เอกสารรับฟังความคิดเห็น

เลขที่ อนพ. 4/2559

เรื่อง

การออกหลักเกณฑ์และแนวทางปฏิบัติเกี่ยวกับการเสนอขายหลักทรัพย์ผ่านระบบหรือเครือข่ายอิเล็กทรอนิกส์ (Crowdfunding)

จัดทำโดย

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

เผยแพร่เมื่อวันที่ 13 มกราคม 2559

เพื่อรับฟังความคิดเห็นจากผู้มีส่วนเกี่ยวข้อง

วันสุดท้ายของการให้ความคิดเห็น วันที่ 12 กุมภาพันธ์ 2559

ท่านสามารถ download เอกสารเผยแพร่ฉบับนี้ได้จาก www.sec.or.th

ฝ่ายนโยบายและพัฒนาธุรกิจตัวกลาง

13 มกราคม 2559

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (http://www.sec.or.th)

เลขที่ 333/3 ถนนวิภาวดีรังสิต แขวงจอมพล เขตจตุจักร กรุงเทพฯ 10900

โทรศัพท์ 0-2695-9554 โทรสาร 0-2695-9763

<u>ส่วนที่ 1</u> : บทนำ

ตามที่ประกาศคณะกรรมการกำกับตลาดทุนที่ ทธ. 7/2558 เรื่อง ข้อกำหนดเกี่ยวกับการเสนอขายหลักทรัพย์ผ่านระบบหรือเครือข่ายอิเล็กทรอนิกส์ ลงวันที่ 2 เมษายน พ.ศ. 2558 ("ประกาศที่ ทจ. 7/2558") มีข้อกำหนดให้สำนักงานกำหนดหลักเกณฑ์เพิ่มเติมหรือแนวทางปฏิบัติเพื่อให้ผู้ให้บริการระบบหรือเครือข่ายอิเล็กทรอนิกส์ (funding portal) สามารถปฏิบัติในรายละเอียดตามหลักเกณฑ์หรือแนวทางปฏิบัติได้อย่างเหมาะสมและเป็นไปในแนวทางเดียวกัน นั้น

สำนักงานจึงได้จัดทำหลักการในการออกหลักเกณฑ์และแนวทางปฏิบัติเกี่ยวกับการเสนอขายหลักทรัพย์ผ่านระบบหรือเครือข่ายอิเล็กทรอนิกส์ เพื่อให้เป็นไปตามเจตนารมณ์ของประกาศที่ ทจ. 7/2558 โดยคำนึงถึงความเป็นไปได้ในทางปฏิบัติและภาระของผู้ที่เกี่ยวข้อง รวมทั้งเพื่อให้ผู้ลงทุนได้รับข้อมูลที่เพียงพอในการประกอบการตัดสินใจลงทุน ดังนั้น จึงเห็นควรให้มีการรับฟังความคิดเห็นของหลักการในการออกประกาศสำนักงานและแนวทางปฏิบัติดังกล่าว โดยส่วนที่จะกำหนดในประกาศสำนักงานจะมีสาระสำคัญสรุปไว้ในส่วนที่ 2 และส่วนที่จะกำหนดเป็นแนวทางปฏิบัติจะมีสาระสำคัญสรุปไว้ในส่วนที่ 3 ของเอกสารรับฟังความคิดเห็นนี้

สำนักงานจัดทำเอกสารฉบับนี้ขึ้นเพื่อขอรับฟังความคิดเห็นจากภาคธุรกิจและบุคคลทั่วไป โดยการรับฟังความคิดเห็นจะมีไปถึงวันที่ 12 กุมภาพันธ์ 2559 ซึ่งผู้ที่ประสงค์จะแสดงความคิดเห็นสามารถส่งความคิดเห็นและข้อเสนอแนะที่เป็นประโยชน์ต่อสำนักงานได้ตามรายละเอียดที่ระบุด้านล่างนี้
ทั้งนี้ สำนักงานขอเสนอชื่อเจ้าหน้าที่สำหรับการติดต่อสอบถามคือ นางสาวกรวรา ยงฤทธิกุล โทรศัพท์ 0-2695-9554

ทางไปรษณีย์ : ฝ่ายนโยบายและพัฒนาธุรกิจตัวกลาง
สำนักงานคณะกรรมการ ก.ล.ต.
ชั้น 25 เลขที่ 333/3 ถนนวิภาวดีรังสิต
แขวงจอมพล เขตจตุจักร กรุงเทพฯ 10900

ทางโทรสาร : 0-2695-9763

Email address : kornwara@sec.or.th

<u>ส่วนที่ 2</u> : หลักการในการออกหลักเกณฑ์ที่จะกำหนดไว้ในประกาศสำนักงาน มีดังนี้

1. การกระทำที่อาจก่อให้เกิดความขัดแย้งทางผลประโยชน์หรือการดำเนินธุรกิจเพื่อให้เป็นไปตามมาตรฐานของผู้ให้บริการระบบหรือเครือข่ายอิเล็กทรอนิกส์ (funding portal)

<u>ที่มา</u>

ข้อ 18(5) ของประกาศที่ ทจ. 7/2558 กำหนดว่า funding portal <u>ต้องไม่กระทำการ</u>ใดที่อาจก่อให้<u>เกิดความขัดแย้งทางผลประโยชน์</u> หรือที่จะทำให้<u>การทำธุรกิจไม่เป็นไปตามมาตรฐาน</u>หรือเยี่ยงผู้ประกอบวิชาชีพในลักษณะเดียวกันจะพึงกระทำ เว้นแต่เป็นการกระทำที่เป็นไปตามหลักเกณฑ์และเงื่อนไขที่สำนักงานประกาศกำหนด หรือเป็นหน้าที่ที่ต้องกระทำตามกฎหมาย

<u>หลักเกณฑ์ที่เสนอ</u>

1.1 เพื่อความยืดหยุ่นในการประกอบธุรกิจ funding portal <u>สามารถกระทำการที่อาจก่อให้เกิดความขัดแย้งทางผลประโยชน์ในบางลักษณะได้</u> หากได้มีการจัดระบบหรือมีการดำเนินการในการป้องกันความขัดแย้งทางผลประโยชน์แล้ว ดังนี้

1.1.1 Funding portal หรือบริษัทในเครือของ funding portal สามารถระดมทุนผ่านระบบหรือเครือข่ายอิเล็กทรอนิกส์ของ funding portal ได้ ทั้งนี้ funding portal ต้องแสดงให้เห็นว่า มีการจัดการความขัดแย้งทางผลประโยชน์ที่อาจจะเกิดขึ้นได้อย่างมีประสิทธิภาพ อาทิเช่น

(1) จัดให้มีผู้เก็บรักษาเงินค่าจองซื้อหลักทรัพย์ที่ไม่มีความเกี่ยวข้องหรือมีความสัมพันธ์กับ funding portal หรือบริษัทในเครือดังกล่าว

(2) จัดให้มีขั้นตอนและการดำเนินการในการเสนอขายเป็นไปในลักษณะเดียวกับผู้เสนอขายหลักทรัพย์รายอื่นที่เสนอขายผ่าน funding portal

(3) ต้องเปิดเผยข้อมูลความสัมพันธ์ให้สมาชิกผู้ลงทุนทราบ เป็นต้น

บริษัทในเครือตาม 1.1.1 หมายถึง (1) บริษัทที่ถือหุ้นใน funding portal เกินกว่าร้อยละ 10 ของจำนวนหุ้นที่จำหน่ายได้แล้วทั้งหมดของ funding portal หรือ (2) บริษัทที่ funding portal ถือหุ้นเกินกว่าร้อยละ 10 ของจำนวนหุ้นที่จำหน่ายได้แล้วทั้งหมดของบริษัทนั้น

1.1.2 Funding portal สามารถลงทุนในหลักทรัพย์ของผู้เสนอขายหลักทรัพย์ก่อนที่จะมีการเสนอขายหลักทรัพย์ผ่านระบบหรือเครือข่ายอิเล็กทรอนิกส์ของตนเองได้ โดยต้องเปิดเผยข้อมูลการลงทุนดังกล่าวให้ชัดเจน

1.1.3 ในกรณีที่ funding portal รวมถึงผู้บริหาร และเจ้าหน้าที่ของ funding portal จะจองซื้อหลักทรัพย์ของผู้เสนอขายหลักทรัพย์ที่มีการเสนอขายผ่านระบบหรือเครือข่ายอิเล็กทรอนิกส์ของตนเอง จะต้องปฏิบัติตามวิธีปฏิบัติในการจองซื้อที่ไม่แตกต่างจากการจองซื้อของสมาชิกในประเภทเดียวกัน รวมทั้งต้องเปิดเผยความขัดแย้งทางผลประโยชน์ที่เกิดขึ้นให้ชัดเจน

1.2 เพื่อให้การดำเนินธุรกิจของ funding portal เป็นไปตามมาตรฐานหรือเยี่ยงผู้ประกอบวิชาชีพในลักษณะเดียวกันจะพึงกระทำ funding portal สามารถดำเนินการในลักษณะดังนี้

1.2.1 ในการนำเสนอข้อมูลเกี่ยวกับหลักทรัพย์ที่เสนอขายผ่านระบบหรือเครือข่ายอิเล็กทรอนิกส์ funding portal ต้องดำเนินการเพื่อให้มั่นใจได้ว่า ผู้ลงทุนมีโอกาสได้รับข้อมูลเกี่ยวกับหลักทรัพย์ที่เสนอขายอยู่บนระบบของตนในทุกหลักทรัพย์ ซึ่งข้อมูลดังกล่าวต้องไม่ก่อให้เกิดความเข้าใจผิดในสาระสำคัญ และไม่เป็นการสนับสนุนหรือกระตุ้นให้เกิดการลงทุนในหลักทรัพย์ของผู้เสนอขายหลักทรัพย์รายใดรายหนึ่งเป็นพิเศษ ทั้งนี้ funding portal สามารถจัดกลุ่มการนำเสนอข้อมูลตามข้อเท็จจริงที่เกิดขึ้นได้ เช่น ประเภทธุรกิจหรือกลุ่มอุตสาหกรรมของผู้เสนอขายหลักทรัพย์ วงเงินที่เสนอขายหลักทรัพย์ ระดับความสำเร็จของการเสนอขายหลักทรัพย์ สถานที่ตั้งของผู้เสนอขายหลักทรัพย์ เป็นต้น

