น การพิสูจน์ตัวตนซ้ำก่อนดำเนินการที่มีความเสี่ยงสูง การจำกัดช่องทางหรือสภาพแวดล้อมที่สามารถใช้สิทธิพิเศษ การจำกัดขอบเขตของการดำเนินการ และการควบคุมระยะเวลาการใช้งานสิทธิพิเศษตามความเหมาะสม เป็นต้น ทั้งนี้ ควรป้องกัน Credential, Token, API Key และข้อมูลหรือปัจจัยที่ใช้ในการพิสูจน์ตัวตนของบัญชีสิทธิพิเศษจากการเปิดเผย สูญหาย ถูกคัดลอก หรือถูกนำไปใช้งานโดยไม่ได้รับอนุญาต และควรจัดให้มีมาตรการควบคุมการจัดเก็บ การส่งผ่าน และการใช้งานข้อมูลดังกล่าวอย่างเหมาะสม ทั้งนี้ ควรหลีกเลี่ยงการฝังหรือจัดเก็บข้อมูลดังกล่าวไว้ใน Source Code, Configuration หรือสภาพแวดล้อมที่ไม่เหมาะสม

สำหรับการดำเนินการที่มีความเสี่ยงสูงหรืออาจส่งผลกระทบในวงกว้างต่อระบบหรือการให้บริการ ควรจัดให้มีการแบ่งแยกหน้าที่ (Segregation of Duties) และการควบคุมโดยบุคคลตั้งแต่สองรายขึ้นไป (Dual Control / Multi-person Control) หรือกระบวนการอนุมัติหลายระดับตามความเหมาะสม เพื่อป้องกันไม่ให้บุคคลใดบุคคลหนึ่งสามารถดำเนินการที่มีความเสี่ยงสูงได้โดยลำพัง

การควบคุมการใช้งานสิทธิพิเศษควรครอบคลุมตั้งแต่การเริ่มเข้าสู่ระบบ การได้รับสิทธิ การยกระดับสิทธิ การดำเนินการภายใต้สิทธิพิเศษ และการสิ้นสุดการใช้งาน โดยควรมีมาตรการป้องกันการใช้สิทธิพิเศษเกินขอบเขตหรือเกินระยะเวลาที่ได้รับอนุญาต ทั้งนี้ การควบคุมการดำเนินการที่เกี่ยวข้องกับกุญแจเข้ารหัสและ Privileged Operation ที่มีผลโดยตรงต่อสถานะหรือสิทธิในหลักทรัพย์โทเคน ให้เป็นไปตามหลักเกณฑ์ในข้อ 6.4

(3) การติดตาม ทบทวน และจัดการสิทธิกรณีฉุกเฉิน (Monitoring, Review and Emergency Access) : ควรบันทึกและติดตามการใช้สิทธิพิเศษ โดยเฉพาะการเข้าสู่ระบบ การเข้าถึงข้อมูลสำคัญ การเปลี่ยนแปลงการตั้งค่าหรือสิทธิการเข้าถึง การติดตั้งหรือปรับปรุงระบบ การนำระบบขึ้นใช้งาน และการดำเนินการอื่นที่มีนัยสำคัญ เพื่อให้สามารถระบุผู้ดำเนินการ เวลา และการดำเนินการที่เกิดขึ้น ตรวจพบพฤติกรรมหรือการใช้งานที่ผิดปกติ และตรวจสอบย้อนหลังได้ ทั้งนี้ ควรป้องกันบันทึกข้อมูล (Logs) จากการแก้ไข ลบ หรือทำลายโดยไม่ได้รับอนุญาต โดยให้เป็นไปตามหลักเกณฑ์ในข้อ 6.6

นอกจากนี้ ควรทบทวนสิทธิพิเศษ เป็นระยะอย่างน้อยปีละหนึ่งครั้งสำหรับบัญชีหรือผู้ใช้งานที่มีสิทธิพิเศษในระบบสำคัญ รวมถึงเมื่อมีการเปลี่ยนแปลงบทบาทหน้าที่หรือเหตุการณ์ที่อาจส่งผลต่อความเหมาะสมของสิทธิ และควรยกเลิกหรือปรับลดสิทธิที่ไม่จำเป็นหรือไม่สอดคล้องกับบทบาทหน้าที่โดยไม่ล่าช้า

สำหรับบัญชีหรือสิทธิกรณีฉุกเฉิน (Emergency Access) ควรกำหนดเงื่อนไขและวัตถุประสงค์ในการใช้งาน ผู้มีอำนาจอนุมัติ ขอบเขตและระยะเวลาการใช้งาน รวมถึง

จัดให้มีการบันทึกเหตุผลและกิจกรรมที่ดำเนินการ และควรทบทวนการใช้งานภายหลังเหตุการณ์ รวมทั้งยกเลิกสิทธิเมื่อสิ้นสุดความจำเป็น

6.4 การบริหารจัดการกุญแจเข้ารหัสและการดำเนินการที่มีสิทธิพิเศษ (Cryptographic Key and Privileged Operations Management)

กุญแจเข้ารหัสและการดำเนินการที่มีสิทธิพิเศษที่ใช้ในระบบหลักทรัพย์โทเคนเป็นองค์ประกอบที่มีความสำคัญสูง เนื่องจากอาจใช้ในการควบคุมการเข้าถึงระบบ การลงนามธุรกรรม การนำระบบขึ้นใช้งาน การอัปเกรดระบบ การออกหรือเพิกถอนโทเคน การระงับธุรกรรม หรือการดำเนินการอื่นที่มีผลต่อสถานะของโทเคนและสิทธิของผู้ถือหลักทรัพย์โทเคน

หัวข้อนี้ครอบคลุมการบริหารจัดการกุญแจเข้ารหัสที่อยู่ภายใต้การควบคุมหรือความรับผิดชอบของผู้ออกหลักทรัพย์โทเคน ผู้ให้บริการ หรือผู้เกี่ยวข้องในระบบ เช่น กุญแจที่ใช้ในการบริหารจัดการกระเป๋าของผู้ออกหลักทรัพย์ (Issuer Wallet Key) กุญแจที่ใช้ในการบริหารจัดการเงินหรือทรัพย์สิน (Treasury Wallet Key) กุญแจที่ใช้ในการออกโทเคน (Mint Authority Key) กุญแจที่ใช้ในการอัปเกรด Smart Contract (Upgrade Authority Key) กุญแจที่ใช้ในการลงนามร่วม (Multisig Signer Key) และกุญแจที่ใช้ในการนำระบบขึ้นใช้งาน (Deployment Key) รวมถึงกุญแจที่ใช้กับโครงสร้างพื้นฐาน DLT เป็นต้น และการควบคุมการดำเนินการที่มีสิทธิพิเศษซึ่งสามารถส่งผลโดยตรงต่อสถานะหรือสิทธิในหลักทรัพย์โทเคน ทั้งนี้ ไม่ครอบคลุมกุญแจส่วนตัว (Private Key) ของผู้ลงทุนที่ผู้ลงทุนเป็นผู้ถือและควบคุมด้วยตนเอง

การบริหารจัดการกุญแจเข้ารหัสและการดำเนินการที่มีสิทธิพิเศษควรคำนึงถึงความมั่นคงปลอดภัยตลอดวงจรชีวิตของกุญแจและการดำเนินการดังกล่าว โดยให้ความสำคัญกับการป้องกันการเข้าถึงหรือการใช้งานโดยไม่ได้รับอนุญาต การควบคุมการใช้กุญแจและสิทธิที่มีผลกระทบสูง การแบ่งแยกหน้าที่ และการควบคุมให้การดำเนินการที่สำคัญเป็นไปตามอำนาจและเงื่อนไขที่กำหนด รวมถึงสามารถตรวจสอบย้อนหลังการดำเนินการที่มีนัยสำคัญได้

6.4.1 การบริหารจัดการวงจรชีวิตของกุญแจเข้ารหัส (Cryptographic Key Lifecycle Management)

หลักการทั่วไป

กุญแจเข้ารหัสที่อยู่ภายใต้การควบคุมหรือความรับผิดชอบของผู้ออกหลักทรัพย์โทเคน ผู้ให้บริการ หรือผู้เกี่ยวข้องในระบบ ควรได้รับการบริหารจัดการอย่างเหมาะสมตลอดวงจรชีวิต ตั้งแต่การสร้าง การจัดเก็บ การส่งมอบหรือแจกจ่าย การใช้งาน การหมุนเวียน การยกเลิก การกู้คืน และการทำลายหรือยุติการใช้งาน

การบริหารจัดการกุญแจควรทำให้สามารถระบุได้อย่างชัดเจนว่าระบบมีการใช้กุญแจประเภทใด กุญแจแต่ละประเภทใช้เพื่อวัตถุประสงค์ใด ใครเป็นผู้รับผิดชอบหรือมีสิทธิเข้าถึง กุญแจถูกจัดเก็บและใช้งานอย่างไร รวมถึงมีมาตรการรองรับกรณีกุญแจสูญหาย ถูกเปิดเผย ถูกใช้งานโดยมิชอบหรือไม่สามารถใช้งานได้

มาตรการตามหัวข้อนี้ควรกำหนดให้เหมาะสมกับระดับความสำคัญของกุญแจและผลกระทบที่อาจเกิดขึ้นหากกุญแจดังกล่าวถูกเข้าถึง สูญหาย ถูกแก้ไข ถูกใช้ผิดวัตถุประสงค์ หรือไม่สามารถใช้งานได้ โดยเฉพาะกุญแจที่เกี่ยวข้องกับการบริหารระบบ การลงนามธุรกรรม การเชื่อมต่อกับระบบภายนอก หรือการดำเนินการที่อาจกระทบต่อสิทธิของผู้ถือหลักทรัพย์โทเคน

ข้อเสนอแนะขั้นต่ำ

ผู้ออกหลักทรัพย์โทเคนและผู้ให้บริการที่เกี่ยวข้องควรดำเนินการอย่างน้อย ดังต่อไปนี้

(1) การระบุและกำกับดูแลกุญแจเข้ารหัส (Key Inventory and Governance) : ควรจัดทำและดูแลรายการกุญแจเข้ารหัส (Key Inventory) ที่อยู่ภายใต้การควบคุมหรือความรับผิดชอบ โดยระบุอย่างน้อยถึงวัตถุประสงค์ ระบบหรือการดำเนินการที่เกี่ยวข้อง ผู้รับผิดชอบ ระดับความสำคัญ และขอบเขตการใช้งานของกุญแจแต่ละประเภท รวมถึงสถานะของกุญแจและข้อมูลที่จำเป็นต่อการบริหารจัดการตลอดวงจรชีวิต ทั้งนี้ ควรกำหนดบทบาทและผู้มีอำนาจในการอนุมัติการดำเนินการที่เกี่ยวข้องกับกุญแจ และกำหนดแนวทางการบริหารจัดการให้เหมาะสมกับระดับความสำคัญและความเสี่ยงของกุญแจ

(2) การสร้าง จัดเก็บ และควบคุมการใช้กุญแจ (Key Generation, Storage and Usage Controls) : ควรสร้างกุญแจด้วยกระบวนการที่มีความมั่นคงปลอดภัยและเหมาะสมกับวัตถุประสงค์และระดับความสำคัญของกุญแจ โดยใช้กลไกการสร้างกุญแจที่มีความมั่นคงปลอดภัยและใช้แหล่งกำเนิดค่าความสุ่มที่เหมาะสม (Secure Randomness) และสามารถป้องกันการเปิดเผยหรือการเข้าถึงกุญแจโดยไม่ได้รับอนุญาตในระหว่างกระบวนการสร้าง ทั้งนี้ สำหรับกุญแจที่มีความสำคัญสูง ควรใช้สภาพแวดล้อมหรืออุปกรณ์ที่ออกแบบมาเพื่อรักษาความลับและความถูกต้องของกุญแจ เช่น Hardware Security Module (HSM)[11], Secure Cryptographic Device หรือมาตรการที่ให้ระดับความปลอดภัยเทียบเท่า และควรพิจารณา

[11] Hardware Security Module (HSM) คือ อุปกรณ์เฉพาะที่ออกแบบมาเพื่อใช้สร้าง private key และสามารถใช้ sign transaction โดย private key ยังคงอยู่ในสภาพแวดล้อมแบบปิด จึงไม่มีความเสี่ยงของการนำ private key ออกมาใช้ข้างนอกหรือเชื่อมต่อ online

กระบวนการสร้างกุญแจที่ลดการควบคุมโดยบุคคลหรือองค์ประกอบใดองค์ประกอบหนึ่งเพียงรายเดียว เช่น Multi-party Computation (MPC) หรือ Threshold Cryptography[12] ตามความเหมาะสมกับสถาปัตยกรรมและระดับความเสี่ยงของระบบ

นอกจากนี้ ควรจัดเก็บและใช้งานกุญแจในสภาพแวดล้อมที่มีการแยกและควบคุมกุญแจอย่างเหมาะสม (Key Isolation) และมีมาตรการป้องกันการเข้าถึง การคัดลอกหรือการนำกุญแจออกจากสภาพแวดล้อมดังกล่าวโดยไม่ได้รับอนุญาต โดยจำกัดสิทธิการเข้าถึงหรือการใช้งานกุญแจเฉพาะผู้หรือระบบที่มีความจำเป็นตามบทบาทหน้าที่ กำหนดวัตถุประสงค์ ขอบเขต และเงื่อนไขการใช้งานกุญแจให้ชัดเจน และใช้ช่องทางที่ปลอดภัยในการแจกจ่าย ส่งมอบ หรือแบ่งปันกุญแจ ทั้งนี้ ควรสามารถระบุผู้ถือครองหรือระบบที่เข้าถึงหรือใช้งานกุญแจได้ และควรป้องกันไม่ให้กุญแจหรือข้อมูลที่สามารถนำไปใช้เพื่อเข้าถึงกุญแจถูกจัดเก็บหรือเปิดเผยใน Source Code, Configuration File หรือสภาพแวดล้อมอื่นที่ไม่เหมาะสม

(3) การหมุนเวียน ยกเลิก และรองรับเหตุผิดปกติ (Key Rotation, Revocation and Incident Handling) : ควรกำหนดกระบวนการหมุนเวียนหรือเปลี่ยนกุญแจ (Key Rotation) และการยกเลิกการใช้งานกุญแจ (Key Revocation) ตามรอบระยะเวลา อายุการใช้งาน ระดับความสำคัญของกุญแจ และระดับความเสี่ยงที่เกี่ยวข้อง รวมถึงเมื่อมีการเปลี่ยนแปลงผู้รับผิดชอบหรือมีเหตุอันควรสงสัยว่ากุญแจอาจถูกเปิดเผย สูญหาย หรือถูกใช้งานโดยไม่ได้รับอนุญาต ทั้งนี้ ควรควบคุมให้การเปลี่ยนหรือหมุนเวียนกุญแจไม่ส่งผลกระทบต่อความถูกต้องและความต่อเนื่องของธุรกรรมหรือบริการที่เกี่ยวข้อง