อย่างไรก็ดี การให้ข้อมูลดังกล่าวต้องไม่เป็นการให้คุณค่าของหลักทรัพย์หรือการให้ความเห็นที่อาจนำไปสู่การประเมินคุณค่าของหลักทรัพย์ ที่อาจเข้าข่ายเป็นการให้บริการเป็นที่ปรึกษาการลงทุน ซึ่งต้องได้รับใบอนุญาตประกอบธุรกิจหลักทรัพย์ประเภทการเป็นที่ปรึกษาการลงทุน

1.2.2 ในกรณีที่มีผู้แนะนำให้ผู้ลงทุนมาสมัครเป็นสมาชิกในระบบหรือเครือข่ายอิเล็กทรอนิกส์ของตนเอง funding portal สามารถจ่ายค่าตอบแทนให้แก่ผู้แนะนำดังกล่าวได้ โดยการจ่ายค่าตอบแทนดังกล่าวต้องไม่เป็นการจ่ายค่าตอบแทนในลักษณะที่อ้างอิงกับมูลค่าการจองซื้อหลักทรัพย์ที่สมาชิกจองซื้อผ่านระบบหรือเครือข่ายอิเล็กทรอนิกส์ (transaction-based compensation) ทั้งนี้ เพื่อเป็นการลดโอกาสที่จะเกิดการกระทำที่ไม่เหมาะสมของผู้แนะนำในการชักชวนให้ผู้ลงทุนสมัครเป็นสมาชิกเพื่อลงทุนผ่านระบบหรือเครือข่ายอิเล็กทรอนิกส์ และการลงทุนดังกล่าวอาจไม่ตรงกับความต้องการลงทุนของผู้ลงทุน รวมทั้งลดแรงจูงใจของผู้แนะนำในการแนะนำให้ผู้ลงทุนมาสมัครเป็นสมาชิกและชักชวนให้ลงทุนในมูลค่าสูงเพื่อผู้แนะนำได้รับค่าตอบแทนที่สูงขึ้นตามมูลค่าการจองซื้อของผู้ลงทุน

1.2.3 ในการจัดให้มีระบบสื่อสารทางอิเล็กทรอนิกส์เพื่อใช้ในการสื่อสารระหว่างสมาชิกด้วยกันหรือระหว่างสมาชิกกับผู้เสนอขายหลักทรัพย์ (เช่น webboard หรือ blog) นั้น ให้ funding มีหน้าที่กำกับดูแล และตรวจสอบข้อมูลในช่องทางการสื่อสารดังกล่าวและดำเนินการ ดังนี้

(1) funding portal ต้องให้ข้อมูล คำแนะนำ ระเบียบ หรือกฎเกณฑ์ เกี่ยวกับวิธีการในการใช้ช่องทางการสื่อสารดังกล่าว แต่ไม่สามารถเข้าร่วมให้ความเห็นหรือให้ข้อมูลใด ๆ ที่เกี่ยวกับหลักทรัพย์หรือความเห็นอื่นใดที่อาจเข้าข่ายเป็นการให้คำแนะนำเกี่ยวกับคุณค่าของหลักทรัพย์หรือความเหมาะสมในการลงทุนที่เกี่ยวกับหลักทรัพย์ ที่อาจนำไปสู่การประเมินคุณค่าของหลักทรัพย์ที่อาจเข้าข่ายเป็นการให้บริการเป็นที่ปรึกษาการลงทุน ซึ่งต้องได้รับใบอนุญาตประกอบธุรกิจหลักทรัพย์ประเภทการเป็นที่ปรึกษาการลงทุน รวมทั้งกำกับดูแลมิให้ผู้ใดใช้ช่องทางดังกล่าวให้ข้อมูลที่อาจเข้าข่ายเป็นการให้บริการเป็นที่ปรึกษาการลงทุนในลักษณะดังกล่าวด้วยเช่นกัน

(2) ในกรณีที่ปรากฏว่า ผู้เสนอขายหลักทรัพย์มีการให้ข้อมูลที่เกี่ยวข้องกับการเสนอขายหลักทรัพย์ที่นอกเหนือไปจากข้อมูลการเสนอขายหลักทรัพย์ที่ได้แสดงไว้แล้วบนระบบหรือเครือข่ายอิเล็กทรอนิกส์ funding portal มีหน้าที่พิจารณาว่า ข้อมูลดังกล่าวส่งผลต่อการตัดสินใจลงทุนของผู้ลงทุนอย่างมีนัยสำคัญหรือไม่ หากข้อมูลดังกล่าวมีผลต่อการตัดสินใจของผู้ลงทุนอย่างมีนัยสำคัญ funding portal ต้องดำเนินการให้ผู้เสนอขายหลักทรัพย์เปิดเผยข้อมูลดังกล่าวโดยแสดงไว้บนระบบหรือเครือข่ายอิเล็กทรอนิกส์ด้วย

(3) กระทำการใด ๆ มิให้ปรากฏข้อมูลดังต่อไปนี้ในช่องทางการสื่อสารดังกล่าว

(ก) ข้อมูลที่เป็นเท็จ เกินความจริง บิดเบือน ปิดบัง หรือทำให้สำคัญผิดในสาระสำคัญของข้อมูลการเสนอขายหลักทรัพย์

(ข) ข้อมูลเกี่ยวกับการประมาณการผลตอบแทนหรือข้อมูลอื่นใด ที่ชี้นำให้สมาชิกสำคัญผิดเกี่ยวกับความเสี่ยงจากการลงทุน

(ค) ข้อมูลที่เป็นการคาดการณ์หรือประมาณการเกี่ยวกับความต้องการซื้อหรือความสนใจในหลักทรัพย์ที่เสนอขาย หรือเกี่ยวกับเรื่องอื่นใดที่อาจจะทำให้สมาชิกเข้าใจสภาพความต้องการซื้อหรือความสนใจในหลักทรัพย์นั้นผิดไปจากสภาพที่แท้จริง

(ง) ข้อมูลอื่นใดที่ไม่เป็นไปตามกฎ กติกา และมารยาทในการสื่อสารผ่านช่องทางดังกล่าวตามที่ funding portal ได้กำหนดไว้ เช่น ข้อความที่อาจก่อให้เกิดความขัดแย้งในสังคม ขัดกับศีลธรรมอันดีของสังคม หรือมีเจตนากลั่นแกล้งให้ผู้อื่นได้รับความเดือดร้อน เป็นต้น

2. การจัดเก็บข้อมูลของสมาชิกที่ติดต่อหรือใช้บริการผ่านระบบหรือเครือข่ายอิเล็กทรอนิกส์ของผู้ให้บริการระบบหรือเครือข่ายอิเล็กทรอนิกส์

<u>ที่มา</u>

ข้อ 30 ของประกาศที่ ทจ. 7/2558 กำหนดว่า การติดต่อหรือให้บริการแก่สมาชิก การแจ้งเตือนเรื่องต่าง ๆ หรือการให้สมาชิกลงนามรับทราบหรือยอมรับการให้บริการหรือความเสี่ยงที่อาจเกิดขึ้นจากการใช้บริการ funding portal สามารถจัดให้อยู่ในรูปแบบอิเล็กทรอนิกส์ในลักษณะที่สามารถจัดเก็บข้อมูลและตรวจดูข้อมูลได้ ทั้งนี้ ตามที่สำนักงานประกาศกำหนด

<u>หลักเกณฑ์ที่เสนอ</u>

2.1 Funding portal ต้องจัดให้มีการจัดการและจัดเก็บข้อมูล เอกสารหรือหลักฐาน ซึ่งเกี่ยวข้องกับการติดต่อหรือให้บริการแก่สมาชิก การแจ้งเตือนเรื่องต่าง ๆ หรือการให้สมาชิกลงนามรับทราบหรือยอมรับการใช้บริการหรือความเสี่ยงที่อาจเกิดขึ้นจากการใช้บริการของ funding portal ทั้งข้อมูลก่อนเริ่มให้บริการแก่สมาชิก และข้อมูลภายหลังเป็นสมาชิกแล้ว ดังต่อไปนี้

2.1.1 จัดให้มีระบบการจัดการและจัดเก็บที่รัดกุม เป็นระเบียบ และพร้อมนำข้อมูล เอกสารหรือหลักฐาน มาใช้งานหรือตรวจสอบได้ภายในระยะเวลาอันสมควร

2.1.2 ระบบตาม 2.1.1 สามารถป้องกัน

(1) การแก้ไข การสูญหาย หรือการถูกทำลาย อย่างไม่เหมาะสม

(2) การใช้หรือเข้าถึงข้อมูลอย่างไม่ถูกต้อง ไม่เหมาะสม หรือขัดกับกฎหมาย โดยเฉพาะอย่างยิ่งข้อมูล เอกสาร หรือหลักฐาน ที่เป็นข้อมูลส่วนบุคคลของลูกค้าหรือข้อมูลที่ไม่เปิดเผย หรือยังไม่ได้เปิดเผยเป็นการทั่วไป

2.2 ประเภทข้อมูล เอกสาร หรือหลักฐาน และระยะเวลาขั้นต่ำในการจัดเก็บข้อมูล ให้เป็นไปตามหลักเกณฑ์ดังนี้

2.2.1 จัดเก็บตลอดระยะเวลาเป็นสมาชิก และจัดเก็บต่อไปอีก 5 ปีนับแต่วันสิ้นสุดการเป็นสมาชิกสำหรับข้อมูลและเอกสารหลักฐานที่เกี่ยวข้องกับการดำเนินการ ดังนี้

(1) ข้อมูลการสมัครเป็นสมาชิก

(2) หลักฐานที่เกี่ยวกับการแจ้งเตือนเรื่องต่าง ๆ หรือการให้สมาชิกลงนามรับทราบหรือยอมรับการให้บริการหรือความเสี่ยงที่อาจเกิดขึ้นจากการใช้บริการของ funding portal

(3) ข้อมูลของสมาชิกเพื่อวัตถุประสงค์ในการทำความรู้จักสมาชิก จัดประเภทสมาชิก และความสามารถในการปฏิบัติตามข้อตกลงในการใช้บริการ รวมทั้งหลักฐานที่เกี่ยวกับการดำเนินการดังกล่าว

(4) ข้อมูลการทำแบบทดสอบความเข้าใจเกี่ยวกับการลงทุนของสมาชิก (knowledge test)

2.2.2 จัดเก็บเป็นระยะเวลา 5 ปีนับแต่วันที่ทำรายการหรือทำธุรกรรม โดยปีแรกต้องเก็บในลักษณะที่พร้อมให้สำนักงานเรียกดู สำหรับเอกสารดังต่อไปนี้