นอกจากนี้ ควรมีแนวทางรองรับกรณีกุญแจสูญหาย ถูกเปิดเผย ถูกใช้งานโดยมิชอบหรือไม่สามารถใช้งานได้ โดยสามารถดำเนินการระงับหรือยกเลิกการใช้กุญแจ เปลี่ยนกุญแจ กู้คืนหรือเรียกคืนการควบคุมกุญแจ และดำเนินการอื่นที่จำเป็นเพื่อจำกัดผลกระทบ รวมถึงการประเมินว่าธุรกรรมหรือระบบที่เกี่ยวข้องได้รับ

[12] Threshold Cryptography คือ เทคนิคที่แบ่งกุญแจเข้ารหัสเป็นส่วนย่อยให้หลายฝ่ายถือไว้ และต้องร่วมกันใช้งานให้ครบจำนวนขั้นต่ำที่กำหนด จึงจะดำเนินการได้ เช่น การลงลายมือชื่อดิจิทัล

ผลกระทบหรือไม่ และการแจ้งผู้เกี่ยวข้องตามความเหมาะสม ทั้งนี้ ควรมีการทดสอบหรือเตรียมความพร้อมสำหรับกระบวนการกู้คืนและเปลี่ยนกุญแจที่มีความสำคัญสูงเพื่อให้สามารถกลับมาใช้งานได้ภายในระยะเวลาที่เหมาะสม

(4) การตรวจสอบการบริหารจัดการกุญแจ (Key Management Auditability) : ควรบันทึกและจัดเก็บหลักฐานที่เกี่ยวข้องกับการบริหารจัดการกุญแจตลอดวงจรชีวิตตามความเหมาะสม เช่น การสร้าง การจัดเก็บ การเข้าถึง การใช้งาน การเปลี่ยนหรือหมุนเวียน การยกเลิกการใช้งาน และเหตุการณ์ที่มีนัยสำคัญ เพื่อให้สามารถตรวจสอบได้ว่ากุญแจถูกบริหารจัดการและใช้งานโดยผู้หรือระบบที่ได้รับอนุญาตและเป็นไปตามวัตถุประสงค์และเงื่อนไขที่กำหนด ทั้งนี้ ควรป้องกันบันทึกและหลักฐานดังกล่าวจากการแก้ไข ลบ หรือทำลายโดยไม่ได้รับอนุญาต และจัดเก็บไว้เป็นระยะเวลาที่เหมาะสมกับระดับความสำคัญและความเสี่ยงของกุญแจ รวมถึงข้อกำหนดที่เกี่ยวข้อง โดยการบันทึก การติดตาม และการตรวจสอบให้เป็นไปตามหลักเกณฑ์ในข้อ 6.6

6.4.2 การจัดการกุญแจสำหรับการดำเนินการที่มีสิทธิพิเศษ (Privileged Key Management)

หลักการทั่วไป

กุญแจที่ใช้สำหรับการดำเนินการที่มีผลกระทบสูงต่อระบบหลักทรัพย์โทเคน หรือสิทธิและสถานะของหลักทรัพย์โทเคนและผู้ถือหลักทรัพย์โทเคน ควรได้รับการควบคุมในระดับที่เหมาะสมกับอำนาจและผลกระทบที่อาจเกิดขึ้น เช่น กุญแจที่ใช้ในการออก การทำลายหรือเพิกถอนโทเคน การอัปเกรด Smart Contract การเปลี่ยนแปลงค่าหรือการตั้งค่าที่สำคัญของระบบ การกู้คืนหรือเปลี่ยนแปลงสิทธิ การระงับหรือปลดระงับการดำเนินการ หรือการดำเนินการอื่นที่มีผลกระทบในลักษณะเดียวกัน

การบริหารจัดการกุญแจที่มีสิทธิพิเศษควรทำให้สามารถระบุได้อย่างชัดเจนว่ากุญแจแต่ละประเภทสามารถใช้ดำเนินการใด มีขอบเขตและเงื่อนไขการใช้งานอย่างไร ใครเป็นผู้ได้รับมอบหมายให้ควบคุมหรือใช้งาน และกุญแจดังกล่าวถูกใช้กับระบบหรือองค์ประกอบใด รวมทั้งควรจัดให้มีการควบคุมเพิ่มเติมเพื่อป้องกันการใช้อำนาจดังกล่าวโดยไม่ได้รับอนุญาตหรือโดยบุคคลหรือองค์ประกอบใดองค์ประกอบหนึ่งเพียงรายเดียว

การควบคุมกุญแจที่มีสิทธิพิเศษควรครอบคลุมการกำหนดผู้มีอำนาจ การแบ่งแยกการควบคุม การอนุมัติ การจำกัดขอบเขตและระยะเวลาการใช้งาน การติดตามและตรวจสอบการใช้งาน

ตลอดจนการรองรับกรณีฉุกเฉิน โดยอาจใช้กลไกทางเทคนิคหรือกระบวนการควบคุมที่เหมาะสมกับสถาปัตยกรรมและระดับความเสี่ยงของระบบ

ข้อเสนอแนะขั้นต่ำ

ผู้ออกหลักทรัพย์โทเคนและผู้ให้บริการที่เกี่ยวข้องควรดำเนินการอย่างน้อย ดังต่อไปนี้

(1) การระบุและกำหนดขอบเขตของกุญแจที่มีสิทธิพิเศษ (Privileged Key Identification and Classification) : ควรระบุกุญแจที่มีอำนาจหรือผลกระทบสูง เช่น กุญแจที่ใช้ในการออกหรือทำลายโทเคน (Mint Key / Burn Key) กุญแจที่ใช้ในการอัปเกรด Smart Contract (Upgrade Key) หรือกุญแจที่ใช้ในการกู้คืนหรือควบคุมการดำเนินการที่มีความสำคัญ และกำหนดวัตถุประสงค์ ขอบเขตการใช้งาน และผลกระทบที่อาจเกิดขึ้นจากการใช้กุญแจแต่ละประเภทให้ชัดเจน รวมทั้งกำหนดผู้ได้รับมอบหมายให้ควบคุมหรือใช้งาน และผู้มีสิทธิเข้าถึงกุญแจดังกล่าว โดยควรจำแนกระดับความสำคัญของกุญแจเพื่อกำหนดมาตรการควบคุมให้เหมาะสมกับระดับความเสี่ยง

(2) การควบคุมการถือครองและการใช้งานกุญแจ (Key Custody and Usage Controls) : ควรจำกัดการเข้าถึงและใช้งานกุญแจเฉพาะผู้ที่มีความจำเป็นตามบทบาทหน้าที่ และไม่ควรให้กุญแจที่มีผลกระทบสูงอยู่ภายใต้การควบคุมของบุคคลเพียงรายเดียว เว้นแต่มีมาตรการควบคุมอื่นที่ให้ผลเทียบเท่าและสามารถอธิบายเหตุผลได้ ทั้งนี้ ควรจัดให้มีมาตรการควบคุมเพิ่มเติมตามระดับความเสี่ยง เช่น การใช้ Multi-signature, Dual Control, Approval Workflow หรือการใช้กลไกหรือสถาปัตยกรรมที่ช่วยลดความเสี่ยงจากการควบคุมกุญแจโดยบุคคลหรือองค์ประกอบใดองค์ประกอบหนึ่งเพียงรายเดียว เช่น Multi-party Computation (MPC) หรือ Threshold Cryptography รวมถึงการใช้ Hardware Security Module (HSM) หรือมาตรการที่ให้ผลเทียบเท่า ตามความเหมาะสมกับลักษณะและระดับความเสี่ยงของกุญแจ

ทั้งนี้ ควรกำหนดวัตถุประสงค์ ขอบเขต เงื่อนไข และระยะเวลาการเข้าถึงหรือใช้งานกุญแจที่มีสิทธิพิเศษให้ชัดเจน และควรควบคุมให้การใช้งานกุญแจเป็นไปตามขอบเขตและเงื่อนไขที่กำหนด

(3) การทบทวนกุญแจที่มีสิทธิพิเศษ (Privileged Key Review) : ควรทบทวนผู้ได้รับมอบหมายให้ควบคุมหรือใช้งานกุญแจ ผู้มีสิทธิเข้าถึง และความเหมาะสมของมาตรการควบคุมเป็นระยะอย่างน้อยปีละหนึ่งครั้ง รวมทั้งเมื่อมีการเปลี่ยนแปลงผู้รับผิดชอบ โครงสร้างการควบคุม หรือเหตุการณ์ที่อาจส่งผลต่อความเหมาะสมของการควบคุม เพื่อให้มั่นใจว่าการควบคุมกุญแจยังสอดคล้องกับอำนาจ หน้าที่ และระดับความเสี่ยงของการดำเนินการ

6.4.3 การกำกับดูแลการดำเนินการบนระบบที่มีสิทธิพิเศษ (Governance of Privileged Operations)

หลักการทั่วไป

การดำเนินการที่มีสิทธิพิเศษ (Privileged Operations) อาจมีผลกระทบสูงต่อระบบข้อมูล สถานะของโทเคน หรือสิทธิของผู้ถือหลักทรัพย์โทเคน จึงควรอยู่ภายใต้กระบวนการกำกับดูแล การควบคุม และการตรวจสอบที่เหมาะสมกับลักษณะและระดับความเสี่ยงของการดำเนินการ โดยควรกำหนดให้การดำเนินการดังกล่าวเป็นไปตามอำนาจ วัตถุประสงค์ ขอบเขต และเงื่อนไขที่กำหนด

การดำเนินการที่มีสิทธิพิเศษอาจรวมถึงการออกโทเคน (Mint) การทำลายหรือเพิกถอนโทเคน (Burn / Revoke) การระงับหรือปลดระงับการใช้งานโทเคน (Freeze / Unfreeze) การโอนโทเคนโดยคำสั่งพิเศษ (Force Transfer) การกู้คืนหรือเปลี่ยนแปลงสิทธิ (Recovery / Reassignment) การปรับปรุง Smart Contract (Contract Upgrade) การเปลี่ยนแปลงค่าหรือการตั้งค่าที่สำคัญของระบบ (Parameter / Configuration Change) การระงับหรือเปิดการทำงานของระบบหรือฟังก์ชัน (Pause / Unpause) การควบคุมทรัพย์สินหรือเงินที่อยู่ภายใต้ระบบ (Treasury Control) หรือการดำเนินการอื่นที่มีผลกระทบสูงต่อระบบ โทเคน หรือสิทธิของผู้ถือหลักทรัพย์โทเคน ทั้งนี้ ขอบเขตของการดำเนินการที่ถือว่ามีผลกระทบสูงควรกำหนดตามลักษณะของผลิตภัณฑ์ ระบบ และระดับความเสี่ยงที่เกี่ยวข้อง

การกำกับดูแลการดำเนินการที่มีสิทธิพิเศษ ควรกำหนดกระบวนการและเงื่อนไขในการดำเนินการ (Operation Workflow and Control) ให้ชัดเจน และจัดให้มีการแบ่งแยกหน้าที่ (Segregation of Duties) ตามความเหมาะสมกับลักษณะและระดับความเสี่ยงของการดำเนินการ รวมทั้งควรบันทึกและเก็บรักษาหลักฐานที่เกี่ยวข้อง เพื่อให้สามารถตรวจสอบย้อนหลังได้

ข้อเสนอแนะขั้นต่ำ

ผู้ออกหลักทรัพย์โทเคนและผู้ให้บริการที่เกี่ยวข้องควรดำเนินการอย่างน้อย ดังต่อไปนี้

(1) การกำหนดขอบเขต บทบาท และอำนาจในการดำเนินการ (Scope, Roles and Authorities) : ควรกำหนดให้ชัดเจนว่าการดำเนินการใดถือเป็นการดำเนินการที่มี

สิทธิพิเศษหรือมีผลกระทบสูง พร้อมระบุผู้มีอำนาจในการเสนอ ขออนุมัติ อนุมัติ ดำเนินการ และตรวจสอบในแต่ละประเภทของการดำเนินการ โดยควรแบ่งแยกหน้าที่และจำกัดอำนาจให้สอดคล้องกับระดับความเสี่ยงและผลกระทบที่อาจเกิดขึ้น

นอกจากนี้ ควรกำหนดบทบาทและอำนาจของผู้ออกหลักทรัพย์โทเคน นายทะเบียน ผู้ให้บริการระบบ หรือผู้เกี่ยวข้องอื่นให้ชัดเจน โดยให้แต่ละฝ่ายสามารถดำเนินการได้เฉพาะการดำเนินการและภายในขอบเขตอำนาจที่ได้รับมอบหมาย และกำหนดการแบ่งแยกหน้าที่ระหว่างการเสนอ การอนุมัติ การดำเนินการ และการตรวจสอบตามความเหมาะสม ทั้งนี้ ขอบเขตบทบาทและอำนาจควรสอดคล้องกับหน้าที่ตามกฎหมาย โครงสร้างของระบบ และรูปแบบการให้บริการ

(2) การอนุมัติและควบคุมการดำเนินการ (Approval and Operation Controls) : ควรกำหนดกระบวนการอนุมัติและการควบคุมการดำเนินการที่มีสิทธิพิเศษให้ชัดเจน โดยจัดให้มีข้อมูลประกอบการพิจารณาที่เพียงพอ เช่น เหตุผล ความจำเป็น ขอบเขต และผลกระทบที่คาดหมาย รวมถึงเอกสารหรือหลักฐานที่เกี่ยวข้อง และกำหนดให้การดำเนินการเป็นไปตามกระบวนการดังกล่าวก่อนดำเนินการ ทั้งนี้ สำหรับการดำเนินการที่มีผลกระทบสูงควรจัดให้มีผู้มีอำนาจมากกว่าหนึ่งราย หรือกลไกควบคุมที่ให้ผลเทียบเท่า เช่น Dual Control, Multi-person Approval หรือ Approval Workflow ตามความเหมาะสมกับระดับความเสี่ยง

การดำเนินการกรณีฉุกเฉิน (Emergency Operation) ควรกำหนดเงื่อนไขและขอบเขตการใช้งาน ผู้มีอำนาจ และกระบวนการที่เกี่ยวข้องไว้อย่างชัดเจน รวมทั้งจัดให้มีการบันทึกเหตุผลและรายละเอียดการดำเนินการ และการทบทวนภายหลังการดำเนินการ

<u>ตัวอย่าง</u>

- กรณีการออกโทเคน (Mint) อาจกำหนดให้ต้องมีคำขอที่ระบุจำนวนและวัตถุประสงค์ของการออกโทเคน ผ่านการตรวจสอบและอนุมัติตามลำดับก่อนดำเนินการ โดยอาจใช้กลไก เช่น Dual Control หรือ Multi-person Approval

เพื่อให้การอนุมัติต้องได้รับความเห็นชอบจากบุคคลมากกว่าหนึ่งราย และให้ผู้ดำเนินการสามารถดำเนินการได้เฉพาะรายการและจำนวนที่ได้รับอนุมัติแล้ว

- กรณีการปรับปรุง Smart Contract (Contract Upgrade) อาจกำหนดให้มีการประเมินผลกระทบและตรวจสอบความถูกต้องของ Smart Contract ที่จะนำมาใช้งาน และได้รับอนุมัติตามระดับความเสี่ยงก่อนดำเนินการ โดยอาจใช้ Approval Workflow หรือกลไกควบคุมอื่นที่ให้ผลเทียบเท่า ทั้งนี้ ควรบันทึกการอนุมัติและผลการดำเนินการไว้เป็นหลักฐาน

(3) การติดตาม บันทึก และทบทวน (Monitoring, Record Keeping and Review) : ควรบันทึกและเก็บรักษาข้อมูลเกี่ยวกับการอนุมัติและการดำเนินการที่มีสิทธิพิเศษให้ครบถ้วน โดยอย่างน้อยควรสามารถระบุผู้ขอ ผู้อนุมัติ ผู้ดำเนินการ เวลา เหตุผล ขอบเขต และผลของการดำเนินการ เพื่อให้สามารถตรวจสอบได้ว่าการดำเนินการเป็นไปตามอำนาจและขั้นตอนที่กำหนด

นอกจากนี้ ควรติดตามการดำเนินการที่มีสิทธิพิเศษอย่างเหมาะสม เพื่อให้สามารถตรวจพบการใช้งานที่ผิดปกติ การใช้อำนาจเกินขอบเขต หรือการดำเนินการที่ไม่เป็นไปตามขั้นตอนที่กำหนด และควรทบทวนรายการการดำเนินการที่มีสิทธิพิเศษ บทบาทของผู้เกี่ยวข้อง และกระบวนการอนุมัติเป็นระยะ รวมทั้งเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ เพื่อให้สอดคล้องกับความเสี่ยง โครงสร้างระบบ และข้อกำหนดของผลิตภัณฑ์

6.5 การรักษาความปลอดภัยของข้อมูล ความถูกต้องครบถ้วน และการรับรองด้วยกลไกการเข้ารหัสลับ (Data Protection, Integrity and Cryptographic Assurance)

ข้อมูลที่เกี่ยวข้องกับการออก การถือครอง การโอน การชำระราคา และการบริหารจัดการหลักทรัพย์โทเคนต้องได้รับการคุ้มครองจากการเปิดเผย การสูญหาย การแก้ไข หรือการใช้งานโดยไม่ได้รับอนุญาต รวมถึงต้องสามารถพิสูจน์ความถูกต้องครบถ้วน ความน่าเชื่อถือ และแหล่งที่มาของข้อมูลหรือธุรกรรมได้ตามความเหมาะสม

หัวข้อนี้ครอบคลุมการรักษาความปลอดภัยของข้อมูล การรักษาความถูกต้องครบถ้วนของข้อมูล การคุ้มครองข้อมูลส่วนบุคคลในบริบทของระบบหลักทรัพย์โทเคน และการใช้กลไกการเข้ารหัสลับ

เพื่อสนับสนุนความน่าเชื่อถือของข้อมูลและธุรกรรม ทั้งข้อมูลที่บันทึกบน DLT ข้อมูลที่จัดเก็บหรือประมวลผลนอก DLT และข้อมูลที่มีการแลกเปลี่ยนหรือเชื่อมโยงระหว่างระบบ

การกำหนดมาตรการตามหัวข้อนี้ควรเป็นไปตามระดับความสำคัญและความเสี่ยงของข้อมูล โดยคำนึงถึงผลกระทบต่อสิทธิของผู้ถือหลักทรัพย์โทเคน ความถูกต้องของธุรกรรม ความต่อเนื่องในการให้บริการ ความเป็นส่วนตัวของผู้เกี่ยวข้อง และการตรวจสอบย้อนหลังของระบบ

6.5.1 การรักษาความปลอดภัยของข้อมูล (Data Protection)

หลักการทั่วไป

ข้อมูลที่เกี่ยวข้องกับหลักทรัพย์โทเคนควรได้รับการระบุ จำแนก และคุ้มครองตามระดับความสำคัญและความเสี่ยง เพื่อให้สามารถป้องกันการเข้าถึง การเปิดเผย การสูญหาย การรั่วไหล หรือการใช้งานโดยไม่ได้รับอนุญาตได้อย่างเหมาะสม

การรักษาความปลอดภัยของข้อมูลควรครอบคลุมข้อมูลที่จัดเก็บ ประมวลผล และรับส่งระหว่างระบบ เช่น ข้อมูลผู้ลงทุน ข้อมูลการถือครอง ข้อมูลธุรกรรม ข้อมูลบัญชีหรือ Wallet Address ข้อมูลที่ใช้ประกอบกระบวนการรู้จักลูกค้า (Know Your Customer : KYC) ข้อมูลการชำระราคา ข้อมูลที่ใช้ในการกำกับเงื่อนไขของโทเคน และข้อมูลที่เกี่ยวข้องกับการทำงานของ DLT หรือระบบสนับสนุนที่เกี่ยวข้อง

มาตรการคุ้มครองข้อมูลควรกำหนดตามลักษณะของข้อมูล แหล่งจัดเก็บและประมวลผล วิธีการใช้งาน ผู้มีสิทธิเข้าถึง และผลกระทบที่อาจเกิดขึ้นหากข้อมูลถูกเปิดเผย สูญหาย หรือถูกใช้งานโดยมิชอบ

ข้อเสนอแนะขั้นต่ำ

ผู้ออกหลักทรัพย์โทเคนและผู้ให้บริการที่เกี่ยวข้องควรดำเนินการอย่างน้อย ดังต่อไปนี้

(1) การระบุและจำแนกข้อมูล (Data Identification and Classification) : ควรระบุประเภทของข้อมูลที่เกี่ยวข้องกับหลักทรัพย์โทเคน และจำแนกระดับความสำคัญหรือความอ่อนไหวตามลักษณะการใช้งาน ความเสี่ยง และผลกระทบที่อาจเกิดขึ้น เพื่อใช้เป็นพื้นฐานในการกำหนดมาตรการคุ้มครอง การเข้าถึง การเก็บรักษา และการทำลายข้อมูลอย่างเหมาะสม

(2) การคุ้มครองและควบคุมการเข้าถึงข้อมูล (Data Protection and Access Control) : ควรกำหนดมาตรการคุ้มครองข้อมูลให้สอดคล้องกับระดับความสำคัญ โดยจำกัดการเข้าถึงเฉพาะผู้ที่มีความจำเป็นตามบทบาทหน้าที่ และคุ้มครองข้อมูล

ทั้งในระหว่างการจัดเก็บ การประมวลผล และการรับส่ง อาจใช้การเข้ารหัส การแยกจัดเก็บ การปกปิดข้อมูล หรือมาตรการป้องกันการรั่วไหลตามความเหมาะสม

(3) การแลกเปลี่ยน การเก็บรักษา และการทำลายข้อมูล (Data Sharing, Retention and Disposal) : ในกรณีที่มีการส่งต่อหรือแลกเปลี่ยนข้อมูลกับบุคคลหรือระบบภายนอก ควรกำหนดวัตถุประสงค์ ขอบเขต ผู้รับข้อมูล ช่องทาง และมาตรการคุ้มครองให้ชัดเจน รวมทั้งควรกำหนดระยะเวลาการเก็บรักษา และดำเนินการลบทำลาย หรือทำให้ไม่สามารถระบุตัวบุคคลได้เมื่อหมดความจำเป็น โดยสอดคล้องกับกฎหมายและข้อกำหนดที่เกี่ยวข้อง

(4) การติดตามและตรวจสอบการใช้งานข้อมูล (Data Access Monitoring and Auditability) : ควรบันทึกและตรวจสอบการเข้าถึงหรือการใช้งานข้อมูลสำคัญตามความเหมาะสม เพื่อให้สามารถระบุผู้ดำเนินการ ตรวจพบการใช้งานผิดปกติ และตรวจสอบย้อนหลังได้

6.5.2 การรักษาความถูกต้องครบถ้วนของข้อมูล (Data Integrity)

<u>หลักการทั่วไป</u>

ข้อมูลที่ใช้ในการออก ถือครอง โอน ชำระราคา และบริหารจัดการหลักทรัพย์โทเคนต้องมีความถูกต้อง ครบถ้วน สอดคล้องกัน และไม่ถูกแก้ไขโดยไม่ได้รับอนุญาต เพื่อให้สามารถใช้เป็นฐานในการพิจารณาสิทธิ สถานะ ธุรกรรม และการกำกับดูแลได้อย่างน่าเชื่อถือ

ในระบบหลักทรัพย์โทเคน ความถูกต้องครบถ้วนของข้อมูลต้องครอบคลุมทั้งข้อมูลที่บันทึกบน DLT ข้อมูลที่จัดเก็บหรือประมวลผลนอก DLT และข้อมูลที่มีการแลกเปลี่ยนหรือเชื่อมโยงระหว่างระบบ รวมถึงความสอดคล้องของข้อมูลที่เกี่ยวข้องกันระหว่างระบบ เช่น ข้อมูลใน Registry Contract กับระบบทะเบียนผู้ถือหลักทรัพย์ ยอดโทเคนกับบัญชีทรัพย์สินของผู้ลงทุน ข้อมูล Corporate Action กับระบบงานภายใน หรือข้อมูลที่บันทึกบน DLT กับข้อมูลของผู้ให้บริการรับฝากทรัพย์สิน เป็นต้น

ระบบควรมีกลไกในการตรวจสอบความถูกต้องของข้อมูล ตรวจพบความคลาดเคลื่อนระหว่างระบบ และแก้ไขหรือจัดการความคลาดเคลื่อนดังกล่าวได้อย่างเหมาะสม โดยไม่กระทบต่อสิทธิของผู้ถือหลักทรัพย์โทเคนหรือความน่าเชื่อถือของระบบ

<u>ข้อเสนอแนะขั้นต่ำ</u>

ผู้ออกหลักทรัพย์โทเคนและผู้ให้บริการที่เกี่ยวข้องควรดำเนินการอย่างน้อย ดังต่อไปนี้

(1) การกำหนดแหล่งข้อมูลและมาตรการควบคุมความถูกต้องครบถ้วน (Data Sources and Integrity Controls) : ควรระบุแหล่งข้อมูล ระบบที่เกี่ยวข้อง และความสัมพันธ์ระหว่างข้อมูลที่บันทึกบน DLT ข้อมูลที่จัดเก็บหรือประมวลผลนอก DLT และข้อมูลที่มีการแลกเปลี่ยนหรือเชื่อมโยงระหว่างระบบให้ชัดเจน รวมทั้งกำหนดมาตรการควบคุมเพื่อให้ข้อมูลมีความถูกต้อง ครบถ้วน และไม่ถูกแก้ไขโดยไม่ได้รับอนุญาตตลอดกระบวนการจัดเก็บ ประมวลผล และรับส่งข้อมูล

(2) การตรวจสอบความสอดคล้องและการกระทบยอดข้อมูล (Data Validation and Reconciliation) : ควรจัดให้มีกลไกตรวจสอบความสอดคล้องและกระทบยอดข้อมูลระหว่างระบบตามรอบเวลาและระดับความเสี่ยงที่เหมาะสม โดยครอบคลุมข้อมูลที่มีผลต่อสิทธิ สถานะ ธุรกรรม การถือครอง และการชำระราคา รวมทั้งควรมีมาตรการตรวจจับหรือแจ้งเตือนเมื่อพบการเปลี่ยนแปลง ความเสียหาย หรือความคลาดเคลื่อนที่ผิดปกติ

(3) การจัดการความคลาดเคลื่อนและการตรวจสอบย้อนหลัง (Discrepancy Management and Auditability) : ควรกำหนดกระบวนการบันทึก วิเคราะห์ และแก้ไขความคลาดเคลื่อนของข้อมูล โดยระบุสาเหตุ ผลกระทบ ผู้รับผิดชอบ และแนวทางดำเนินการให้ชัดเจน การแก้ไขข้อมูลสำคัญควรได้รับอนุมัติจากผู้มีอำนาจ และไม่ทำลายหลักฐานเดิมที่จำเป็นต่อการตรวจสอบ ทั้งนี้ ควรจัดเก็บหลักฐานเกี่ยวกับการตรวจสอบ การกระทบยอด และการแก้ไขข้อมูลให้ครบถ้วนและสามารถตรวจสอบย้อนหลังได้

6.5.3 การคุ้มครองข้อมูลส่วนบุคคล (Privacy Protection)

หลักการทั่วไป

ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับหลักทรัพย์โทเคนควรได้รับการคุ้มครองอย่างเหมาะสม โดยคำนึงถึงความมั่นคงปลอดภัยของข้อมูลและการออกแบบระบบ (Security and Privacy by Design) ทั้งนี้ การพิจารณาว่าข้อมูลใดเป็นข้อมูลส่วนบุคคลไม่ควรจำกัดเฉพาะข้อมูลที่สามารถระบุตัวบุคคลได้โดยตรง แต่ควรรวมถึงข้อมูลที่สามารถเชื่อมโยงหรือระบุตัวบุคคลได้เมื่อพิจารณาร่วมกับข้อมูลอื่นที่เกี่ยวข้อง

ข้อมูลที่ควรให้ความสำคัญอาจรวมถึงข้อมูลที่ใช้ประกอบกระบวนการรู้จักลูกค้า (Know Your Customer: KYC) ข้อมูลผู้ลงทุน ข้อมูลผู้รับประโยชน์ที่แท้จริง (Beneficial Owner) ข้อมูล

การถือครองหลักทรัพย์ ข้อมูลธุรกรรม และ Wallet Address ที่สามารถเชื่อมโยงกลับไปยังบุคคลได้ รวมถึงข้อมูลที่เกิดจากการเชื่อมโยงหรือวิเคราะห์ข้อมูลจากหลายแหล่ง ซึ่งอาจทำให้สามารถระบุหรืออนุมานข้อมูลเกี่ยวกับบุคคลได้

การคุ้มครองข้อมูลส่วนบุคคลในบริบทของหลักทรัพย์โทเคนควรคำนึงถึงการเก็บรวบรวม การใช้ การเปิดเผย และการเข้าถึงข้อมูลเท่าที่จำเป็นตามวัตถุประสงค์ที่กำหนด การจำกัดสิทธิการเข้าถึงและการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต ตลอดจนความเสี่ยงที่เกิดจากการเชื่อมโยงข้อมูลระหว่างระบบหรือจากหลายแหล่ง ทั้งนี้ ควรพิจารณาความเสี่ยงดังกล่าวตั้งแต่การออกแบบระบบ แม้ข้อมูลที่บันทึกบนระบบ DLT จะไม่แสดงชื่อหรือข้อมูลที่ระบุตัวบุคคลโดยตรงก็ตาม