(1) หลักฐานเกี่ยวกับการจองซื้อหลักทรัพย์ของสมาชิก

(2) หลักฐานการรับรองของสมาชิกที่เป็นผู้ลงทุนรายบุคคลเกี่ยวกับมูลค่าการลงทุนภายในรอบระยะเวลา 12 เดือนใด ๆ ก่อนจองซื้อหลักทรัพย์ว่า มีมูลค่าไม่เกินห้าแสนบาท (self-declare)

(3) หลักฐานเกี่ยวกับการรับเงินค่าจองซื้อหลักทรัพย์จากสมาชิก หรือการจ่ายคืนเงินค่าจองซื้อหลักทรัพย์ให้สมาชิก

(4) หลักฐานเกี่ยวกับการทำธุรกรรมที่มีความขัดแย้งทางผลประโยชน์ตามที่กล่าวแล้วในข้อ 1.1

(5) หลักฐานที่แสดงได้ว่า funding portal มีการดำเนินการตามข้อ 29 ของประกาศที่ ทจ. 7/2558 ที่กำหนดหน้าที่ให้ funding portal ต้องเปิดเผยข้อมูลตามที่กำหนดในการติดต่อหรือให้บริการแก่สมาชิกใหม่

(6) หลักฐานที่แสดงได้ว่า funding portal มีการดำเนินการตามข้อ 37 ของประกาศที่ ทจ. 7/2558 ที่กำหนดหน้าที่ให้ funding portal ต้องจัดให้มีการให้ความรู้แก่สมาชิกเกี่ยวกับการเสนอขายหลักทรัพย์ผ่านระบบหรือเครือข่ายอิเล็กทรอนิกส์ แจ้งสรุปข้อมูลเกี่ยวกับการรับจองซื้อหลักทรัพย์ของสมาชิก

แจ้งการยืนยันให้สมาชิกที่จองซื้อหลักทรัพย์ทราบเมื่อการเสนอขายได้ครบตามมูลค่าที่กำหนดไว้ และแจ้งให้สมาชิกที่จองซื้อหลักทรัพย์ทราบเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญเกี่ยวกับข้อมูลของผู้เสนอขายหลักทรัพย์หรือการเสนอขายหลักทรัพย์ โดยต้องสามารถแสดงถึงข้อมูลที่มีการให้ความรู้แก่สมาชิกหรือการแจ้งสมาชิก

(7) หลักฐานการสื่อสารทางอิเล็กทรอนิกส์ระหว่างสมาชิกด้วยกันหรือระหว่างสมาชิกกับบริษัทที่เสนอขายหลักทรัพย์ หรือระหว่างสมาชิกกับ funding portalโดยต้องสามารถแสดงถึงข้อความทั้งหมดที่มีการสื่อสารผ่านช่องทางดังกล่าว รวมถึงข้อความที่ถูกลบออกจากช่องทางดังกล่าวตามข้อ 1.2.3

(8) หลักฐานเกี่ยวกับการรับส่งข้อมูลอัตโนมัติทางอิเล็กทรอนิกส์ระหว่าง funding portal และสมาชิก

2.2.3 จัดเก็บเอกสารหลักฐานที่เกี่ยวข้องกับเรื่องร้องเรียนและการดำเนินการในเรื่องดังกล่าวไม่น้อยกว่า 2 ปีนับแต่วันที่มีข้อยุติเกี่ยวกับเรื่องร้องเรียนนั้น

3. ระบบงานในการกำกับดูแลการปฏิบัติงานของผู้ให้บริการระบบหรือเครือข่ายอิเล็กทรอนิกส์

<u>ที่มา</u>

ข้อ 23(10) ของประกาศที่ ทจ. 7/2558 กำหนดว่า funding portal ต้องควบคุมดูแลให้มีระบบงานในการกำกับดูแลการปฏิบัติงานของตน (compliance) ตามแนวทางที่สำนักงานประกาศกำหนด

<u>หลักเกณฑ์ที่เสนอ</u>

ระบบงานในการกำกับดูแลการปฏิบัติงานของ funding portal ต้องครอบคลุมเรื่องอย่างน้อยดังต่อไปนี้

3.1 จัดให้มีผู้กำกับดูแลการปฏิบัติงานที่มีความรู้ความสามารถในจำนวนที่เพียงพอกับลักษณะของธุรกิจ และขอบเขตหน้าที่ความรับผิดชอบ รวมทั้งต้องเป็นบุคลากรที่ปฏิบัติงานในตำแหน่งที่สามารถทำหน้าที่ได้โดยอิสระจากผู้บริหาร และสามารถสอบทานการทำงานของหน่วยงานอื่นได้ ทั้งนี้ ต้องมีการมอบหมายอำนาจหน้าที่ให้ผู้กำกับดูแลการปฏิบัติงานสามารถเข้าถึงข้อมูลและบุคลากรที่จำเป็นเพื่อการปฏิบัติงานได้

3.2 กำหนดขอบเขตหน้าที่และความรับผิดชอบของผู้กำกับดูแลการปฏิบัติงานเป็นลายลักษณ์อักษร ทั้งนี้ หน้าที่และความรับผิดชอบของผู้กำกับดูแลการปฏิบัติงานดังกล่าวต้องมีอย่างน้อย ดังนี้

3.2.1 เป็นศูนย์กลางในการให้ความรู้และคำแนะนำแก่บุคลากรของ funding portal เพื่อให้บุคคลดังกล่าวเข้าใจและสามารถปฏิบัติงานตามกฎเกณฑ์ได้อย่างถูกต้อง

3.2.2 ติดตามกฎเกณฑ์ที่มีการแก้ไข และรายงานให้ผู้ปฏิบัติงานที่เกี่ยวข้องรับทราบและถือปฏิบัติ

3.2.3 ตรวจสอบหรือสอบทานการปฏิบัติงานตามกฎเกณฑ์ของ funding portal และรายงานผลการตรวจสอบหรือสอบทานต่อคณะกรรมการของ funding portal หรือคณะกรรมการที่ได้รับมอบหมาย และผู้บริหารระดับสูงของ funding portal

3.2.4 จัดทำรายงานการกำกับดูแลการปฏิบัติงานประจำปี (annual compliance report) เสนอต่อคณะกรรมการของ funding portal หรือคณะกรรมการอื่นที่คณะกรรมการบริษัทมอบหมายที่ต้องเป็นอิสระจากการบริหารจัดการของ funding portal อย่างน้อยปีละ 1 ครั้ง โดยอาจมีการรายงานผู้บริหารระดับสูงของ funding portal ไปในเวลาเดียวกันได้ รวมทั้งจัดส่งรายงานดังกล่าวให้สำนักงานภายในสองเดือนนับแต่วันสิ้นปีปฏิทิน โดยรายงานการกำกับดูแลการปฏิบัติงานประจำปี ต้องมีรายการอย่างน้อยดังต่อไปนี้

(1) ขอบเขตการตรวจสอบหรือสอบทานการปฏิบัติงาน

(2) ผลการตรวจสอบหรือสอบทานการปฏิบัติงาน

(3) การกระทำความผิด ฝ่าฝืน หรือไม่ปฏิบัติงานตามกฎเกณฑ์อย่างมีนัยสำคัญและแนวทางการแก้ไข

3.2.5 เป็นผู้ประสานงานและรายงานให้สำนักงานทราบโดยไม่ชักช้า ในกรณีที่พบการปฏิบัติที่เข้าข่ายหรืออาจเข้าข่ายฝ่าฝืนหรือไม่ปฏิบัติตามกฎเกณฑ์อย่างมีนัยสำคัญ

3.3 มีการจัดเก็บเอกสารหลักฐานเกี่ยวกับการกำกับดูแลการปฏิบัติงานของ funding portal เป็นเวลาไม่น้อยกว่า 5 ปี โดยปีแรกต้องเก็บในลักษณะที่พร้อมให้สำนักงานเรียกดู เพื่อให้สำนักงานสามารถตรวจสอบได้

3.4 กรณีมีการมอบหมายให้บุคคลอื่นเป็นผู้รับดำเนินการในการกำกับดูแลการปฏิบัติงาน funding portal ต้องกำกับดูแลให้ผู้รับดำเนินการปฏิบัติตามหลักเกณฑ์ข้างต้นด้วย และยังมีความรับผิดชอบเสมือน funding portal ดำเนินการด้วยตนเอง

4. การจัดทำงบการเงินประจำปีของผู้ให้บริการระบบหรือเครือข่ายอิเล็กทรอนิกส์

<u>ที่มา</u>

ข้อ 29 ของประกาศที่ ทจ. 7/2558 กำหนดให้ในการติดต่อหรือให้บริการแก่สมาชิกรายใหม่ funding portal ต้องเปิดเผยข้อมูลตามที่กำหนดให้สมาชิกทราบ เพื่อใช้เป็นข้อมูลประกอบการตัดสินใจเลือกใช้บริการ และพิจารณาความเสี่ยงที่อาจเกิดขึ้นจากการใช้บริการ ประกอบกับข้อ 3(1) ของประกาศที่ ทจ. 7/2558 ให้สำนักงานสามารถกำหนดหลักเกณฑ์ในรายละเอียดที่กำหนดไว้ในประกาศที่ ทจ. 7/2558 ให้มีความชัดเจนเพียงพอที่ funding portal จะสามารถปฏิบัติตามประกาศได้ในแนวทางเดียวกัน ทั้งนี้ การกำหนดหลักเกณฑ์ดังกล่าวอาจกำหนดตามประเภทหลักทรัพย์หรือผู้ลงทุนก็ได้

<u>หลักเกณฑ์ที่เสนอ</u>

เพื่อให้สมาชิกหรือผู้ลงทุนมีข้อมูลด้านฐานะการเงินและผลการดำเนินการของ funding portal เพื่อประกอบการเลือกใช้บริการและการพิจารณาความเสี่ยงที่อาจจะเกิดขึ้นจากการใช้บริการ funding portal ต้องจัดทำงบการเงินประจำปี ซึ่งต้องผ่านการตรวจสอบและแสดงความเห็นโดยผู้สอบบัญชีรับอนุญาต

โดยให้เปิดเผยไว้บนระบบหรือเครือข่ายอิเล็กทรอนิกส์ของ funding portal และจัดส่งให้สำนักงานตามวิธีการที่สำนักงานจัดไว้ในระบบงานอิเล็กทรอนิกส์ของสำนักงาน ทั้งนี้ funding portal ต้องดำเนินการให้แล้วเสร็จภายใน 21 วันนับแต่วันที่ได้รับอนุมัติจากที่ประชุมใหญ่ แต่ต้องไม่เกิน 4 เดือนนับแต่วันสิ้นปีบัญชี

5. การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของผู้ให้บริการระบบหรือเครือข่ายอิเล็กทรอนิกส์ (IT Security)