ข้อเสนอแนะขั้นต่ำ

ผู้ออกหลักทรัพย์โทเคนและผู้ให้บริการที่เกี่ยวข้องควรดำเนินการอย่างน้อย ดังต่อไปนี้

(1) การระบุและประเมินความเสี่ยงของข้อมูลส่วนบุคคล (Personal Data Identification and Privacy Risk Assessment) : ควรระบุประเภทและแหล่งที่มาของข้อมูลส่วนบุคคล รวมถึงข้อมูลที่สามารถเชื่อมโยงหรือระบุตัวบุคคลได้ และควรระบุการเก็บรวบรวม การใช้ การเปิดเผย และการส่งต่อข้อมูลดังกล่าวตามความเหมาะสม พร้อมทั้งประเมินความเสี่ยงด้านความเป็นส่วนตัวโดยคำนึงถึงลักษณะและความอ่อนไหวของข้อมูล วัตถุประสงค์และลักษณะการใช้งาน และผลกระทบที่อาจเกิดขึ้น ทั้งนี้ ควรทบทวนการประเมินความเสี่ยงเมื่อมีการเปลี่ยนแปลงระบบ รูปแบบการใช้ข้อมูล หรือการเชื่อมโยงข้อมูลที่มีนัยสำคัญ

(2) การจำกัดการใช้และการเข้าถึงข้อมูล (Data Minimization and Access Control) : ควรจำกัดการเก็บรวบรวม การใช้ การเปิดเผย และการเข้าถึงข้อมูลส่วนบุคคลให้เท่าที่จำเป็นและสอดคล้องกับวัตถุประสงค์ที่กำหนด โดยควรกำหนดสิทธิการเข้าถึงให้เฉพาะผู้ที่มีความจำเป็นตามบทบาทและหน้าที่ และควรกำหนดมาตรการคุ้มครองข้อมูลให้เหมาะสมกับลักษณะและระดับความเสี่ยงของข้อมูล

(3) การลดความเสี่ยงจากการเปิดเผยและการเชื่อมโยงข้อมูล (Disclosure and Data Linkage Risk Controls) : ควรประเมินความเสี่ยงจากการเปิดเผยหรือการเชื่อมโยงข้อมูลส่วนบุคคลระหว่างข้อมูลที่บันทึกบน DLT ข้อมูลที่จัดเก็บหรือประมวลผลนอก DLT และข้อมูลที่มีการแลกเปลี่ยนหรือเชื่อมโยงระหว่างระบบ ซึ่งอาจทำให้สามารถระบุหรืออนุมานข้อมูลเกี่ยวกับบุคคลได้ และควรกำหนด

มาตรการลดความเสี่ยงตามความเหมาะสม เช่น การแยกข้อมูล การปกปิดข้อมูลบางส่วน การจำกัดรายละเอียดของข้อมูลที่เปิดเผย หรือการจำกัดการเข้าถึงข้อมูลที่สามารถเชื่อมโยงกลับไปยังบุคคลได้

(4) การเปิดเผยข้อมูลต่อบุคคลภายนอกและการตรวจสอบย้อนหลัง (Third-Party Disclosure and Auditability) : ในกรณีที่มีการเปิดเผยหรือแลกเปลี่ยนข้อมูลส่วนบุคคลกับบุคคลภายนอก ควรดำเนินการให้สอดคล้องกับกฎหมายและข้อกำหนดที่เกี่ยวข้อง และกำหนดวัตถุประสงค์ ขอบเขต ผู้รับข้อมูล และมาตรการคุ้มครองข้อมูลให้ชัดเจนและเหมาะสมกับความเสี่ยง รวมทั้งควรบันทึกการเข้าถึง การเปิดเผย และการส่งต่อข้อมูลส่วนบุคคลที่สำคัญ เพื่อให้สามารถติดตามและตรวจสอบย้อนหลังได้

6.5.4 การรับรองความถูกต้องและความน่าเชื่อถือด้วยกลไกการเข้ารหัสลับ (Cryptographic Assurance)

หลักการทั่วไป

ระบบหลักทรัพย์โทเคนควรใช้กลไกการเข้ารหัสลับที่เหมาะสม เพื่อสนับสนุนการพิสูจน์ความถูกต้องและความครบถ้วนของข้อมูลหรือธุรกรรม การยืนยันแหล่งที่มาและผู้มีสิทธิในการดำเนินการ รวมถึงลดความเสี่ยงจากการปลอมแปลงหรือการแก้ไขข้อมูลโดยไม่ได้รับอนุญาต

กลไกการเข้ารหัสลับในหัวข้อนี้ไม่ได้จำกัดเฉพาะการเข้ารหัสข้อมูลเพื่อปกปิดข้อมูล (Encryption) แต่รวมถึงกลไกที่ใช้สนับสนุนการตรวจสอบความถูกต้องและความครบถ้วนของข้อมูล การยืนยันแหล่งที่มาของข้อมูลหรือธุรกรรม และการยืนยันผู้ส่งหรือผู้ดำเนินการ เช่น การใช้ Hash, Digital Signature, Public Key Infrastructure (PKI)[13] หรือกลไกอื่นที่มีวัตถุประสงค์ในลักษณะเดียวกัน

การเลือกใช้และกำหนดกลไกการเข้ารหัสลับควรพิจารณาตามวัตถุประสงค์และลักษณะของการใช้งาน ความสำคัญและความอ่อนไหวของข้อมูลหรือธุรกรรม ระดับความเสี่ยง อายุการใช้งานของข้อมูล และความสามารถในการตรวจสอบและพิสูจน์ย้อนหลังของระบบ รวมทั้งควรคำนึงถึงการเปลี่ยนแปลงของภัยคุกคามและความเหมาะสมของกลไกที่ใช้ตลอดอายุการใช้งาน

ข้อเสนอแนะขั้นต่ำ

ผู้ออกหลักทรัพย์โทเคนและผู้ให้บริการที่เกี่ยวข้องควรดำเนินการอย่างน้อย ดังต่อไปนี้

[13] Public Key Infrastructure (PKI) คือ ระบบสำหรับออก จัดการ และเพิกถอนใบรับรองดิจิทัล เพื่อยืนยันว่ากุญแจสาธารณะเป็นของบุคคลหรือหน่วยงานที่ระบุ

(1) การเลือกใช้กลไกการเข้ารหัสลับ (Selection and Use of Cryptographic Mechanisms) : ควรกำหนดวัตถุประสงค์และความต้องการด้านความมั่นคงปลอดภัยของการใช้กลไกการเข้ารหัสลับให้ชัดเจน และเลือกใช้กลไกที่เหมาะสมกับลักษณะของข้อมูลหรือธุรกรรม ระดับความสำคัญและความเสี่ยง รวมถึงระยะเวลาที่ต้องคงไว้ซึ่งการคุ้มครองหรือการพิสูจน์ข้อมูล โดยพิจารณาความเหมาะสมของวิธีการเข้ารหัส การสร้างและตรวจสอบค่า Hash การลงลายมือชื่อดิจิทัล (Digital Signature) การบริหารจัดการกุญแจเข้ารหัสลับ (Cryptographic Key Management) และกลไกที่เกี่ยวข้องตามวัตถุประสงค์การใช้งาน ทั้งนี้ ควรหลีกเลี่ยงกลไกหรือวิธีการที่ล้าสมัย มีช่องโหว่ หรือไม่เหมาะสมกับระดับความเสี่ยง และควรมีการทบทวนหรือปรับปรุงเมื่อเทคโนโลยี ภัยคุกคาม หรือมาตรฐานด้านความมั่นคงปลอดภัยมีการเปลี่ยนแปลง

ตัวอย่าง :

- กรณีที่มีการจัดเก็บหรือส่งข้อมูลส่วนบุคคล อาจเลือกใช้การเข้ารหัสข้อมูล เช่น AES (Advanced Encryption Standard)[14] โดยกำหนดการบริหารจัดการกุญแจเข้ารหัสลับให้เหมาะสมกับระดับความเสี่ยง
- กรณีที่ต้องตรวจสอบว่าข้อมูลหรือเอกสารสำคัญไม่ได้ถูกเปลี่ยนแปลง อาจใช้ฟังก์ชันแฮช (Cryptographic Hash Function) เช่น SHA-256 (Secure Hash Algorithm 256-bit) เพื่อสร้างค่า Hash สำหรับใช้ตรวจสอบการเปลี่ยนแปลงของข้อมูล
- กรณีที่ต้องส่งคำสั่งหรือธุรกรรมที่มีผลต่อการออก โอน ระงับ หรือเปลี่ยนแปลงสิทธิในหลักทรัพย์โทเคน อาจใช้การลงลายมือชื่อดิจิทัล (Digital Signature) เช่น ECDSA (Elliptic Curve Digital Signature Algorithm) ร่วมกับคู่กุญแจส่วนตัวและกุญแจสาธารณะ (Private/Public Key Pair) เพื่อสนับสนุนการยืนยันผู้ลงนามและตรวจสอบว่าข้อมูลที่ลงลายมือชื่อไม่ได้ถูกแก้ไข

(2) การตรวจสอบความถูกต้องและแหล่งที่มาของข้อมูลหรือธุรกรรม (Integrity and Authenticity Verification) : ควรจัดให้มีกระบวนการและกลไกสำหรับตรวจสอบ

[14] Advanced Encryption Standard (AES) คือ มาตรฐานการเข้ารหัสเพื่อรักษาความลับของข้อมูล โดยใช้กุญแจเดียวกันในการเข้ารหัสและถอดรหัส รองรับกุญแจขนาด 128, 192 และ 256 บิต

ความถูกต้องและความครบถ้วนของข้อมูล เอกสาร ข้อความ หรือธุรกรรมสำคัญ รวมถึงตรวจสอบว่าข้อมูลดังกล่าวไม่ได้ถูกแก้ไขโดยไม่ได้รับอนุญาต และสามารถยืนยันแหล่งที่มาหรือผู้ลงลายมือชื่อได้ตามความเหมาะสม โดยควรกำหนดวิธีการตรวจสอบและเงื่อนไขที่เกี่ยวข้องกับกลไกที่ใช้ เช่น การตรวจสอบค่า Hash การตรวจสอบ Digital Signature และ Certificate หรือข้อมูลอ้างอิงอื่นที่เกี่ยวข้องให้ชัดเจนและสามารถตรวจสอบได้

(3) การจัดเก็บหลักฐานและการทบทวนความเหมาะสม (Evidence Retention and Review) : ควรจัดเก็บข้อมูลและหลักฐานที่จำเป็นต่อการตรวจสอบและยืนยันความถูกต้องของข้อมูลหรือธุรกรรมที่เกี่ยวข้องกับการใช้กลไกการเข้ารหัสลับให้ครบถ้วน และสามารถตรวจสอบย้อนหลังได้ โดยเฉพาะกรณีที่กลไกดังกล่าวมีผลต่อสิทธิ สถานะ หรือธุรกรรมของผู้ถือหลักทรัพย์โทเคน ทั้งนี้ ควรทบทวนความเหมาะสมของกลไกการเข้ารหัสลับและมาตรการที่เกี่ยวข้องเป็นระยะ โดยคำนึงถึงการเปลี่ยนแปลงของความเสี่ยง เทคโนโลยี ภัยคุกคาม และมาตรฐานด้านความมั่นคงปลอดภัย และควรปรับปรุงมาตรการตามความเหมาะสม

6.6 การติดตามเหตุการณ์ การบันทึกข้อมูล และการตรวจสอบย้อนหลัง (Monitoring, Logging and Auditability)

ระบบที่เกี่ยวข้องกับหลักทรัพย์โทเคนควรจัดให้มีกลไกการติดตามและบันทึกเหตุการณ์ การดำเนินการ และข้อมูลที่สำคัญอย่างเหมาะสม เพื่อให้สามารถตรวจพบความผิดปกติ ระบุผู้ดำเนินการและรายละเอียดของการดำเนินการ ตรวจสอบผลที่เกิดขึ้น และใช้เป็นหลักฐานในการตรวจสอบหรือพิสูจน์ข้อเท็จจริงย้อนหลังได้ ทั้งนี้ การติดตามและบันทึกควรครอบคลุมเหตุการณ์หรือการดำเนินการที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัย ความถูกต้องครบถ้วนของข้อมูล การทำงานของระบบ ธุรกรรม หรือสิทธิของผู้ถือหลักทรัพย์โทเคน

การดำเนินการตามหัวข้อนี้ควรครอบคลุมระบบและองค์ประกอบที่เกี่ยวข้องกับการให้บริการหลักทรัพย์โทเคน รวมถึงระบบหรือบริการที่มีการเชื่อมโยงหรือพึ่งพากัน โดยพิจารณาให้ครอบคลุมทั้งการดำเนินการของผู้ใช้งานและผู้ดูแลระบบ การใช้สิทธิพิเศษ การเปลี่ยนแปลงระบบหรือข้อมูล เหตุการณ์ด้านความมั่นคงปลอดภัย และธุรกรรมหรือการดำเนินการที่มีนัยสำคัญต่อหลักทรัพย์โทเคน ทั้งนี้ ขอบเขตและระดับของการติดตามและบันทึกควรสอดคล้องกับความสำคัญและระดับความเสี่ยง

ข้อมูลบันทึกและหลักฐานควรมีความครบถ้วน ถูกต้อง และสามารถเชื่อมโยงเหตุการณ์ที่เกี่ยวข้องกันได้ รวมทั้งควรได้รับการป้องกันจากการแก้ไข ลบ หรือเข้าถึงโดยไม่ได้รับอนุญาต และสามารถสืบค้นและนำมาใช้เพื่อสนับสนุนการตรวจสอบ การวิเคราะห์เหตุการณ์ และการตอบสนองต่อเหตุการณ์ได้ภายในระยะเวลาที่เหมาะสม โดยควรกำหนดระยะเวลาการเก็บรักษาและทบทวนความเพียงพอของการติดตามและบันทึกให้สอดคล้องกับความเสี่ยงและข้อกำหนดที่เกี่ยวข้อง

6.6.1 การบันทึกข้อมูล การตรวจสอบย้อนหลัง และการบริหารจัดการหลักฐาน (Logging, Audit Trail and Evidence Management)

หลักการทั่วไป

ระบบที่เกี่ยวข้องกับหลักทรัพย์โทเคนควรมีการบันทึกเหตุการณ์และการดำเนินการที่สำคัญอย่างเพียงพอ เพื่อให้สามารถตรวจสอบและตรวจสอบย้อนหลังได้ว่า ใครเป็นผู้ดำเนินการ ดำเนินการอะไร เมื่อใด ผ่านระบบหรือช่องทางใด และเกิดผลอย่างไร ต่อระบบ ข้อมูล ธุรกรรม หรือหลักทรัพย์โทเคน

การบันทึกข้อมูลควรครอบคลุมเหตุการณ์และการดำเนินการที่มีนัยสำคัญต่อ ความมั่นคงปลอดภัย การทำงานของระบบ ความถูกต้องครบถ้วนของข้อมูล ธุรกรรม และสิทธิของผู้ถือหลักทรัพย์โทเคน โดยกำหนดขอบเขตของการบันทึกให้สอดคล้องกับความสำคัญและระดับความเสี่ยงของระบบและการดำเนินงาน

ข้อมูลบันทึกและหลักฐานควรมีความครบถ้วน ถูกต้อง และน่าเชื่อถือ สามารถเชื่อมโยงและสืบค้นเหตุการณ์ที่เกี่ยวข้องกันได้ และควรได้รับการป้องกันจากการแก้ไข ลบ หรือเข้าถึงโดยไม่ได้รับอนุญาต เพื่อให้สามารถนำมาใช้สนับสนุนการตรวจสอบ การวิเคราะห์เหตุการณ์ การตอบสนองต่อเหตุการณ์ หรือการพิสูจน์ข้อเท็จจริงย้อนหลังได้ตามความเหมาะสม

ข้อเสนอแนะขั้นต่ำ

ผู้ออกหลักทรัพย์โทเคนและผู้ให้บริการที่เกี่ยวข้องควรดำเนินการอย่างน้อย ดังต่อไปนี้

(1) การกำหนดขอบเขตและรายละเอียดของข้อมูลบันทึก (Logging Scope and Content) : ควรกำหนดประเภทของเหตุการณ์ การดำเนินการ ระบบ ข้อมูล และฟังก์ชันสำคัญที่เกี่ยวข้องกับหลักทรัพย์โทเคนซึ่งต้องมีการบันทึก โดยครอบคลุมอย่างน้อยเหตุการณ์ด้านความมั่นคงปลอดภัย การเข้าถึงระบบและข้อมูลสำคัญ การเปลี่ยนแปลงสิทธิหรือการตั้งค่า การดำเนินการของผู้ดูแลระบบและผู้มีสิทธิพิเศษ ตลอดจนกิจกรรมสำคัญที่เกี่ยวข้องกับ Smart Contract หรือระบบ DLT ทั้งนี้ ข้อมูลที่บันทึกควรเพียงพอต่อการระบุผู้ดำเนินการ ช่วงเวลาที่เกิดเหตุการณ์ ระบบ

หรือช่องทางที่เกี่ยวข้อง รายละเอียดและผลของการดำเนินการ เพื่อให้สามารถตรวจสอบและตรวจสอบย้อนหลังได้อย่างเหมาะสม

(2) การคุ้มครองและจัดเก็บข้อมูลบันทึกและหลักฐาน (Log and Evidence Protection and Retention) : ควรจัดให้ข้อมูลบันทึกและหลักฐานมีการระบุเวลาที่ถูกต้องและสอดคล้องกันระหว่างระบบที่เกี่ยวข้อง เพื่อให้สามารถเชื่อมโยงเหตุการณ์ได้อย่างเหมาะสม พร้อมทั้งป้องกันการแก้ไข ลบ หรือเข้าถึงโดยไม่ได้รับอนุญาต และกำหนดการแบ่งแยกสิทธิระหว่างผู้ใช้งานระบบกับผู้ที่มีหน้าที่บริหารจัดการข้อมูลบันทึกตามความเหมาะสม นอกจากนี้ ควรกำหนดระยะเวลาและวิธีการเก็บรักษาข้อมูลบันทึกและหลักฐานให้สอดคล้องกับความสำคัญของข้อมูล ระดับความเสี่ยง และกฎหมายหรือข้อกำหนดที่เกี่ยวข้อง เพื่อให้สามารถนำข้อมูลดังกล่าวมาใช้ตรวจสอบหรือพิสูจน์ข้อเท็จจริงได้เมื่อจำเป็น

(3) การสืบค้น การเรียกใช้ และการทบทวนข้อมูลบันทึกและหลักฐาน (Retrieval, Use and Review) : ควรจัดให้สามารถสืบค้น เชื่อมโยง และเรียกใช้ข้อมูลบันทึกหรือหลักฐานที่เกี่ยวข้องได้ภายในระยะเวลาที่เหมาะสม เพื่อสนับสนุนการตรวจสอบ การวิเคราะห์เหตุการณ์ การตอบสนองต่อเหตุการณ์ และการให้ข้อมูลแก่หน่วยงานที่เกี่ยวข้อง รวมทั้งควรทบทวนความครบถ้วน ความถูกต้อง และความเพียงพอของการบันทึกข้อมูลเป็นระยะ และปรับปรุงเมื่อมีการเปลี่ยนแปลงระบบ ความเสี่ยง หรือข้อกำหนดที่มีนัยสำคัญ

6.6.2 การติดตามและตรวจจับเหตุการณ์ผิดปกติ (Monitoring and Detection)

หลักการทั่วไป

นอกจากการบันทึกข้อมูลและหลักฐานแล้ว ระบบที่เกี่ยวข้องกับหลักทรัพย์โทเคนควรจัดให้มีกลไกการติดตามและตรวจจับเหตุการณ์ที่อาจส่งผลกระทบต่อ ความมั่นคงปลอดภัย ความถูกต้องครบถ้วนของข้อมูล ความพร้อมใช้งานของระบบ การดำเนินงาน หรือสิทธิของผู้ถือหลักทรัพย์โทเคนอย่างเหมาะสมและสอดคล้องกับระดับความเสี่ยง

การติดตามและตรวจจับควรครอบคลุมเหตุการณ์หรือรูปแบบการดำเนินงานที่มีนัยสำคัญ โดยพิจารณาทั้งเหตุการณ์ที่เกิดขึ้นภายในระบบและเหตุการณ์ที่เกิดจากการเชื่อมโยงหรือพึ่งพาระหว่างระบบ ทั้งนี้ ขอบเขตและระดับของการติดตามและตรวจจับควรสอดคล้องกับความสำคัญและระดับความเสี่ยงของระบบและการดำเนินงาน

ระบบควรสามารถแจ้งเตือนเมื่อพบเหตุการณ์หรือพฤติกรรมที่ผิดปกติหรือมีนัยสำคัญ และมีกระบวนการในการประเมิน ตรวจสอบ และยกระดับเหตุการณ์ตามความเหมาะสม เพื่อให้ผู้รับผิดชอบสามารถประเมินผลกระทบและดำเนินการตอบสนองได้อย่างทันท่วงที

ข้อเสนอแนะขั้นต่ำ

ผู้ออกหลักทรัพย์โทเคนและผู้ให้บริการที่เกี่ยวข้องควรดำเนินการอย่างน้อย ดังต่อไปนี้

(1) การกำหนดขอบเขตและเกณฑ์การติดตาม (Monitoring Scope and Detection Criteria) : ควรกำหนดระบบ องค์ประกอบ เหตุการณ์ และสัญญาณที่ต้องติดตามและตรวจจับ โดยพิจารณาจากความสำคัญและระดับความเสี่ยง และให้ครอบคลุมอย่างน้อย สถานะและความพร้อมใช้งานของระบบ เหตุการณ์ด้านความมั่นคงปลอดภัย ตลอดจนธุรกรรมหรือการดำเนินการที่มีนัยสำคัญต่อหลักทรัพย์โทเคน เช่น การเข้าถึงระบบหรือการใช้สิทธิพิเศษที่ผิดปกติ การเปลี่ยนแปลงการตั้งค่าที่มีนัยสำคัญ การเรียกใช้ฟังก์ชันสำคัญของ Smart Contract การเปลี่ยนแปลงสถานะของโทเคน หรือธุรกรรมที่มีรูปแบบผิดปกติ รวมถึงสัญญาณที่อาจบ่งชี้ถึงความผิดปกติของระบบหรือองค์ประกอบที่มีนัยสำคัญ เช่น DLT Infrastructure, API, Oracle หรือ Bridge เป็นต้น ทั้งนี้ ขอบเขตและเกณฑ์การติดตามควรสอดคล้องกับผลกระทบที่อาจเกิดขึ้นต่อระบบ ข้อมูล ธุรกรรม หรือสิทธิของผู้ถือหลักทรัพย์โทเคน

(2) การแจ้งเตือน การวิเคราะห์ และการยกระดับเหตุการณ์ (Alerting, Analysis and Escalation) : ควรกำหนดเกณฑ์และระดับความรุนแรงของการแจ้งเตือนให้เหมาะสมกับลักษณะและผลกระทบของเหตุการณ์ รวมทั้งกำหนดผู้รับผิดชอบและขั้นตอนในการตรวจสอบ วิเคราะห์ และยกระดับเหตุการณ์อย่างชัดเจน โดยควรสามารถเชื่อมโยงข้อมูลจาก Log และแหล่งข้อมูลที่เกี่ยวข้อง เพื่อช่วยประเมินลักษณะและผลกระทบของเหตุการณ์ แยกแยะเหตุการณ์ที่อาจเป็นความผิดปกติออกจากการดำเนินงานตามปกติ และสนับสนุนการดำเนินการตอบสนองได้อย่างทันท่วงที

(3) การบันทึกและทบทวนประสิทธิผลของการติดตาม (Record Keeping and Monitoring Effectiveness Review) : ควรบันทึกผลการแจ้งเตือน

การตรวจสอบ การวิเคราะห์ และการดำเนินการต่อเหตุการณ์ที่มีนัยสำคัญ เพื่อให้สามารถตรวจสอบและตรวจสอบย้อนหลังได้ รวมทั้งควรทบทวนขอบเขตการติดตาม เกณฑ์การตรวจจับและแจ้งเตือน และกระบวนการยกระดับเหตุการณ์เป็นระยะ และเมื่อมีการเปลี่ยนแปลงระบบ ความเสี่ยง หรือเหตุการณ์ที่มีนัยสำคัญ เพื่อให้การติดตามและตรวจจับยังคงมีประสิทธิผล และสามารถตรวจพบเหตุการณ์สำคัญได้อย่างเหมาะสมโดยไม่ก่อให้เกิดการแจ้งเตือนที่ไม่จำเป็นมากเกินไป

6.7 การบริหารจัดการช่องโหว่และการทดสอบด้านความมั่นคงปลอดภัย (Vulnerability Management and Security Testing)

ระบบ แอปพลิเคชัน Smart Contract และองค์ประกอบที่เกี่ยวข้องกับหลักทรัพย์โทเคนควรได้รับการบริหารจัดการและประเมินด้านความมั่นคงปลอดภัยอย่างเหมาะสม เพื่อให้สามารถค้นหาและระบุช่องโหว่ ประเมินความเสี่ยง ทดสอบประสิทธิผลของมาตรการควบคุม และระบุข้อบกพร่องที่อาจส่งผลกระทบต่อระบบ ข้อมูล ธุรกรรม หรือสิทธิของผู้ถือหลักทรัพย์โทเคนได้อย่างเหมาะสมและทันท่วงที

การบริหารจัดการตามหัวข้อนี้ควรดำเนินการอย่างเป็นระบบและต่อเนื่อง โดยครอบคลุมการค้นหาและจัดการช่องโหว่ และการทดสอบด้านความมั่นคงปลอดภัย ทั้งนี้ ขอบเขต วิธีการ และความถี่ของการดำเนินการควรกำหนดตามลักษณะ ความสำคัญ การเปลี่ยนแปลง และระดับความเสี่ยงของระบบ รวมถึงความเสี่ยงที่เกิดจากการเชื่อมโยงหรือพึ่งพาระหว่างระบบและองค์ประกอบที่เกี่ยวข้อง

ผลจากการประเมินและทดสอบควรถูกนำไปใช้ในการจัดลำดับความสำคัญของความเสี่ยง กำหนดและดำเนินการแก้ไขหรือลดความเสี่ยง รวมถึงติดตามผลการดำเนินการอย่างเหมาะสม และควรจัดเก็บข้อมูลและหลักฐานที่เกี่ยวข้องให้สามารถติดตามและตรวจสอบย้อนหลังได้ เพื่อสนับสนุนการปรับปรุงมาตรการควบคุมอย่างต่อเนื่อง

6.7.1 การบริหารจัดการช่องโหว่ (Vulnerability Management)

หลักการทั่วไป

ช่องโหว่ของระบบหรือองค์ประกอบที่เกี่ยวข้องกับหลักทรัพย์โทเคนควรได้รับการบริหารจัดการตามระดับความเสี่ยง โดยพิจารณาถึงความรุนแรงของช่องโหว่ ความเป็นไปได้ในการถูกโจมตี และผลกระทบที่อาจเกิดขึ้นต่อระบบ ข้อมูล ธุรกรรม สิทธิของผู้ถือหลักทรัพย์โทเคน หรือความต่อเนื่องของการให้บริการ

การบริหารจัดการช่องโหว่ควรครอบคลุมการค้นหาและระบุช่องโหว่ การประเมินความเสี่ยง การจัดลำดับความสำคัญ การแก้ไขหรือลดความเสี่ยง และการติดตามผล โดยขอบเขตและความถี่

ของการดำเนินการควรเหมาะสมกับลักษณะ ความสำคัญ และระดับความเสี่ยงของระบบ รวมถึงการเปลี่ยนแปลงที่มีนัยสำคัญหรือข้อมูลเกี่ยวกับช่องโหว่ใหม่ที่อาจส่งผลกระทบต่อระบบ

ช่องโหว่ที่ไม่สามารถแก้ไขได้ในทันทีควรมีมาตรการเพื่อลดความเสี่ยงหรือมาตรการควบคุมทดแทนที่เหมาะสม และควรมีหลักฐานแสดงการประเมิน การดำเนินการ และสถานะของช่องโหว่เพื่อให้สามารถติดตามและตรวจสอบย้อนหลังได้

ข้อเสนอแนะขั้นต่ำ

ผู้ออกหลักทรัพย์โทเคนและผู้ให้บริการที่เกี่ยวข้องควรดำเนินการอย่างน้อย ดังต่อไปนี้