ที่มา

ข้อ 3(1) ของประกาศที่ ทจ. 7/2558 ให้สำนักงานสามารถกำหนดหลักเกณฑ์ในรายละเอียดที่กำหนดไว้ในประกาศที่ ทจ. 7/2558 ให้มีความชัดเจนเพียงพอที่ funding portal จะสามารถปฏิบัติตามประกาศได้ในแนวทางเดียวกัน ทั้งนี้ การกำหนดหลักเกณฑ์ดังกล่าวอาจกำหนดตามประเภทหลักทรัพย์หรือผู้ลงทุนก็ได้

หลักเกณฑ์ที่เสนอ

เพื่อให้ funding portal มีมาตรการด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศอย่างเพียงพอในการป้องกันและบริหารความเสี่ยงด้านระบบสารสนเทศที่อาจส่งผลกระทบต่อการรักษาความลับของข้อมูล (confidentiality) ความครบถ้วนถูกต้องน่าเชื่อถือของข้อมูล (integrity) และสภาพพร้อมใช้งานของข้อมูลและระบบสารสนเทศ (availability) ได้อย่างมีประสิทธิภาพ funding portal ต้องจัดให้มีมาตรการดังกล่าวข้างต้นอย่างน้อยครอบคลุมในเรื่องดังต่อไปนี้

5.1 นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Policy) และการควบคุมการปฏิบัติงานให้เป็นไปตามข้อกำหนด (Compliance)

เพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และรับทราบเกี่ยวกับหน้าที่ความรับผิดชอบและแนวทางปฏิบัติในการควบคุมความเสี่ยงต่าง ๆ รวมทั้งเพื่อให้การบริหารจัดการความมั่นคงปลอดภัยของระบบสารสนเทศเป็นไปตามนโยบายและหลักปฏิบัติที่ funding portal ได้กำหนดไว้

5.2 การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร (Human Resource Security)

เพื่อให้พนักงานและบุคคลภายนอกที่ปฏิบัติงานโดยเชื่อมต่อกับข้อมูลหรือระบบงานภายในองค์กร มีความตระหนักรู้และปฏิบัติงานโดยคำนึงถึงการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของ funding portal

5.3 การบริหารจัดการทรัพย์สินสารสนเทศ (Asset Management)

เพื่อให้ทรัพย์สินสารสนเทศของ funding portal ได้รับการป้องกันอย่างเหมาะสม มิให้มีการเปิดเผย เปลี่ยนแปลงแก้ไข หรือสร้างความเสียหายแก่ทรัพย์สินสารสนเทศดังกล่าว

ทั้งนี้ ทรัพย์สินสารสนเทศ หมายถึง

5.3.1 ทรัพย์สินสารสนเทศ**ประเภทระบบ** ซึ่งได้แก่ ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

5.3.2 ทรัพย์สินสารสนเทศ**ประเภทอุปกรณ์** ซึ่งได้แก่ ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด

5.3.3 ทรัพย์สินสารสนเทศ**ประเภทข้อมูล** ซึ่งได้แก่ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

5.4 การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ (Access Control)

เพื่อควบคุมการเข้าถึงข้อมูลและสิ่งอำนวยความสะดวกในการประมวลผลข้อมูล รวมทั้งควบคุมสิทธิการใช้งานระบบสารสนเทศอย่างเหมาะสมและป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงระบบสารสนเทศได้

5.5 การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

เพื่อป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึงพื้นที่หวงห้าม และป้องกันอุปกรณ์สารสนเทศมิให้สูญหาย ถูกโจรกรรม ก่อให้เกิดความเสียหาย เข้าถึงหรือถูกใช้งานโดยบุคคลที่ไม่เกี่ยวข้อง รวมทั้งเพื่อให้อุปกรณ์สารสนเทศสามารถทำงานได้อย่างต่อเนื่อง

5.6 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ (Operations Security)

เพื่อให้มั่นใจว่าการปฏิบัติงานด้านระบบสารสนเทศเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย ได้รับการป้องกันภัยคุกคามจากโปรแกรมไม่ประสงค์ดี และป้องกันการสูญหายของข้อมูล รวมทั้งมีการตรวจสอบระบบสารสนเทศ และจัดเก็บบันทึกและหลักฐานเกี่ยวกับการใช้งานระบบสารสนเทศอย่างครบถ้วนและเพียงพอสำหรับการตรวจสอบการใช้งานดังกล่าว

5.7 การบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ (Communications Security)

เพื่อป้องกันการกระทำที่มีความเสี่ยงต่อข้อมูลสารสนเทศในระบบเครือข่ายคอมพิวเตอร์ และป้องกันโครงสร้างพื้นฐานที่สนับสนุนระบบเครือข่ายคอมพิวเตอร์ รวมทั้งเพื่อรักษาความมั่นคงปลอดภัยในการรับส่งข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์

5.8 การจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ (System Acquisition, Development and Maintenance)

เพื่อให้กระบวนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นส่วนหนึ่งของระบบสารสนเทศของทั้งภายในองค์กรและที่เกี่ยวข้องกับการให้บริการภายนอกผ่านเครือข่ายสาธารณะ ตลอดช่วงอายุการใช้งานระบบสารสนเทศ และเพื่อให้การพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศ

ประมวลผลได้อย่างถูกต้องครบถ้วนและเป็นไปตามความต้องการของผู้ใช้งาน (change management) รวมถึงการรักษาไว้ซึ่งความมั่นคงปลอดภัยของระบบสารสนเทศตลอดช่วงการพัฒนาระบบงานสารสนเทศ (system development life cycle)

5.9 การใช้บริการจากผู้ให้บริการภายนอก (Supplier Relationships)

เพื่อรักษาความมั่นคงปลอดภัยของทรัพย์สินสารสนเทศของ funding portal จากการเข้าถึงโดยผู้ให้บริการภายนอกอย่างไม่เหมาะสม และเพื่อรักษาความมั่นคงปลอดภัยจากการใช้บริการ cloud computing ของระบบสารสนเทศที่มีความสำคัญ

5.10 การบริหารจัดการสถานการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Incident Management)

เพื่อให้มีการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศได้อย่างถูกต้องและมีประสิทธิภาพ ในช่วงระยะเวลาที่เหมาะสม

5.11 การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Aspects of Business Continuity Management)

เพื่อให้มาตรการด้านรักษาความมั่นคงปลอดภัยของระบบสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และระบบสารสนเทศอยู่ในสภาพที่พร้อมใช้งานอยู่เสมอ

ส่วนที่ 3 : หลักการในการออกหลักเกณฑ์ที่จะกำหนดไว้ในประกาศแนวทางปฏิบัติ มีดังนี้

1. การเปิดเผยข้อมูลของบริษัทที่เสนอขายหลักทรัพย์และการสิ้นสุดการเปิดเผยข้อมูลของการเสนอขายหลักทรัพย์ผ่านระบบหรือเครือข่ายอิเล็กทรอนิกส์

ที่มา

ข้อ 36(4)(ก) ของประกาศที่ ทจ. 7/2558 กำหนดให้ funding portal จัดทำข้อตกลงกับผู้เสนอขายหลักทรัพย์ โดยอย่างน้อยต้องมีข้อกำหนดให้ผู้เสนอขายหลักทรัพย์มีหน้าที่ในการเปิดเผยข้อมูลที่เพียงพอบนระบบหรือเครือข่ายอิเล็กทรอนิกส์ทั้งก่อนและต่อเนื่องไปภายหลังการเสนอขายหลักทรัพย์ ซึ่งจะกระทำในรูปแบบอิเล็กทรอนิกส์ลักษณะใดก็ได้ แต่จะต้องชัดเจน ง่ายต่อการทำความเข้าใจ และไม่ทำให้สำคัญผิด ทั้งนี้ การเปิดเผยข้อมูลต่อเนื่องไปภายหลังการเสนอขายหลักทรัพย์อาจมีการตกลงกันให้สิ้นสุดหน้าที่นั้นได้ตามแนวทางที่สำนักงานกำหนด

ข้อ 18 ของประกาศที่ ทจ. 7/2558 กำหนดให้ funding portal ต้องปฏิบัติตามมาตรฐานตามที่กำหนด ประกอบกับข้อ 41 ของประกาศที่ ทจ. 7/2558 กำหนดกรณี funding portal ไม่สามารถปฏิบัติหน้าที่ตามที่กำหนดในประกาศอย่างไม่เหมาะสม บกพร่อง หรือไม่ครบถ้วน หรือฝ่าฝืนไม่ปฏิบัติตามหลักเกณฑ์ที่กำหนด สำนักงานอาจดำเนินการให้ funding portal ชี้แจง ส่งเอกสารหรือหลักฐานที่เกี่ยวข้อง

ให้ดำเนินการแก้ไขให้เป็นไปตามหลักเกณฑ์ ให้กระทำการหรืองดเว้นกระทำการ หรือพักหรือเพิกถอนการให้ความเห็นชอบได้

หลักเกณฑ์ที่เสนอ

1.1 Funding portal ต้องจัดทำข้อตกลงกับผู้เสนอขายหลักทรัพย์เพื่อให้ทำหน้าที่เปิดเผยข้อมูลที่เพียงพอบนระบบหรือเครือข่ายอิเล็กทรอนิกส์ ซึ่งการเปิดเผยข้อมูลดังกล่าวควรครอบคลุมข้อมูลอย่างน้อย ดังนี้

1.1.1 ข้อมูลก่อนและระหว่างการเสนอขายหลักทรัพย์

(1) ข้อมูลเกี่ยวกับธุรกิจ

(ก) ชื่อ ที่อยู่ โทรศัพท์ website

(ข) รายชื่อคณะกรรมการและคณะผู้บริหาร พร้อมระบุรายละเอียดเกี่ยวกับการดำรงตำแหน่งและระยะเวลาในการดำรงตำแหน่ง รวมทั้งประสบการณ์ล่าสุดในช่วง 3 ปีที่ผ่านมาของบุคคลดังกล่าว

(ค) ลักษณะของธุรกิจ

(2) ข้อมูลทางการเงิน เช่น งบการเงินประจำปี ซึ่งต้องผ่านการตรวจสอบและแสดงความเห็นโดยผู้สอบบัญชีรับอนุญาต ผลประกอบการในอดีต ประมาณการผลการดำเนินงานหรือฐานะการเงินในอนาคต พร้อมสมมติฐานที่ใช้ในการประมาณการและคำเตือนเกี่ยวกับประมาณการดังกล่าวไม่ได้เป็นการรับประกันผลการดำเนินงานในอนาคต เป็นต้น