(1) การกำหนดกระบวนการและขอบเขตการบริหารจัดการช่องโหว่ (Vulnerability Management Process and Scope) : ควรจัดให้มีกระบวนการบริหารจัดการช่องโหว่ที่เป็นลายลักษณ์อักษร โดยกำหนดขอบเขตให้ครอบคลุมระบบและองค์ประกอบทางเทคโนโลยีที่ใช้ในการออก การถือครอง การโอน การบันทึก หรือการบริหารจัดการหลักทรัพย์โทเคน รวมถึงระบบหรือองค์ประกอบที่มีการเชื่อมต่อหรือพึ่งพาซึ่งหากเกิดช่องโหว่อาจส่งผลกระทบอย่างมีนัยสำคัญต่อความมั่นคงปลอดภัย ความถูกต้องครบถ้วนของข้อมูล ธุรกรรม สิทธิของผู้ถือหลักทรัพย์โทเคน หรือความต่อเนื่องของการให้บริการ โดยควรครอบคลุมทั้งระบบบน DLT ระบบที่ทำงานนอก DLT และระบบหรือองค์ประกอบที่เชื่อมต่อหรือพึ่งพาระบบดังกล่าว เช่น Smart Contract, DLT Infrastructure, Wallet หรือ Custody System, Key Management System, ระบบจัดการตัวตนและสิทธิการเข้าถึง (Identity and Access Management), ระบบที่เชื่อมต่อผ่าน API, Oracle, Bridge และระบบสนับสนุนอื่นใดที่มีนัยสำคัญ

กระบวนการบริหารจัดการช่องโหว่ควรครอบคลุมการค้นหาและระบุช่องโหว่ การประเมินความเสี่ยง การจัดลำดับความสำคัญ การแก้ไขหรือลดความเสี่ยง และการติดตามผล โดยควรมีการประเมินช่องโหว่ของ **ระบบและองค์ประกอบที่มีความสำคัญอย่างน้อยปีละหนึ่งครั้ง** และควรดำเนินการเพิ่มเติมเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ หรือมีข้อมูลเกี่ยวกับช่องโหว่หรือภัยคุกคามใหม่ที่อาจส่งผลกระทบต่อระบบ

(2) การประเมินและจัดการช่องโหว่ตามระดับความเสี่ยง (Risk-based Vulnerability Assessment and Remediation) : ควรประเมินช่องโหว่

โดยพิจารณาอย่างน้อยถึงความรุนแรงของช่องโหว่ ความเป็นไปได้ในการถูกโจมตี และผลกระทบที่อาจเกิดขึ้นต่อความมั่นคงปลอดภัยของระบบ ข้อมูล ธุรกรรม สิทธิของผู้ถือหลักทรัพย์โทเคน และความต่อเนื่องของการให้บริการ เพื่อจัดลำดับความสำคัญของช่องโหว่และกำหนดแนวทางและกรอบระยะเวลาในการดำเนินการที่เหมาะสมกับระดับความเสี่ยง

ช่องโหว่ที่ตรวจพบควรได้รับการแก้ไขหรือลดความเสี่ยงภายในระยะเวลาที่เหมาะสมตามระดับความเสี่ยง หรือจัดให้มีมาตรการควบคุมทดแทน (Compensating Controls) ที่มีประสิทธิผลในกรณีที่ไม่สามารถแก้ไขได้ทันที ทั้งนี้ การยอมรับความเสี่ยง (Risk Acceptance) ควรได้รับการอนุมัติจากผู้มีอำนาจตามที่องค์กรกำหนด และควรมีเหตุผลและเงื่อนไขในการยอมรับความเสี่ยงที่ชัดเจน

(3) การติดตามและตรวจสอบย้อนหลัง (Tracking and Auditability) : ควรจัดให้มีการติดตามสถานะของช่องโหว่ที่ตรวจพบจนกว่าจะได้รับการแก้ไข ลดความเสี่ยง หรือมีการยอมรับความเสี่ยงตามกระบวนการที่กำหนด โดยควรกำหนดผู้รับผิดชอบและสถานะการดำเนินการที่ชัดเจน เพื่อให้สามารถติดตามความคืบหน้าและมั่นใจได้ว่าช่องโหว่ได้รับการจัดการตามระดับความเสี่ยง

ควรจัดเก็บหลักฐานที่เกี่ยวข้องกับการบริหารจัดการช่องโหว่ให้ครบถ้วนและสามารถตรวจสอบย้อนหลังได้ เช่น รายละเอียดและสถานะของช่องโหว่ ผลการประเมินความเสี่ยง การดำเนินการแก้ไขหรือมาตรการควบคุมทดแทน และการอนุมัติการยอมรับความเสี่ยง ทั้งนี้ ควรป้องกันหลักฐานดังกล่าวจากการแก้ไข ลบ หรือทำลายโดยไม่ได้รับอนุญาต และจัดเก็บไว้ตามระยะเวลาที่เหมาะสมกับระดับความเสี่ยงและข้อกำหนดที่เกี่ยวข้อง

6.7.2 การทดสอบด้านความมั่นคงปลอดภัย (Security Testing)

หลักการทั่วไป

ระบบที่เกี่ยวข้องกับหลักทรัพย์โทเคนควรได้รับการทดสอบด้านความมั่นคงปลอดภัย (Security Testing) อย่างเหมาะสม เพื่อประเมินประสิทธิผลของมาตรการควบคุมด้านความมั่นคงปลอดภัยและความสามารถของระบบในการป้องกัน ตรวจจับ และรองรับการโจมตีหรือเหตุการณ์ด้านความมั่นคงปลอดภัย

การทดสอบควรครอบคลุมระบบและองค์ประกอบที่มีนัยสำคัญต่อการให้บริการหลักทรัพย์โทเคน โดยกำหนดขอบเขตและวิธีการทดสอบให้เหมาะสมกับลักษณะ ความสำคัญ และระดับความเสี่ยงของระบบ รวมถึงความเสี่ยงจากการเชื่อมต่อหรือพึ่งพาระบบและบริการอื่นที่เกี่ยวข้อง

ผลการทดสอบควรได้รับการนำมาพิจารณาในการปรับปรุงมาตรการควบคุมด้านความมั่นคงปลอดภัยและการบริหารจัดการความเสี่ยงของระบบอย่างต่อเนื่อง โดยคำนึงถึงผลกระทบที่อาจเกิดขึ้นต่อระบบ ข้อมูล ธุรกรรม สิทธิของผู้ถือหลักทรัพย์โทเคน และความต่อเนื่องของการให้บริการ

ข้อเสนอแนะขั้นต่ำ

ผู้ออกหลักทรัพย์โทเคนและผู้ให้บริการที่เกี่ยวข้องควรดำเนินการอย่างน้อย ดังต่อไปนี้

(1) การกำหนดขอบเขตและแนวทางการทดสอบ (Security Testing Scope and Approach) : ควรจัดให้มีการทดสอบด้านความมั่นคงปลอดภัย (Security Testing) โดยกำหนดวัตถุประสงค์และขอบเขตการทดสอบให้เหมาะสมกับลักษณะ ความสำคัญ และระดับความเสี่ยงของระบบ โดยการทดสอบอาจใช้วิธีการที่หลากหลายตามวัตถุประสงค์และลักษณะของระบบ เช่น การตรวจสอบการตั้งค่าด้านความมั่นคงปลอดภัย (Security Configuration Review) การตรวจสอบ Source Code หรือ Smart Contract และการทดสอบประสิทธิผลของมาตรการควบคุมด้านความมั่นคงปลอดภัย (Security Control Testing)

ขอบเขตการทดสอบควรครอบคลุมระบบและองค์ประกอบทางเทคโนโลยีที่มีนัยสำคัญต่อการให้บริการหลักทรัพย์โทเคน ทั้งระบบที่ทำงานบน DLT ระบบที่ทำงานนอก DLT และระบบหรือองค์ประกอบที่มีการเชื่อมต่อหรือพึ่งพาระบบดังกล่าว โดยควรพิจารณาถึงจุดเชื่อมต่อ ช่องทางการเข้าถึง และความสัมพันธ์ระหว่างระบบที่อาจทำให้เกิดช่องทางการโจมตีหรือส่งผลกระทบต่อระบบข้อมูล ธุรกรรม หรือสิทธิของผู้ถือหลักทรัพย์โทเคน เช่น Smart Contract, DLT Infrastructure, Application, API, Wallet หรือ Custody System, Key Management System, ระบบบริหารจัดการตัวตนและสิทธิการเข้าถึง (Identity and Access Management), Oracle, Bridge และระบบหรือบริการภายนอกที่มีนัยสำคัญ

นอกจากนี้ ควรจัดให้มีการทดสอบแบบจำลองการโจมตี (Penetration Testing)[15] อย่างน้อยปีละหนึ่งครั้ง สำหรับระบบและองค์ประกอบที่มีนัยสำคัญต่อการให้บริการหลักทรัพย์โทเคน และควรดำเนินการเพิ่มเติมเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ หรือเมื่อมีเหตุหรือข้อมูลใหม่ที่อาจส่งผลให้ระดับความเสี่ยงของระบบเปลี่ยนแปลงอย่างมีนัยสำคัญ โดยควรกำหนดขอบเขตและแนวทางการทดสอบให้เหมาะสมกับลักษณะและระดับความเสี่ยงของระบบ รวมทั้งสถานการณ์การโจมตีที่ต้องการจำลอง

ตัวอย่าง : การทดสอบแบบ Black-box อาจเหมาะสำหรับการจำลองการโจมตีจากผู้โจมตีภายนอกที่มีข้อมูลเกี่ยวกับระบบอย่างจำกัด / การทดสอบแบบ Grey-box อาจเหมาะสำหรับการจำลองการโจมตีโดยผู้ที่มีข้อมูลหรือสิทธิในการเข้าถึงระบบบางส่วน / การทดสอบแบบ White-box อาจเหมาะสำหรับการประเมินจุดอ่อนเชิงลึกโดยผู้ทดสอบได้รับข้อมูลเกี่ยวกับโครงสร้างหรือการทำงานภายในของระบบ ทั้งนี้ การเลือกใช้รูปแบบการทดสอบควรสอดคล้องกับวัตถุประสงค์และสถานการณ์การโจมตีที่ต้องการประเมิน และอาจใช้หลายรูปแบบร่วมกันได้ตามความเหมาะสม

(2) การดำเนินการทดสอบและการควบคุมผลกระทบ (Security Testing and Impact Control) : ควรดำเนินการทดสอบโดยผู้ที่มีความรู้ ความสามารถ และประสบการณ์ที่เหมาะสมกับลักษณะและระดับความเสี่ยงของการทดสอบ และควรมีความเป็นอิสระจากการออกแบบ พัฒนา หรือดูแลระบบและมาตรการควบคุมที่นำมาทดสอบ เพื่อให้ผลการทดสอบมีความเป็นกลางและน่าเชื่อถือ ทั้งนี้ อาจดำเนินการโดยบุคลากรภายในองค์กรหรือบุคคลภายนอกก็ได้ โดยผู้ทดสอบภายในควรมีการแยกหน้าที่และไม่มีส่วนรับผิดชอบโดยตรงต่อระบบหรือมาตรการควบคุมที่ตนเองทดสอบ

การทดสอบควรครอบคลุมการประเมินมาตรการควบคุมด้านความมั่นคงปลอดภัยที่สำคัญของระบบตามลักษณะและความเสี่ยงที่เกี่ยวข้อง เช่น การควบคุมการยืนยัน

[15] Penetration Testing คือ การทดสอบเจาะระบบภายใต้ขอบเขตที่กำหนด โดยใช้วิธีการเสมือนผู้โจมตี เพื่อค้นหาและประเมินช่องโหว่ที่อาจนำไปใช้โจมตีระบบได้จริง

ตัวตนและสิทธิการเข้าถึง การจัดการสิทธิพิเศษ การควบคุมการตั้งค่าระบบ การป้องกันข้อมูล การเชื่อมต่อและการรับส่งข้อมูลระหว่างระบบ ตลอดจนการทำงานของ Application และ Smart Contract หรือฟังก์ชันที่มีผลต่อธุรกรรมและสิทธิของผู้ถือหลักทรัพย์โทเคน โดยควรทดสอบให้สามารถระบุจุดอ่อนหรือข้อบกพร่องของมาตรการควบคุม และประเมินผลกระทบที่อาจเกิดขึ้นได้

ก่อนดำเนินการทดสอบควรกำหนดเงื่อนไขและขอบเขตการปฏิบัติงาน (Rules of Engagement) ให้ชัดเจน โดยอย่างน้อยควรกำหนดระบบและข้อมูลที่อยู่ในขอบเขต วิธีการและข้อจำกัดในการทดสอบ ช่วงเวลาที่อนุญาตให้ทดสอบ และผู้มีอำนาจอนุมัติการทดสอบ รวมทั้งควรจัดให้มีมาตรการควบคุมเพื่อป้องกันหรือลดผลกระทบต่อระบบที่ให้บริการจริง ข้อมูล ธุรกรรม ผู้ใช้งาน หรือสิทธิของผู้ถือหลักทรัพย์โทเคน และกำหนดแนวทางในการระงับหรือยุติการทดสอบเมื่อพบว่าการทดสอบอาจก่อให้เกิดผลกระทบอย่างมีนัยสำคัญ

(3) การรายงาน การแก้ไข และการติดตามผล (Reporting, Remediation and Follow-up) : ควรจัดทำรายงานผลการทดสอบด้านความมั่นคงปลอดภัย โดยระบุขอบเขตและวิธีการทดสอบ ข้อค้นพบหรือข้อบกพร่องที่ตรวจพบ ระดับความเสี่ยงและผลกระทบที่อาจเกิดขึ้น รวมถึงข้อเสนอแนะในการแก้ไขหรือลดความเสี่ยง และควรกำหนดผู้รับผิดชอบและแนวทางการดำเนินการที่เหมาะสมกับระดับความเสี่ยงของข้อค้นพบ

ข้อค้นพบที่มีนัยสำคัญควรได้รับการแก้ไขหรือลดความเสี่ยงภายในระยะเวลาที่เหมาะสมตามระดับความเสี่ยง หรือจัดให้มีมาตรการควบคุมทดแทน (Compensating Controls) ที่มีประสิทธิผลในกรณีที่ไม่สามารถแก้ไขได้ทันที ทั้งนี้ การยอมรับความเสี่ยง (Risk Acceptance) ควรได้รับการอนุมัติจากผู้มีอำนาจตามที่องค์กรกำหนด และควรมีเหตุผลและเงื่อนไขในการยอมรับความเสี่ยงที่ชัดเจน

นอกจากนี้ ควรติดตามการดำเนินการแก้ไขหรือลดความเสี่ยงจนแล้วเสร็จ และควรตรวจสอบผลการแก้ไขสำหรับข้อค้นพบที่มีนัยสำคัญ เพื่อให้มั่นใจว่ามาตรการที่ดำเนินการสามารถจัดการความเสี่ยงได้อย่างเหมาะสม รวมทั้งควรจัดเก็บรายงาน

และหลักฐานที่เกี่ยวข้องกับการทดสอบและการดำเนินการแก้ไขไว้ให้สามารถตรวจสอบย้อนหลังได้

6.8 การตอบสนองต่อเหตุการณ์และความพร้อมด้านการดำเนินงาน (Incident Response and Operational Resilience)