(3) ข้อมูลเกี่ยวกับโครงสร้างกิจการ เช่น โครงสร้างการถือหุ้น รายชื่อและสัดส่วนการถือหุ้นของผู้ถือหุ้น จำนวนพนักงาน เป็นต้น

(4) ข้อมูลเกี่ยวกับการเสนอขายหลักทรัพย์

(ก) วัตถุประสงค์ของการเสนอขายหลักทรัพย์ เช่น จะนำเงินที่ได้รับจากการเสนอขายหลักทรัพย์ไปลงทุนอะไร จำนวนค่าใช้จ่ายที่อาจเกิดขึ้น เป็นต้น

(ข) แผนโครงการทางธุรกิจ เช่น การดำเนินการในแต่ละช่วงเวลา การนำเงินที่ได้รับจากการเสนอขายไปใช้ในแต่ละช่วงเวลา ระยะเวลาที่คาดว่าโครงการจะดำเนินการแล้วเสร็จ ปัจจัยที่เกี่ยวข้องกับการดำเนินโครงการ เป็นต้น

(ค) ประเภทหลักทรัพย์ที่เสนอขาย

(ง) สัดส่วนการเสนอขายหลักทรัพย์ต่อ II/VC/PE/angel และผู้ลงทุนรายบุคคล

(จ) จำนวนหลักทรัพย์ที่เสนอขาย

(ฉ) มูลค่าการเสนอขายหลักทรัพย์ และในกรณีที่จะเสนอขายหลักทรัพย์เกินกว่าจำนวนที่ระบุไว้ (oversubscribe) ต้องเปิดเผยมูลค่าสูงสุดของหลักทรัพย์ส่วนเกินที่จะเสนอขายตั้งแต่วันแรกของการเสนอขาย รวมถึงขั้นตอนและวิธีการในการจัดสรรหลักทรัพย์ส่วนเกินดังกล่าว

(ช) ราคาหลักทรัพย์ที่เสนอขาย

(ซ) จำนวนหรือมูลค่าการจองซื้อขั้นต่ำ

(ฌ) ขั้นตอนและวิธีการในการจัดสรรหลักทรัพย์ให้ผู้ลงทุน เช่น pro-rata first come-first serve เป็นต้น

(ญ) วิธีการประเมินราคาหลักทรัพย์ที่ทำการเสนอขาย

(ฎ) วันที่เสนอขาย / ครั้งที่เสนอขาย

(ฏ) กรณีที่การเสนอขายหลักทรัพย์ถึงมูลค่าการเสนอขายที่ตั้งไว้ก่อนครบระยะเวลาที่กำหนดไว้ ผู้เสนอขายหลักทรัพย์อาจปิดการเสนอขายก่อนกำหนดระยะเวลาที่กำหนดไว้ และต้องแจ้งกำหนดระยะเวลาปิดการเสนอขายใหม่ให้ผู้ให้บริการระบบหรือเครือข่ายอิเล็กทรอนิกส์ทราบล่วงหน้าอย่างน้อย 5 วันก่อนวันที่จะปิดการเสนอขายก่อนกำหนด

(5) สิทธิในการยกเลิกการจองซื้อหลักทรัพย์

(6) ความเสี่ยงต่าง ๆ ที่ผู้ลงทุนควรทราบ เช่น ปัจจัยความเสี่ยงในธุรกิจของผู้เสนอขายหลักทรัพย์อาจมีการขายหลักทรัพย์ของธุรกิจออกไป การทำธุรกรรมที่มีความเกี่ยวโยงระหว่างผู้เสนอขายหลักทรัพย์และบุคคลที่มีความเกี่ยวโยง เป็นต้น

(7) ข้อมูลอื่น ๆ ที่มีประโยชน์ต่อการตัดสินใจลงทุน เช่น ข้อมูลที่ผู้เสนอขายหลักทรัพย์มีการเปิดเผยในแหล่งข้อมูลหรือช่องทางการสื่อสารอื่น ๆ การใช้สิทธิออกเสียงของผู้ถือหุ้นในหลักทรัพย์ที่เสนอขาย ภาระผูกพันของผู้เสนอขายหลักทรัพย์ เป็นต้น

1.1.2 <u>ข้อมูลภายหลังการเสนอขายหลักทรัพย์</u>

(1) จำนวนหลักทรัพย์ที่ขายได้ทั้งหมด

(2) ข้อมูลเกี่ยวกับความคืบหน้าในการใช้เงินที่ได้รับจากการเสนอขายหลักทรัพย์ผ่านระบบหรือเครือข่ายอิเล็กทรอนิกส์

(3) งบการเงินประจำปี ซึ่งต้องผ่านการตรวจสอบและแสดงความเห็นโดยผู้สอบบัญชีรับอนุญาต โดยให้เปิดเผยบนระบบหรือเครือข่ายอิเล็กทรอนิกส์ของ funding portal จัดส่งให้สำนักงาน 1 ฉบับ ทั้งนี้ ผู้เสนอขายหลักทรัพย์ต้องดำเนินการให้แล้วเสร็จภายใน 21 วันนับแต่วันที่ได้รับอนุมัติจากที่ประชุมใหญ่ แต่ต้องไม่เกิน 4 เดือนนับแต่วันสิ้นปีบัญชี

1.2 ในการทำข้อตกลงกับผู้เสนอขายหลักทรัพย์เพื่อให้ funding portal ทำหน้าที่เปิดเผยข้อมูล funding portal และผู้เสนอขายหลักทรัพย์อาจมีการตกลงกันเกี่ยวกับการสิ้นสุดการทำหน้าที่เปิดเผยข้อมูลของผู้เสนอขายหลักทรัพย์ภายหลังการเสนอขายหลักทรัพย์ เมื่อเกิดเหตุการณ์ใดเหตุการณ์หนึ่ง ดังนี้

1.2.1 ผู้เสนอขายหลักทรัพย์มีหน้าที่เปิดเผยข้อมูลเกี่ยวกับฐานะการเงินและผลการดำเนินงานตามมาตรา 56 ของ พ.ร.บ. หลักทรัพย์และตลาดหลักทรัพย์ พ.ศ. 2535

1.2.2 ผู้เสนอขายหลักทรัพย์เลิกกิจการ

1.2.3 ผู้เสนอขายหลักทรัพย์และ funding portal มีการตกลงเกี่ยวกับระยะเวลาที่จะสิ้นสุดการเปิดเผยข้อมูล เช่น 5 ปี 10 ปี เป็นต้น โดยผู้เสนอขายหลักทรัพย์ต้องมีช่องทางอื่นในการสื่อสารให้สมาชิกทราบข้อมูลเกี่ยวกับผู้เสนอขายหลักทรัพย์ด้วย

ทั้งนี้ ผู้เสนอขายหลักทรัพย์ต้องแจ้งให้สมาชิกทราบภายใน 5 วันนับแต่ปรากฏกรณีที่ทำให้สิ้นสุดหน้าที่การรายงาน

2. การประกอบธุรกิจอื่นของผู้ให้บริการระบบหรือเครือข่ายอิเล็กทรอนิกส์

ที่มา

ข้อ 20 ของประกาศที่ ทจ. 7/2558 กำหนดห้ามมิให้ funding portal ประกอบธุรกิจอื่นนอกเหนือจากการให้บริการระบบหรือเครือข่ายอิเล็กทรอนิกส์ที่ได้รับความเห็นชอบ เว้นแต่เป็นกิจการที่เกี่ยวเนื่อง เป็นประโยชน์ หรือสนับสนุนการประกอบธุรกิจเป็น funding portal และไม่มีลักษณะที่อาจก่อให้เกิดความขัดแย้งทางผลประโยชน์กับการเป็น funding portal เว้นแต่จะแสดงได้ว่าสามารถจัดให้มีระบบในการป้องกันความขัดแย้งทางผลประโยชน์ในเรื่องดังกล่าวได้อย่างมีประสิทธิภาพ

หลักเกณฑ์ที่เสนอ

เพื่อให้ funding portal ทราบว่า ธุรกิจใดที่ funding portal สามารถประกอบธุรกิจได้ และธุรกิจใดที่ไม่สามารถทำได้ สำนักงานจึงเห็นควรกำหนดเป็นแนวทางให้ทราบโดยทั่วกัน ดังนี้

2.1 การประกอบธุรกิจอื่นที่ funding portal ไม่สามารถดำเนินการได้ มีดังนี้

2.1.1 การให้กู้ยืมเงินหรือจัดหาแหล่งเงินทุนให้แก่สมาชิก เพื่อนำเงินมาลงทุนในหลักทรัพย์ของผู้เสนอขายหลักทรัพย์ เนื่องจากอาจทำให้พิจารณาได้ว่า funding portal มีการสนับสนุนให้สมาชิกลงทุนในหลักทรัพย์ของผู้เสนอขายหลักทรัพย์

2.1.2 การให้คำปรึกษา คำแนะนำ หรือชักชวนสมาชิก เพื่อให้มีการจองซื้อหลักทรัพย์ในระบบหรือเครือข่ายอิเล็กทรอนิกส์ของ funding portal ในลักษณะเดียวกับการเป็นที่ปรึกษาการลงทุนหรือการเป็นนายหน้าซื้อขายหลักทรัพย์

2.1.3 การใช้ระบบหรือเครือข่ายอิเล็กทรอนิกส์ของ funding portal เป็นช่องทางในการซื้อขายสินค้าหรือบริการที่ไม่เกี่ยวกับการระดมทุนผ่านระบบหรือเครือข่ายอิเล็กทรอนิกส์

2.2 การประกอบธุรกิจอื่นที่ funding portal สามารถดำเนินการได้ มีดังนี้

2.2.1 การใช้ระบบหรือเครือข่ายอิเล็กทรอนิกส์ของ funding portal ในการระดมทุนผ่านระบบหรือเครือข่ายอิเล็กทรอนิกส์ในรูปแบบอื่น เช่น donation หรือ reward เป็นต้น โดยให้ดำเนินการแสดงข้อมูลดังกล่าวออกจากข้อมูลการระดมทุนผ่านระบบหรือเครือข่ายอิเล็กทรอนิกส์อย่างชัดเจน

2.2.2 การให้บริการโฆษณาหรือประชาสัมพันธ์ให้กับผู้เสนอขายหลักทรัพย์ที่มีลักษณะดังนี้

(1) ข้อมูลหรือสาระสำคัญของข้อมูลที่ทำการโฆษณาหรือประชาสัมพันธ์ต้องไม่เกินกว่าข้อมูลการเสนอขายหลักทรัพย์ของผู้เสนอขายหลักทรัพย์ที่ได้แสดงไว้บนระบบหรือเครือข่ายอิเล็กทรอนิกส์ของ funding portal

(2) ไม่มีข้อความที่เป็นเท็จ เกินความจริง อาจก่อให้เกิดความเข้าใจผิด หรือมีลักษณะให้คุณค่าของหลักทรัพย์ที่เสนอขายบนระบบหรือเครือข่ายอิเล็กทรอนิกส์ของ funding portal ที่อาจทำให้พิจารณาได้ว่ามีการประกอบธุรกิจเป็นที่ปรึกษาการลงทุน

(3) ไม่ได้รับค่าตอบแทนเกินกว่าค่าตอบแทนปกติที่พึงได้รับเพื่อเป็นการส่งเสริมการเสนอขายหลักทรัพย์ของผู้เสนอขายหลักทรัพย์รายใดรายหนึ่งเป็นพิเศษ

2.2.3 การให้คำปรึกษาแนะนำ บ่มเพาะ พัฒนา หรือเพิ่มศักยภาพทางธุรกิจ ให้แก่กิจการอื่นในลักษณะการเป็น incubator

2.2.4 การนำทรัพย์สินที่มีอยู่ออกให้เช่าหรือหาประโยชน์อื่นใด เช่น การให้เช่า server หรือพื้นที่ส่วนที่เหลือจากการใช้งานของ funding portal เป็นต้น

2.2.5 การติดต่อหรือประสานงานกับสถาบันการเงินให้แก่ผู้เสนอขายหลักทรัพย์ที่ใช้บริการ / ให้คำปรึกษาหรือให้บริการข้อมูลแก่ผู้เสนอขายหลักทรัพย์ เกี่ยวกับผู้ให้บริการหรือบริการทางการเงินการธนาคารของสถาบันการเงินหรือบริษัททั่วไป

2.2.6 การจำหน่ายโปรแกรมคอมพิวเตอร์ที่บริษัทมีการพัฒนาเพื่อใช้ในการปฏิบัติงานอยู่แล้วหรือรับจ้างประมวลผลข้อมูลโดยใช้ capacity ส่วนที่เหลือ

2.2.7 การให้คำปรึกษาหรือให้บริการด้านงานสนับสนุนแก่ funding portal รายอื่นและบริษัททั่วไป

2.2.8 การให้คำแนะนำแก่ผู้เสนอขายหลักทรัพย์ในการจัดเตรียมข้อมูลต่าง ๆ และจัดรูปแบบของเอกสารที่ใช้ในการเสนอขายหลักทรัพย์ รวมทั้งให้คำแนะนำเกี่ยวกับกฎเกณฑ์ต่าง ๆ และประเภทของหลักทรัพย์ที่อาจเสนอขายหลักทรัพย์ได้

2.2.9 การเป็นนายทะเบียนหลักทรัพย์ และบริการที่เกี่ยวเนื่อง

2.2.10 การรับมอบสิทธิในการออกเสียงจากผู้ถือหุ้นที่มีการถือหุ้นในหลักทรัพย์ของผู้เสนอขายหลักทรัพย์ ที่มีการระดมทุนผ่านระบบหรือเครือข่ายอิเล็กทรอนิกส์บริการ โดยต้องใช้สิทธิออกเสียงให้เป็นไปตามการตัดสินใจของผู้ถือหุ้นนั้น

3. หลักทรัพย์ที่ห้ามเสนอขายผ่านระบบหรือเครือข่ายอิเล็กทรอนิกส์

<u>ที่มา</u>

ข้อ 3(2) ของประกาศที่ ทจ. 7/2558 ให้สำนักงานสามารถกำหนดแนวทางการปฏิบัติในรายละเอียดของข้อกำหนดในประกาศที่ ทจ. 7/2558 เพื่อเป็นการให้แนวทางปฏิบัติที่ถือว่าเหมาะสมและสอดคล้องตามประกาศดังกล่าว และหาก funding portal มีการปฏิบัติตามแนวทางดังกล่าวแล้ว ให้ถือว่า funding portal มีการปฏิบัติตามข้อกำหนดในประกาศดังกล่าวในเรื่องที่มีการออกแนวทางนั้นแล้ว

หลักเกณฑ์ที่เสนอ

ในการพิจารณารับหลักทรัพย์เพื่อมาเสนอขายหลักทรัพย์ผ่านระบบหรือเครือข่ายอิเล็กทรอนิกส์ของตน funding portal ต้องพิจารณาถึงวัตถุประสงค์ของการเสนอขายหลักทรัพย์ของผู้เสนอขายหลักทรัพย์ว่าต้องไม่เป็นการนำเงินที่ได้รับจากการเสนอขายหลักทรัพย์ไปใช้เพื่อวัตถุประสงค์ของโครงการดังต่อไปนี้

3.1 โครงการที่มีส่วนเกี่ยวข้องกับธุรกิจที่ไม่ชอบด้วยกฎหมาย เช่น ธุรกิจการพนัน เป็นต้น

3.2 โครงการที่มีข้อเท็จจริงซึ่งทำให้พิจารณาได้ว่าความมุ่งหมายหรือเนื้อหาสาระที่แท้จริง (substance) ของการเสนอขายหลักทรัพย์นั้นเข้าลักษณะเป็นการหลีกเลี่ยงบทบัญญัติตามกฎหมายว่าด้วยหลักทรัพย์และตลาดหลักทรัพย์

3.3 โครงการที่อาจขัดต่อนโยบายสาธารณะหรือนโยบายของรัฐ เช่น โครงการที่กระทบสิ่งแวดล้อม เป็นต้น

3.4 โครงการที่อาจก่อให้เกิดผลกระทบต่อความน่าเชื่อถือต่อตลาดทุนไทยโดยรวม

3.5 โครงการที่อาจก่อให้เกิดความเสียหายต่อผู้ลงทุนโดยรวม หรืออาจทำให้ผู้ลงทุนโดยรวมไม่ได้รับความเป็นธรรม หรือผู้ลงทุนอาจไม่ได้รับข้อมูลที่ถูกต้องหรือเพียงพอประกอบการตัดสินใจลงทุน

4. การโฆษณาและการส่งเสริมการขาย

ที่มา

ข้อ 25 วรรคสอง (3) ของประกาศที่ ทจ. 7/2558 กำหนดให้ผู้ให้บริการระบบหรือเครือข่ายอิเล็กทรอนิกส์ที่ประสงค์จะจัดให้มีการโฆษณาต้องดำเนินการให้การโฆษณานั้น มีความเหมาะสมทั้งในด้านเนื้อหา สัดส่วนของเนื้อหา และวิธีการนำเสนอ เพื่อทำให้สมาชิกได้รับข้อมูลที่จำเป็นและเป็นประโยชน์ต่อการใช้บริการของผู้ให้บริการระบบหรือเครือข่ายอิเล็กทรอนิกส์หรือต่อการตัดสินใจลงทุน โดยหลักเกณฑ์หนึ่งกำหนดให้การโฆษณาต้องไม่มีลักษณะชี้นำหรือประกันผลตอบแทนที่จะได้รับจากการลงทุน เว้นแต่ได้รับการผ่อนผันจากสำนักงาน

ข้อ 3(1) ของประกาศที่ ทจ. 7/2558 ให้สำนักงานสามารถกำหนดหลักเกณฑ์ในรายละเอียดที่กำหนดไว้ในประกาศที่ ทจ. 7/2558 ให้มีความชัดเจนเพียงพอที่ funding portal จะสามารถปฏิบัติตามประกาศได้ในแนวทางเดียวกัน ทั้งนี้ การกำหนดหลักเกณฑ์ดังกล่าวอาจกำหนดตามประเภทหลักทรัพย์หรือผู้ลงทุนก็ได้

หลักเกณฑ์ที่เสนอ

ในกรณีข้อมูลในโฆษณาจะมีลักษณะเป็นการชี้นำหรือประกันผลตอบแทนจากการลงทุนนั้น สำนักงานจะผ่อนผันการชี้นำหรือประกันผลตอบแทนในกรณีที่ข้อมูลดังกล่าวเป็นการแสดงผลการดำเนินงานในอดีตอย่างเหมาะสม หรือเป็นการประมาณการผลตอบแทนในอนาคตที่มีลักษณะครบถ้วนดังต่อไปนี้

4.1 มีข้อมูลประกอบการประมาณการอย่างเหมาะสม

4.2 มีข้อมูลความเสี่ยงที่อาจเกิดขึ้นจากการประมาณการผลตอบแทนในแต่ละเงื่อนไข

4.3 ข้อมูลตาม 4.1 และ 4.2 อยู่ในรูปแบบที่ลูกค้าสามารถเข้าใจได้อย่างถูกต้องโดยไม่สำคัญผิด

5. การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของผู้ให้บริการระบบหรือเครือข่ายอิเล็กทรอนิกส์

ที่มา

ข้อ 3(2) ของประกาศที่ ทจ. 7/2558 ให้สำนักงานสามารถกำหนดแนวทางการปฏิบัติในรายละเอียดของข้อกำหนดในประกาศที่ ทจ. 7/2558 เพื่อเป็นการให้แนวทางปฏิบัติที่ถือว่าเหมาะสมและสอดคล้องตามประกาศดังกล่าว และหาก funding portal มีการปฏิบัติตามแนวทางดังกล่าวแล้ว ให้ถือว่า funding portal มีการปฏิบัติตามข้อกำหนดในประกาศดังกล่าวในเรื่องที่มีการออกแนวทางนั้นแล้ว

หลักเกณฑ์ที่เสนอ

บทนิยาม

“ทรัพย์สินสารสนเทศ” หมายถึง

(1) ทรัพย์สินสารสนเทศ**ประเภทระบบ** ซึ่งได้แก่ ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

(2) ทรัพย์สินสารสนเทศ**ประเภทอุปกรณ์** ซึ่งได้แก่ ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด

(3) ทรัพย์สินสารสนเทศ**ประเภทข้อมูล** ซึ่งได้แก่ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

“ทรัพย์สินสารสนเทศที่มีความสำคัญ” หมายถึง ทรัพย์สินสารสนเทศที่เกี่ยวข้องหรือจำเป็นต้องใช้ประกอบกับงานที่มีความสำคัญ

“ระบบสารสนเทศที่มีความสำคัญ” หมายถึง ระบบสารสนเทศที่รองรับการปฏิบัติงานที่สำคัญ เช่น ระบบการจองซื้อ ระบบปฏิบัติการ back office เป็นต้น