ระบบและบริการที่เกี่ยวข้องกับหลักทรัพย์โทเคนควรมีความสามารถในการเตรียมความพร้อมและตอบสนองต่อเหตุการณ์ที่อาจกระทบต่อความมั่นคงปลอดภัย การทำงานของระบบ ข้อมูล ธุรกรรม หรือสิทธิของผู้ถือหลักทรัพย์โทเคน รวมถึงความสามารถในการกู้คืนระบบและข้อมูลและรักษาความต่อเนื่องของการให้บริการที่สำคัญได้อย่างเหมาะสมและภายในระดับที่ยอมรับได้

หัวข้อนี้ครอบคลุมการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย ความต่อเนื่องในการดำเนินงาน และการสำรองข้อมูลและกู้คืนระบบ โดยครอบคลุมระบบและองค์ประกอบที่มีความสำคัญต่อการให้บริการหลักทรัพย์โทเคน รวมถึงระบบหรือบริการที่มีการเชื่อมโยงหรือพึ่งพากัน

การกำหนดมาตรการตามหัวข้อนี้ควรพิจารณาตามลักษณะและระดับความสำคัญของระบบและบริการ ผลกระทบที่อาจเกิดขึ้นต่อผู้ถือหลักทรัพย์โทเคน ความต่อเนื่องของการให้บริการ ความถูกต้องครบถ้วนของข้อมูล และข้อกำหนดด้านกฎหมายหรือการกำกับดูแลที่เกี่ยวข้อง

6.8.1 การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย (Incident Response)

หลักการทั่วไป

เมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย ผู้เกี่ยวข้องควรสามารถระบุและประเมินเหตุการณ์ ดำเนินมาตรการควบคุมและลดผลกระทบ รวมทั้งดำเนินการแก้ไขและจัดการเหตุการณ์ได้อย่างเหมาะสม เพื่อจำกัดผลกระทบต่อระบบ ข้อมูล ธุรกรรม และสิทธิของผู้ถือหลักทรัพย์โทเคน

กระบวนการบริหารจัดการเหตุการณ์ต้องครอบคลุมการรับแจ้งหรือค้นพบเหตุการณ์ การประเมินความรุนแรงและผลกระทบ การยกระดับการดำเนินการ การควบคุมและลดผลกระทบ การสื่อสารและประสานงานกับผู้เกี่ยวข้อง การแจ้งหน่วยงานที่เกี่ยวข้องตามข้อกำหนด ตลอดจนการเก็บรักษาข้อมูลและหลักฐานที่เกี่ยวข้อง และการทบทวนเหตุการณ์และผลการดำเนินการภายหลังเกิดเหตุ

ทั้งนี้ ควรจัดให้มีแผนและกระบวนการบริหารจัดการเหตุการณ์ที่เหมาะสมกับลักษณะและระดับความสำคัญของระบบและบริการ และควรทดสอบและทบทวนแผนและกระบวนการดังกล่าวเป็นระยะ รวมทั้งเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ เพื่อให้สามารถนำไปใช้ในการตอบสนองต่อเหตุการณ์ได้อย่างมีประสิทธิผล

ข้อเสนอแนะขั้นต่ำ

ผู้ออกหลักทรัพย์โทเคนและผู้ให้บริการที่เกี่ยวข้องควรดำเนินการอย่างน้อย ดังต่อไปนี้

(1) การกำหนดแผน บทบาท และการยกระดับเหตุการณ์ (Incident Response Plan, Roles and Escalation) : ควรจัดให้มีแผนหรือกระบวนการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร โดยกำหนดประเภทของเหตุการณ์ ระดับความรุนแรง เกณฑ์การประเมินผลกระทบ และแนวทางการยกระดับการดำเนินการอย่างชัดเจน รวมทั้งกำหนดบทบาท หน้าที่ และอำนาจตัดสินใจของผู้รับผิดชอบ ตลอดจนช่องทางการประสานงานทั้งภายในและภายนอกองค์กรให้เหมาะสมกับลักษณะและระดับความรุนแรงของเหตุการณ์

(2) การควบคุมเหตุ การลดผลกระทบ และการสื่อสาร (Containment, Impact Mitigation and Communication) : เมื่อเกิดเหตุการณ์ ควรจัดให้มีการประเมินและดำเนินมาตรการควบคุมเหตุและลดผลกระทบอย่างเหมาะสม เช่น การจำกัดการเข้าถึง การแยกองค์ประกอบที่ได้รับผลกระทบ หรือการระงับการทำงานบางส่วน รวมทั้งควรกำหนดแนวทางการสื่อสารและการแจ้งเหตุแก่ผู้เกี่ยวข้อง เช่น ผู้บริหาร ผู้ให้บริการภายนอก ผู้ถือหลักทรัพย์โทเคน และหน่วยงานกำกับดูแล ตามความเหมาะสมและข้อกำหนดที่เกี่ยวข้อง

(3) การจัดเก็บหลักฐาน การทบทวน และการทดสอบแผน (Evidence Management, Post-incident Review and Testing) : ควรเก็บรักษาข้อมูลและหลักฐานที่เกี่ยวข้องกับเหตุการณ์และการตอบสนองให้ครบถ้วน เพื่อสนับสนุนการวิเคราะห์สาเหตุ การตรวจสอบย้อนหลัง และการดำเนินการตามกฎหมายหรือข้อกำหนดที่เกี่ยวข้อง ภายหลังเหตุการณ์ที่มีนัยสำคัญ ควรทบทวนสาเหตุ ผลกระทบ และประสิทธิผลของการตอบสนอง เพื่อนำผลการทบทวนไปปรับปรุงระบบ มาตรการควบคุม และแผนหรือกระบวนการบริหารจัดการเหตุการณ์ ทั้งนี้ ควรทดสอบและทบทวนแผนหรือกระบวนการดังกล่าวอย่างน้อยปีละหนึ่งครั้ง และเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญต่อระบบหรือการให้บริการ

6.8.2 ความต่อเนื่องในการดำเนินงาน (Business Continuity)

หลักการทั่วไป

ควรจัดให้มีความสามารถในการรักษาการดำเนินงานหรือการให้บริการที่สำคัญให้ดำเนินต่อไปได้อย่างเหมาะสมเมื่อเกิดเหตุการณ์ที่กระทบต่อการดำเนินงานตามปกติ เช่น เหตุขัดข้องของระบบ

เหตุด้านความมั่นคงปลอดภัย ความล้มเหลวของผู้ให้บริการภายนอก ภัยพิบัติ หรือเหตุการณ์อื่นที่ทำให้ไม่สามารถให้บริการได้ตามปกติ

ความต่อเนื่องในการดำเนินงานควรครอบคลุมบุคลากร กระบวนการ เครื่องมือ แนวทางการดำเนินงานทดแทน การสื่อสารภายในและภายนอก และการประสานงานกับผู้ให้บริการหรือผู้เกี่ยวข้องที่สำคัญ เพื่อให้บริการที่มีความสำคัญสามารถดำเนินต่อไปหรือกลับมาให้บริการได้ภายในระดับที่ยอมรับได้

แผนความต่อเนื่องในการดำเนินงานควรสอดคล้องกับลักษณะของผลิตภัณฑ์ บริการ และผลกระทบต่อผู้ถือหลักทรัพย์โทเคน และควรได้รับการทดสอบและปรับปรุงให้สามารถนำไปใช้งานได้จริง

ข้อเสนอแนะขั้นต่ำ

ผู้ออกหลักทรัพย์โทเคนและผู้ให้บริการที่เกี่ยวข้องควรดำเนินการอย่างน้อย ดังต่อไปนี้

(1) การระบุบริการสำคัญและการประเมินผลกระทบ (Critical Services and Business Impact Assessment) : ควรระบุบริการ กระบวนการ ระบบทรัพยากร และผู้เกี่ยวข้องที่มีความสำคัญต่อการให้บริการหลักทรัพย์โทเคน รวมถึงระบบหรือบริการที่มีความเชื่อมโยงหรือพึ่งพากัน และประเมินผลกระทบที่อาจเกิดขึ้นจากการหยุดชะงัก โดยพิจารณาถึงผลกระทบต่อการให้บริการผู้ถือหลักทรัพย์โทเคน และการปฏิบัติตามข้อกำหนดที่เกี่ยวข้อง เพื่อกำหนดลำดับความสำคัญของบริการและกระบวนการ ตลอดจนเป้าหมายและกรอบระยะเวลาที่เหมาะสมในการรักษาความต่อเนื่องหรือกู้คืนการดำเนินงาน ทั้งนี้ ควรพิจารณาความเสี่ยงจากการพึ่งพาผู้ให้บริการภายนอกหรือระบบที่มีความสำคัญ และกำหนดแนวทางรองรับกรณีที่การพึ่งพาดังกล่าวไม่สามารถให้บริการได้ตามปกติ

(2) การจัดทำแผนและแนวทางการดำเนินงานทดแทน (Business Continuity Plan and Alternate Arrangements) : ควรจัดให้มีแผนความต่อเนื่องในการดำเนินงานที่เป็นลายลักษณ์อักษร ซึ่งสอดคล้องกับบริการและกระบวนการที่มีความสำคัญ โดยกำหนดบทบาท หน้าที่ ผู้มีอำนาจตัดสินใจ และขั้นตอนการประสานงานในกรณีเกิดเหตุหยุดชะงักอย่างชัดเจน รวมทั้งกำหนดแนวทางการดำเนินงานทดแทนสำหรับกรณีที่บุคลากร สถานที่ ระบบ หรือผู้ให้บริการที่สำคัญไม่สามารถดำเนินงานหรือให้บริการได้ตามปกติ โดยพิจารณาให้มีช่องทางหรือวิธีการทดแทนที่เหมาะสมกับลักษณะและระดับความสำคัญของบริการ เช่น การใช้ระบบหรือช่องทางสำรอง การดำเนินงานแบบ manual เป็นการชั่วคราว หรือการใช้ผู้ให้

บริการทดแทนตามความเหมาะสม ทั้งนี้ ควรกำหนดแนวทางการสื่อสารและประสานงานกับผู้ถือหลักทรัพย์โทเคน ผู้ให้บริการภายนอก หน่วยงานกำกับดูแล และผู้เกี่ยวข้องอื่นในกรณีที่เกิดเหตุหยุดชะงักที่มีผลกระทบต่อการให้บริการ

(3) การทดสอบ ทบทวน และปรับปรุงแผน (Testing, Review and Improvement) : ควรทดสอบและทบทวนแผนความต่อเนื่องในการดำเนินงานอย่างน้อยปีละหนึ่งครั้ง และเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญต่อระบบ กระบวนการ หรือรูปแบบการให้บริการ เพื่อประเมินความเหมาะสมและประสิทธิผลของแผนและแนวทางการดำเนินงานทดแทน ทั้งนี้ ควรนำผลการทดสอบ การทบทวน เหตุการณ์จริง และข้อมูลหรือบทเรียนที่เกี่ยวข้องมาใช้ปรับปรุงแผน กระบวนการ ทรัพยากร และมาตรการรองรับเหตุหยุดชะงักอย่างต่อเนื่อง

6.8.3 การสำรองข้อมูลและการกู้คืนระบบ (Backup and Recovery)

หลักการทั่วไป

ข้อมูลสำคัญที่เกี่ยวข้องกับหลักทรัพย์โทเคนควรได้รับการสำรองอย่างเหมาะสม และควรจัดให้มีความสามารถในการกู้คืนระบบและข้อมูลดังกล่าวเมื่อเกิดเหตุการณ์ที่ทำให้ข้อมูลสูญหาย ระบบขัดข้อง หรือบริการหยุดชะงัก เพื่อให้สามารถกลับมาให้บริการได้ภายในระดับที่กำหนด

การสำรองและกู้คืนควรครอบคลุมข้อมูลสำคัญ เช่น ฐานข้อมูล ข้อมูลธุรกรรม ข้อมูลผู้ถือหลักทรัพย์โทเคน ข้อมูลการถือครอง และข้อมูลที่จัดเก็บหรือประมวลผลนอก DLT รวมถึงการตั้งค่าระบบและข้อมูลอื่นที่จำเป็นต่อการกู้คืนระบบและการให้บริการ ทั้งนี้ ควรมีการสำรองและเก็บรักษาเอกสารหรือหลักฐานสำคัญที่จำเป็นต่อการตรวจสอบและการดำเนินงานอย่างเหมาะสม และควรพิจารณาความสัมพันธ์และความสอดคล้องระหว่างข้อมูลที่เกี่ยวข้องจากแหล่งต่าง ๆ เพื่อให้การกู้คืนไม่ทำให้ข้อมูลคลาดเคลื่อนหรือไม่สอดคล้องกัน

นอกจากนี้ ควรกำหนดเป้าหมายในการกู้คืนระบบและข้อมูลให้เหมาะสมกับความสำคัญและระดับความเสี่ยงของบริการ และควรทดสอบความสามารถในการกู้คืนอย่างสม่ำเสมอ เพื่อประเมินว่าสามารถกู้คืนระบบและข้อมูลได้ภายในกรอบระยะเวลาที่กำหนด และข้อมูลที่กู้คืนมีความถูกต้องและสอดคล้องกัน

ข้อเสนอแนะขั้นต่ำ

ผู้ออกหลักทรัพย์โทเคนและผู้ให้บริการที่เกี่ยวข้องควรดำเนินการอย่างน้อย ดังต่อไปนี้

(1) การกำหนดขอบเขตและมาตรการสำรองข้อมูล (Backup Scope and Protection) : ควรระบุข้อมูลและระบบที่สำคัญต่อการให้บริการหลักทรัพย์โทเคน

ซึ่งควรได้รับการสำรองและสามารถกู้คืนได้ โดยกำหนดวิธีการและความถี่ในการสำรอง สถานที่จัดเก็บ และระยะเวลาการเก็บรักษาข้อมูลสำรอง โดยพิจารณาจากความสำคัญของข้อมูลและระบบ ความถี่ในการเปลี่ยนแปลงข้อมูล ความเสียหายที่อาจเกิดขึ้นหากข้อมูลสูญหาย และเป้าหมายในการกู้คืนที่กำหนดไว้ ทั้งนี้ ควรคุ้มครองข้อมูลสำรองจากการเข้าถึง แก้ไข ลบ ทำลาย หรือใช้งานโดยไม่ได้รับอนุญาต และพิจารณาแยกข้อมูลสำรองออกจากระบบใช้งานจริงตามความเหมาะสม

(2) การกำหนดเป้าหมายและแผนการกู้คืน (Recovery Objectives and Recovery Plan) : ควรกำหนดเป้าหมายในการกู้คืนระบบและข้อมูล เช่น ระยะเวลาเป้าหมายในการกู้คืนระบบ (Recovery Time Objective: RTO)[16] และจุดข้อมูลเป้าหมายในการกู้คืน (Recovery Point Objective: RPO)[17] โดยพิจารณาจากความสำคัญของบริการ ผลกระทบที่อาจเกิดขึ้นต่อผู้ถือหลักทรัพย์โทเคน ความเสียหายจากการหยุดชะงักหรือการสูญหายของข้อมูล และความสัมพันธ์ระหว่างระบบและข้อมูลที่เกี่ยวข้อง พร้อมจัดทำแผนการกู้คืนที่ระบุลำดับขั้นตอน ผู้รับผิดชอบ ระบบที่เกี่ยวข้อง และวิธีตรวจสอบความครบถ้วนและความสอดคล้องของข้อมูลภายหลังการกู้คืน

ตัวอย่าง : สำหรับบริการหรือระบบที่มีความสำคัญสูง อาจกำหนด RTO ไม่เกิน 2 - 4 ชั่วโมง และ RPO ไม่เกิน 15 - 30 นาที ขณะที่ระบบที่มีความสำคัญรองลงมาอาจกำหนด RTO และ RPO ในระดับที่เหมาะสมกับความสำคัญของระบบและบริการ

(3) การทดสอบ ทบทวน และปรับปรุงความสามารถในการกู้คืน (Recovery Testing, Review and Improvement) : ควรทดสอบความสามารถในการกู้คืนระบบและข้อมูลเป็นระยะ รวมทั้งเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ โดยควรครอบคลุมการตรวจสอบความพร้อมใช้งานของข้อมูลสำรอง ระยะเวลาที่ใช้ในการกู้คืน และความสอดคล้องของข้อมูลระหว่างระบบบนและนอก DLT ทั้งนี้

[16] Recovery Time Objective (RTO) คือ ระยะเวลาเป้าหมายที่กำหนดให้กู้คืนระบบกลับมาใช้งานได้หลังหยุดชะงัก เพื่อจำกัดผลกระทบต่อการดำเนินงาน

[17] Recovery Point Objective (RPO) คือ เป้าหมายว่าต้องกู้คืนข้อมูลให้กลับมาได้ถึงจุดเวลาใดก่อนระบบหยุดชะงัก เพื่อกำหนดขอบเขตการสูญหายของข้อมูลที่ยอมรับได้

ควรบันทึกผลการทดสอบ ปัญหาที่พบ และแนวทางแก้ไข รวมทั้งนำผลดังกล่าวมาใช้ปรับปรุงแผน กระบวนการ และมาตรการสำรองและกู้คืนอย่างต่อเนื่อง

ควรทดสอบความสามารถในการกู้คืนระบบและข้อมูลอย่างน้อยปีละหนึ่งครั้ง และเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญต่อระบบหรือการให้บริการ เพื่อประเมินว่าสามารถกู้คืนได้ตามเป้าหมายที่กำหนด รวมทั้งควรตรวจสอบความพร้อมใช้งานของข้อมูลสำรอง ระยะเวลาที่ใช้ในการกู้คืน และความถูกต้องและความสอดคล้องของข้อมูลภายหลังการกู้คืน ทั้งนี้ ควรบันทึกผลการทดสอบ ปัญหาที่พบ และแนวทางแก้ไข และควรนำผลการทดสอบ เหตุการณ์ที่เกิดขึ้นจริง และบทเรียนที่ได้รับมาใช้ในการทบทวนและปรับปรุงแผน กระบวนการ และมาตรการสำรองและกู้คืนอย่างต่อเนื่อง

เอกสารแนบท้าย

ตัวอย่างสาระสำคัญของข้อกำหนดและเงื่อนไข เกี่ยวกับการออกหลักทรัพย์ในรูปแบบโทเคน (Tokenization Terms)

1. ขอบเขตและวัตถุประสงค์
   - ควรระบุข้อมูลทั่วไปเกี่ยวกับการออกหลักทรัพย์ในรูปแบบโทเคน และวัตถุประสงค์ของการจัดทำข้อกำหนดและเงื่อนไขของการออกหลักทรัพย์โทเคน (Tokenization Terms) รวมถึงระบุคู่สัญญา
     หรือผู้ที่เกี่ยวข้อง ขอบเขตการบังคับใช้ และกฎหมายที่ใช้บังคับ
   - ตัวอย่างของสาระสำคัญที่ควรมี
     - วัตถุประสงค์ของการจัดทำ Tokenization Terms
     - ประเภทของหลักทรัพย์ที่ออกในรูปแบบโทเคน
     - ผู้ออกหลักทรัพย์ (Issuer) และ/หรือผู้ให้บริการสนับสนุนการออกหลักทรัพย์ในรูปแบบโทเคน (Securities Tokenizer)
     - คู่สัญญาหรือผู้ที่เกี่ยวข้องกับ Tokenization Terms
     - ขอบเขตการบังคับใช้ของ Tokenization Terms
     - กฎหมายที่ใช้บังคับ และวิธีการระงับข้อพิพาท (ถ้ามี)

2. การเชื่อมโยงหลักทรัพย์กับโทเคน
   - ควรระบุข้อมูลที่ใช้แสดงความเชื่อมโยงระหว่างหลักทรัพย์กับหลักทรัพย์โทเคน รวมถึงข้อมูลอ้างอิง
     ที่จำเป็นต่อการพิสูจน์และตรวจสอบความเชื่อมโยงดังกล่าว
   - ตัวอย่างของสาระสำคัญที่ควรมี
     - ข้อมูลของหลักทรัพย์และหลักทรัพย์โทเคน เช่น ชื่อหลักทรัพย์ / ประเภทหลักทรัพย์ / จำนวนและหน่วยของหลักทรัพย์โทเคนที่ออก / ข้อมูลที่ใช้ระบุหลักทรัพย์และโทเคน เป็นต้น
     - วิธีการเชื่อมโยงหลักทรัพย์กับโทเคน (Legal Linkage)
     - ข้อมูลอ้างอิงที่ใช้พิสูจน์ความเชื่อมโยง เช่น Unique Identifier (UID) / Smart contract address / ข้อมูลอ้างอิงจากหนังสือชี้ชวน เป็นต้น

3. ธุรกรรมและผลทางกฎหมายของหลักทรัพย์โทเคน
   - ควรระบุหลักเกณฑ์เกี่ยวกับธุรกรรมที่เกี่ยวข้องกับหลักทรัพย์โทเคน รวมถึงผลทางกฎหมายของธุรกรรมดังกล่าว และข้อจำกัดหรือเงื่อนไขที่เกี่ยวข้อง

- ตัวอย่างของสาระสำคัญที่ควรมี
    - หลักเกณฑ์เกี่ยวกับการโอนหลักทรัพย์โทเคน และเงื่อนไขที่ทำให้การโอนมีผลตามกฎหมาย
    - หลักเกณฑ์เกี่ยวกับความสมบูรณ์ของธุรกรรม (Transaction Finality)
    - ข้อจำกัดหรือเงื่อนไขในการโอนหลักทรัพย์โทเคน เช่น การโอนเฉพาะผู้ลงทุนที่มีคุณสมบัติ หรือการใช้ Whitelist
    - การดำเนินการเมื่อมีการโอนโดยมิชอบ การโอนที่ไม่เป็นไปตามเงื่อนไข หรือกรณีมีข้อพิพาทเกี่ยวกับธุรกรรม
    - การดำเนินการเกี่ยวกับการจำนำ การอายัด หรือการจำกัดสิทธิในหลักทรัพย์โทเคน (ถ้ามี)

4. การดำเนินการในกรณีพิเศษ
    - ควรระบุหลักเกณฑ์ เงื่อนไข และกระบวนการในการดำเนินการเมื่อเกิดเหตุการณ์พิเศษที่อาจมีผลต่อสิทธิหรือการถือครองหลักทรัพย์โทเคน รวมถึงผู้มีอำนาจในการดำเนินการและวิธีการดำเนินการที่เกี่ยวข้อง
    - ตัวอย่างของสาระสำคัญที่ควรมี
        - กรณีที่ผู้ถือหลักทรัพย์สูญเสียหรือไม่สามารถเข้าถึงหลักทรัพย์โทเคน รวมถึงกระบวนการพิสูจน์สิทธิของผู้ถือหลักทรัพย์
        - หลักเกณฑ์และเงื่อนไขในการออกหลักทรัพย์โทเคนทดแทน หรือการดำเนินการอื่นเพื่อคงไว้ซึ่งสิทธิของผู้ถือหลักทรัพย์
        - กรณีที่ต้องดำเนินการตามคำสั่งของศาลหรือหน่วยงานที่มีอำนาจ รวมถึงขอบเขตอำนาจและวิธีดำเนินการ
        - วิธีการหรือกลไกที่ใช้ในการดำเนินการ เช่น การระงับการโอน การยกเลิกโทเคน (Burn) การออกหลักทรัพย์โทเคนทดแทน (Reissue) การโอนคืน หรือวิธีการอื่นที่ให้ผลเทียบเท่า
        - เอกสารหรือหลักฐานที่ใช้ประกอบการพิจารณา รวมถึงขั้นตอนที่เกี่ยวข้อง
        - ผู้มีอำนาจอนุมัติและกระบวนการอนุมัติสำหรับการดำเนินการในแต่ละกรณี

5. การแก้ไขเพิ่มเติมข้อกำหนดและเงื่อนไขเกี่ยวกับการออกหลักทรัพย์ในรูปแบบโทเคน
    - ควรระบุหลักเกณฑ์และกระบวนการในการแก้ไขเพิ่มเติมข้อกำหนดและเงื่อนไขเกี่ยวกับการออกหลักทรัพย์ในรูปแบบโทเคน รวมถึงกรณีหรือเหตุที่สามารถแก้ไขได้ และผลของการแก้ไขดังกล่าวต่อผู้ถือหลักทรัพย์โทเคนหรือผู้ที่เกี่ยวข้อง

- ตัวอย่างของสาระสำคัญที่ควรมี
    - กรณีหรือเหตุที่สามารถแก้ไขได้
    - ผู้มีอำนาจในการอนุมัติการแก้ไข
    - กระบวนการและเงื่อนไขในการขอแก้ไข
    - วิธีการแจ้งหรือเปิดเผยการแก้ไขแก่ผู้ถือหลักทรัพย์โทเคนหรือผู้เกี่ยวข้อง (ถ้ามี)

บรรณานุกรม

(1) Capital Markets and Technology Association. (2025). Standard for the tokenization of debt instruments using distributed ledger technology.

(2) Monetary Authority of Singapore. (2025). Guide on the tokenisation of capital markets products.

(3) Committee on Payment and Settlement Systems & International Organization of Securities Commissions. (2012). Principles for financial market infrastructures. Bank for International Settlements.

(4) United Nations Commission on International Trade Law. (2018). UNCITRAL model law on electronic transferable records. United Nations.

(5) Monetary Authority of Singapore. (2023). Enabling open & interoperable networks.

(6) Guardian Fixed Income Industry Group. (2025). Guardian fixed income framework (Version 1.1). Monetary Authority of Singapore.

(7) International Telecommunication Union. (2020). Security framework for distributed ledger technology (ITU-T Recommendation X.1402).

(8) International Telecommunication Union. (2025). Security controls for distributed ledger technology (ITU-T Recommendation X.1413).

(9) National Institute of Standards and Technology. (2025). Security and privacy controls for information systems and organizations (NIST Special Publication 800-53, Revision 5, Release 5.2.0)

(10) National Institute of Standards and Technology. (2024). The NIST cybersecurity framework (CSF) 2.0 (NIST CSWP 29).

(11) Nethermind & PwC Germany. (2025). Tokenization standards: The missing link for institutional adoption.

(12) กระทรวงการคลัง. (2561). ประกาศกระทรวงการคลัง เรื่อง การอนุญาตการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561.

(13) คณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์. (2561). ประกาศคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ กธ. 19/2561 เรื่อง หลักเกณฑ์ เงื่อนไข และวิธีการประกอบธุรกิจสินทรัพย์ดิจิทัล และที่แก้ไขเพิ่มเติม.

(14) คณะกรรมการกำกับตลาดทุน. (2561). ประกาศคณะกรรมการกำกับตลาดทุน ที่ ทธ. 60/2561 เรื่อง หลักเกณฑ์ เงื่อนไข และวิธีการในการมอบหมายให้บุคคลอื่นเป็นผู้รับดำเนินการในงานที่เกี่ยวข้องกับการประกอบธุรกิจ.

(15) สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์. (2565). ประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ สธ. 38/2565 เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ และที่แก้ไขเพิ่มเติม.

(16) คณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์. (2566). ประกาศคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ กธ. 18/2566 เรื่อง หลักเกณฑ์ เงื่อนไข และวิธีการในการขอรับใบอนุญาต และการออกใบอนุญาตประกอบการเป็นศูนย์รับฝากหลักทรัพย์.

(17) สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2568). ร่างข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้งานตราสารเปลี่ยนมืออิเล็กทรอนิกส์ (Electronic Transferable Records Guideline) (เวอร์ชัน 0.1) [ร่างเพื่อรับฟังความคิดเห็น].

ช่องทางติดต่อและเอกสารฉบับปัจจุบัน

หน่วยงานรับผิดชอบ

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
ศูนย์พัฒนาโครงสร้างพื้นฐานตลาดทุน
อีเมล: cmic@sec.or.th

การสอบถามและเสนอข้อคิดเห็น

สำหรับข้อสอบถามหรือข้อคิดเห็นเกี่ยวกับเนื้อหาของมาตรฐาน
โปรดติดต่อผู้ประสานงานตามหัวข้อที่เกี่ยวข้อง ดังนี้

ด้านกฎหมาย (Legal)

นายพีร์นิธิ ฐานิวัฒนานนท์
อีเมล: phiniti@sec.or.th
โทรศัพท์: 0-2263-6529

ด้านหลักทรัพย์โทเคนและความมั่นคงปลอดภัยทางไซเบอร์ (Token and Cybersecurity)

นายโสภณ ชาติทองคำ
อีเมล: sopon@sec.or.th
โทรศัพท์: 0-2033-9954

ด้านผู้ให้บริการสนับสนุนการออกและเสนอขายหลักทรัพย์โทเคน (Securities Tokenizer)

นายคีริศวร์ ตันอมาตยรัตน์
อีเมล: keeris@sec.or.th
โทรศัพท์: 0-2263-6153

เอกสารฉบับปัจจุบันและการปรับปรุง

ก่อนนำมาตรฐานไปใช้งาน ควรตรวจสอบ เวอร์ชัน และวันที่เผยแพร่ เพื่อให้มั่นใจว่าใช้เอกสารฉบับปัจจุบัน
แหล่งเผยแพร่เอกสารฉบับปัจจุบัน
[URL XXXXXXXXXXX]