“งานที่สำคัญ” หมายถึง งานที่เกี่ยวกับการให้บริการ การทำธุรกรรม หรืองานอื่น ๆ ของ funding portal ซึ่งหากมีการหยุดชะงักอาจส่งผลกระทบต่อลูกค้า การดำเนินงาน ธุรกิจ ชื่อเสียง ฐานะ และผลการดำเนินงานของ funding portal อย่างมีนัยสำคัญ

“cloud computing” หมายถึง รูปแบบการใช้งานระบบสารสนเทศร่วมกันบนระบบเครือข่ายคอมพิวเตอร์ เพื่อการประมวลผลตามความต้องการของผู้ใช้งาน ทั้งนี้ ให้อ้างอิงจากนิยามที่กำหนดโดย National Institute of Standards and Technology (NIST)

“ผู้ให้บริการภายนอก” หมายถึง บุคคลจากภายนอกองค์กรซึ่ง funding portal ว่าจ้างเพื่อใช้บริการที่เกี่ยวข้องกับระบบสารสนเทศ

“สิ่งอำนวยความสะดวกในการประมวลผลข้อมูล (information processing facility)” หมายถึง อุปกรณ์ ระบบงาน หรือสภาพแวดล้อม ที่จำเป็นหรือมีส่วนช่วยให้การประมวลผลข้อมูลเป็นไปอย่างครบถ้วน ถูกต้อง และมีประสิทธิภาพ เช่น อุปกรณ์หรือโปรแกรมประมวลผลข้อมูล ระบบเครือข่ายคอมพิวเตอร์ ขั้นตอนหรือสถานที่ประมวลผลข้อมูล เป็นต้น

5.1 <u>นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Policy) และการควบคุมการปฏิบัติงานให้เป็นไปตามข้อกำหนด (Compliance)</u>

5.1.1 นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (information security policy)

<u>ที่มา</u>

เพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และได้รับทราบถึงหน้าที่ความรับผิดชอบและแนวทางปฏิบัติในการควบคุมความเสี่ยงต่าง ๆ โดย funding portal ต้องจัดให้มีนโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ โดยคำนึงถึงลักษณะ ขนาด และความซับซ้อนของการประกอบธุรกิจ รวมทั้งกฎเกณฑ์ต่าง ๆ ที่เกี่ยวข้อง

<u>แนวทางปฏิบัติ</u>

1. Funding portal ควรจัดให้มีนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศอย่างเป็นลายลักษณ์อักษร โดยได้รับการอนุมัติจากคณะกรรมการบริษัทหรือคณะกรรมการอื่นที่คณะกรรมการบริษัทมอบหมาย และเผยแพร่นโยบายดังกล่าวในลักษณะที่ให้ผู้ใช้งานเข้าถึงได้ง่าย เพื่อให้บุคลากรที่เกี่ยวข้องทราบและถือปฏิบัติให้เป็นไปตามที่นโยบายกำหนด
2. นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศควรมีเนื้อหาขั้นต่ำครอบคลุมในเรื่องดังต่อไปนี้

2.1 การรักษาความปลอดภัยต่อทรัพย์สินสารสนเทศ

(1) การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ (access control)

(2) การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (physical and environmental security)

2.2 การจัดการข้อมูลสารสนเทศและการรักษาความลับ

(1) การจำแนกประเภทของข้อมูลสารสนเทศ (information classification) เพื่อกำหนดมาตรการรักษาความมั่นคงปลอดภัย

(2) การสำรองข้อมูล (backup)

2.3 การควบคุมดูแลบุคลากรผู้ปฏิบัติงาน

(1) การควบคุมการใช้งานของผู้ใช้งาน (end user) เช่น มาตรการป้องกันอุปกรณ์สารสนเทศระหว่างที่ไม่มีผู้ใช้งาน (protection of unattended user equipment)

(2) การควบคุมดูแลผู้ให้บริการภายนอก (supplier relationships)

2.4 การจัดการระบบเครือข่ายคอมพิวเตอร์และการรับส่งข้อมูลสารสนเทศ

(1) การรักษาความมั่นคงปลอดภัยด้านการสื่อสารและระบบเครือข่ายคอมพิวเตอร์ (communications security)

(2) การควบคุมการรับส่งข้อมูลสารสนเทศ (information transfer)

2.5 การป้องกันภัยคุกคามต่อระบบสารสนเทศ

(1) การป้องกันโปรแกรมไม่ประสงค์ดี (protection from malware)

(2) การบริหารจัดการช่องโหว่ทางเทคนิค (technical vulnerability management)

3. Funding portal ควรจัดให้มีขั้นตอนและวิธีการปฏิบัติงานให้เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศที่ได้กำหนดไว้

4. Funding portal ควรจัดให้มีการทบทวนหรือปรับปรุงนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงของสภาพแวดล้อมต่าง ๆ ที่อาจส่งผลกระทบต่อการประกอบธุรกิจอย่างมีนัยสำคัญ เช่น การเปลี่ยนแปลงสภาพธุรกิจ หลักเกณฑ์ กฎหมาย และเทคโนโลยี เป็นต้น พร้อมทั้งปรับปรุงขั้นตอนและวิธีการปฏิบัติงานให้สอดคล้องกับนโยบายที่เปลี่ยนแปลงไป

5. ผู้บริหารระดับสูงควรกำหนดรายละเอียดหน้าที่ความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศอย่างเป็นลายลักษณ์อักษรให้เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ รวมทั้งจัดสรรหน้าที่ความรับผิดชอบและกำหนดแนวทางในการปฏิบัติหน้าที่ให้กับพนักงาน เพื่อให้มั่นใจได้ว่าบุคคลดังกล่าวสามารถปฏิบัติหน้าที่ด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศได้อย่างครบถ้วน

5.1.2 การควบคุมการปฏิบัติงานให้เป็นไปตามข้อกำหนด (compliance)

ที่มา

เพื่อให้การบริหารจัดการความมั่นคงปลอดภัยของระบบสารสนเทศเป็นไปตามนโยบายและหลักปฏิบัติของ funding portal

แนวทางปฏิบัติ

Funding portal ควรจัดให้มีการตรวจสอบขั้นตอนและการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศให้เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศโดยผู้ตรวจสอบที่เป็นอิสระจากการบริหารจัดการความมั่นคงปลอดภัยของระบบสารสนเทศ ซึ่งอาจเป็นหน่วยงานตรวจสอบภายในของ funding portal หรือผู้ตรวจสอบภายนอกตามการประเมินความเสี่ยงของ funding portal และเมื่อมีเหตุการณ์ที่มีนัยสำคัญ

5.2 การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร (Human Resource Security)

ที่มา

เพื่อให้พนักงานและบุคคลภายนอกที่ปฏิบัติงานโดยเชื่อมต่อกับข้อมูลหรือระบบงานภายในองค์กรมีความตระหนักรู้ และปฏิบัติงานโดยคำนึงถึงการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

แนวทางปฏิบัติ

1. Funding portal ควรจัดให้มีการสร้างความตระหนักรู้ (awareness) เกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศแก่พนักงานและบุคคลภายนอกที่ปฏิบัติงานโดยเชื่อมต่อกับข้อมูลหรือระบบงานภายในองค์กรอย่างสม่ำเสมอ โดยมีเนื้อหาสอดคล้องกับนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และหน้าที่ความรับผิดชอบ

2. Funding portal ควรสื่อสารให้พนักงานและบุคคลภายนอกที่ปฏิบัติงานโดยเชื่อมต่อกับข้อมูลหรือระบบงานภายในองค์กรระมัดระวังและละเว้นการใช้งานระบบสารสนเทศในลักษณะที่อาจก่อให้เกิดความเสียหายกับ funding portal ตลาดทุนโดยรวม หรือความมั่นคงของประเทศ เช่น การหมิ่นประมาท การข่มขู่ การปลอมแปลงเป็นบุคคลอื่น การส่งจดหมายอิเล็กทรอนิกส์แบบลูกโซ่ และการเปิดเผยข้อมูลที่เป็นความลับของ funding portal เป็นต้น

3. Funding portal ควรสื่อสารให้พนักงานและบุคคลภายนอกที่ปฏิบัติงานโดยเชื่อมต่อกับข้อมูลหรือระบบงานภายในองค์กร ตระหนักและสังเกตถึงความผิดปกติใด ๆ ที่เป็นสาระสำคัญซึ่งอาจส่งผลต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (security weaknesses) และรายงานบุคคลหรือหน่วยงานที่ทำหน้าที่รับแจ้งสถานการณ์ (point of contact) โดยไม่ชักช้า เมื่อพบความผิดปกติดังกล่าวทุกครั้ง

5.3 การบริหารจัดการทรัพย์สินสารสนเทศ (Asset Management)

ที่มา

เพื่อให้ข้อมูลและทรัพย์สินสารสนเทศที่มีความสำคัญได้รับการปกป้องในระดับที่เหมาะสมตามระดับความสำคัญ

แนวทางปฏิบัติ

1. Funding portal ควรกำหนดให้มีการจำแนกทรัพย์สินสารสนเทศประเภทข้อมูลสารสนเทศตามระดับชั้นความลับ และทรัพย์สินสารสนเทศอื่น ๆ ตามระดับความสำคัญต่อ funding portal และทบทวนการจำแนกประเภทดังกล่าวอย่างสม่ำเสมอ

2. Funding portal ควรจัดให้มีมาตรการดูแลรักษาความมั่นคงปลอดภัยที่สอดคล้องเหมาะสมกับทรัพย์สินสารสนเทศแต่ละประเภทที่ได้จำแนกไว้ เช่น การควบคุมการเข้าถึงการจัดให้มีการเข้ารหัสข้อมูลที่เป็นความลับหรือต้องการความถูกต้องในระดับสูง เป็นต้น

5.4 การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ (Access Control)

5.4.1 การควบคุมการเข้าถึงตามข้อกำหนดทางธุรกิจ (business requirements of access control)

ที่มา

เพื่อควบคุมการเข้าถึงข้อมูลและสิ่งอำนวยความสะดวกในการประมวลผลข้อมูล (information processing facilities)

แนวทางปฏิบัติ

Funding portal ควรจัดให้มีนโยบายควบคุมการเข้าถึงข้อมูลและสิ่งอำนวยความสะดวกในการประมวลผลข้อมูล (information processing facilities) ต่าง ๆ เช่น อุปกรณ์หรือโปรแกรมประมวลผลข้อมูล ระบบเครือข่ายคอมพิวเตอร์ ขั้นตอนหรือสถานที่ประมวลผลข้อมูลตามที่ funding portal กำหนด เป็นต้น เพื่อควบคุมการเข้าถึงเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น โดยจัดทำเป็นลายลักษณ์อักษรและทบทวนนโยบายดังกล่าวอย่างสม่ำเสมอ ทั้งนี้ นโยบายดังกล่าวต้องสอดคล้องกับข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ โดยขั้นต่ำควรครอบคลุมเรื่องดังต่อไปนี้

1. การกำหนดสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศให้เหมาะสมกับการใช้งานและหน้าที่ความรับผิดชอบของผู้ใช้งาน รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ และยกเลิกสิทธิของบุคคลที่ไม่มีความจำเป็นในการเข้าถึงโดยทันที

2. การแบ่งแยกบทบาทหน้าที่ของบุคคลที่เกี่ยวข้อง เช่น บุคคลผู้ร้องขอ (access request) บุคคลผู้มีอำนาจอนุมัติ (access authorization) และบุคคลผู้บริหารสิทธิการเข้าถึง (access administration) เป็นต้น

5.4.2 การบริหารจัดการบัญชีผู้ใช้งาน (user access management)

ที่มา

เพื่อให้มีการควบคุมสิทธิการใช้งานระบบสารสนเทศอย่างเหมาะสมและป้องกันไม่ให้ผู้ที่ไม่มีสิทธิใช้งานสามารถเข้าถึงระบบสารสนเทศได้

แนวทางปฏิบัติ

1. Funding portal ควรจัดให้มีการลงทะเบียนบัญชีผู้ใช้งานระบบสารสนเทศ (user registration) และยกเลิกบัญชีผู้ใช้งานอย่างเป็นทางการ เพื่อควบคุมการให้สิทธิและการยกเลิกสิทธิในการเข้าถึง

2. ในการกำหนดสิทธิการเข้าถึงระดับสูง (privileged access rights) funding portal ควรจัดสรรอย่างจำกัดและอยู่ภายใต้การควบคุมอย่างเคร่งครัด

3. Funding portal ควรจัดให้มีขั้นตอนการบริหารจัดการเรื่องการกำหนดรหัสผ่าน (user password management) อย่างเหมาะสม

4. Funding portal ควรจัดให้มีการติดตามทบทวนระดับสิทธิการเข้าถึงอย่างสม่ำเสมอ และยกเลิกสิทธิการเข้าถึงโดยทันที เมื่อบุคคลที่ได้รับสิทธิลาออก เลิกสัญญาว่าจ้าง หรือเปลี่ยนแปลงหน้าที่ปฏิบัติงาน

5.4.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities)

ที่มา

เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิ สามารถเข้าถึงระบบสารสนเทศได้

แนวทางปฏิบัติ

Funding portal ควรจัดให้มีข้อบังคับให้ผู้ใช้งานดูแลรับผิดชอบบัญชีผู้ใช้งาน (user ID) และรหัสผ่าน (password) รวมทั้งข้อมูลส่วนบุคคลที่อาจนำมาใช้เพื่อขอเปลี่ยนแปลงข้อมูลบัญชีการใช้งานระบบได้อย่างมั่นคงปลอดภัย (accountable for safeguard)

5.4.4 การควบคุมการเข้าถึงระบบสารสนเทศและแอพพลิเคชั่น (system and application access control)

ที่มา

เพื่อป้องกันการเข้าถึงระบบสารสนเทศและแอพพลิเคชั่นโดยไม่ได้รับอนุญาต

แนวทางปฏิบัติ

1. Funding portal ควรจัดให้มีควบคุมการเข้าถึงข้อมูลสารสนเทศและฟังก์ชั่นต่าง ๆ ในแอพพลิเคชั่นของผู้ใช้งาน และผู้ดูแลระบบสารสนเทศ โดยให้สอดคล้องกับสิทธิที่ได้รับ

2. Funding portal ควรจัดให้มีควบคุมการเข้าใช้งาน (log-on) ระบบสารสนเทศและแอพพลิเคชั่น เช่น มีการป้องกันการเข้าใช้งานโดยวิธีเดาสุ่ม (brute force) แจ้งเตือนกรณีที่มีความพยายามเข้าใช้งานอย่างไม่เหมาะสม (breach of log-on control) และจัดเก็บหลักฐานดังกล่าว เป็นต้น

3. Funding portal ควรจัดให้มีระบบการบริหารจัดการรหัสผ่านที่มีความมั่นคงปลอดภัย โดยอาจพิจารณากำหนดกระบวนการที่จำเป็น ดังนี้

(1) กำหนดให้ผู้ใช้งานแต่ละรายรับผิดชอบ (accountable) บัญชีผู้ใช้งาน (user ID) และรหัสผ่าน (password) ของตนเอง

(2) ให้ผู้ใช้งานสามารถตั้งค่าหรือเปลี่ยนแปลงรหัสผ่านได้ด้วยตนเอง และระบบควรมีขั้นตอนให้ยืนยันความถูกต้อง

(3) บังคับให้ผู้ใช้งานตั้งรหัสผ่านที่ยากต่อการคาดเดา เช่น มีความยาวขั้นต่ำ 6 - 8 ตัวอักษร โดยอาจมีอักขระพิเศษ (เช่น “#”) ประกอบด้วย

(4) บังคับให้ผู้ใช้งานเปลี่ยนแปลงรหัสผ่านทันทีที่ได้รับรหัสผ่านครั้งแรก และควรเปลี่ยนรหัสผ่านอย่างน้อยทุก 6 เดือน

(5) ในการเปลี่ยนรหัสผ่านแต่ละครั้ง ไม่ควรกำหนดรหัสผ่านใหม่ให้ซ้ำกับรหัสที่ใช้งานครั้งล่าสุด

(6) ระหว่างที่ผู้ใช้งานใส่รหัสผ่าน ระบบไม่ควรแสดงให้เห็นค่ารหัสผ่านบนหน้าจอ

(7) ควรมีระบบการเข้ารหัส (encryption) ข้อมูลรหัสผ่าน เพื่อป้องกันการล่วงรู้หรือแก้ไขเปลี่ยนแปลง รวมทั้งไม่จัดเก็บข้อมูลรหัสผ่านใน folder เดียวกันกับ folder ที่จัดเก็บข้อมูลของแอพพลิเคชั่น

(8) ควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด ซึ่งในทางปฏิบัติโดยทั่วไปไม่ควรเกิน 10 ครั้ง

(9) ควรมีวิธีการจัดส่งรหัสผ่านให้แก่ผู้ใช้งานอย่างรัดกุมและปลอดภัย เช่น การใส่ซองปิดผนึก เป็นต้น

5.5 <u>การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (Physical and Environmental Security)</u>

5.5.1 พื้นที่หวงห้าม (secure areas)

<u>ที่มา</u>

เพื่อป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึงพื้นที่หวงห้าม เช่น ศูนย์คอมพิวเตอร์ (data center) เป็นต้น และพื้นที่ที่ตั้งอุปกรณ์ระบบเครือข่ายคอมพิวเตอร์ ได้แก่ floor switch หรือ router ซึ่งอาจก่อให้เกิดความเสียหายต่ออุปกรณ์สารสนเทศหรือมีผลกระทบต่อข้อมูลที่เป็นความลับหรือมีความสำคัญ

<u>แนวทางปฏิบัติ</u>

1. Funding portal ควรประเมินความเสี่ยงและกำหนดระดับความสำคัญของทรัพย์สินสารสนเทศ พร้อมทั้งกำหนดพื้นที่การจัดวางทรัพย์สินสารสนเทศที่มีความสำคัญให้เป็นพื้นที่หวงห้าม (physical security perimeter)

2. Funding portal ควรกำหนดสิทธิการเข้าออกพื้นที่หวงห้ามให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้องภายใต้หลักความจำเป็นในการรู้ข้อมูล (need-to-know basis) รวมทั้งควรจัดให้มีระบบการควบคุมการเข้าออกอย่างรัดกุม และทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ funding portal ควรติดตามและควบคุมบุคคลภายนอกที่เข้าปฏิบัติงานภายในพื้นที่หวงห้ามอย่างใกล้ชิด

3. Funding portal ควรจัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น เครื่องแม่ข่าย เป็นต้น ไว้ในพื้นที่หวงห้ามอย่างมั่นคงปลอดภัย

5.5.2 อุปกรณ์สารสนเทศ (equipment)

<u>ที่มา</u>

เพื่อป้องกันทรัพย์สินสารสนเทศประเภทอุปกรณ์มิให้สูญหาย ถูกโจรกรรม เกิดความเสียหาย เข้าถึง หรือถูกใช้งานโดยบุคคลที่ไม่เกี่ยวข้อง รวมทั้งเพื่อให้ทรัพย์สินดังกล่าวสามารถทำงานได้อย่างต่อเนื่อง

<u>แนวทางปฏิบัติ</u>

Funding portal ควรจัดให้มีการควบคุมป้องกันทรัพย์สินสารสนเทศประเภทอุปกรณ์ระหว่างที่ไม่มีผู้ใช้งาน (unattended user equipment) ให้มีความปลอดภัย รวมทั้งควรกำหนดการควบคุมเอกสาร ข้อมูล หรือสื่อบันทึกข้อมูลต่าง ๆ เช่น thumbdrive และ external harddisk ที่มีข้อมูลสารสนเทศที่จัดเก็บหรือบันทึกอยู่ไม่ให้วางทิ้งไว้บนโต๊ะทำงานหรือสถานที่ไม่ปลอดภัยในขณะที่ไม่ได้ใช้งาน (clear desk)

ตลอดจนการควบคุมหน้าจอคอมพิวเตอร์ไม่ให้มีข้อมูลสำคัญปรากฏในขณะที่ไม่ได้ใช้งาน (clear screen) เช่น การตัดออกจากระบบ (session time out) และการล็อคหน้าจอ (lock screen) อัตโนมัติ เป็นต้น

5.6 <u>การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ (Operations Security)</u>

5.6.1 หน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติงาน (operational procedures and responsibilities)

<u>ที่มา</u>

เพื่อให้มั่นใจว่าการปฏิบัติงานด้านระบบสารสนเทศเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย

<u>แนวทางปฏิบัติ</u>

1. Funding portal ควรจัดให้มีวิธีปฏิบัติงานด้านระบบสารสนเทศที่สำคัญเป็นลายลักษณ์อักษรเพื่อให้พนักงานปฏิบัติการคอมพิวเตอร์ (computer operator) สามารถปฏิบัติงานได้อย่างถูกต้องและเป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ เช่น ขั้นตอนในการเปิด-ปิดระบบการประมวลผล การตรวจสอบประสิทธิภาพการทำงานของระบบ และตารางเวลาในการปฏิบัติงาน เป็นต้น และควรทบทวนวิธีปฏิบัติดังกล่าวให้เป็นปัจจุบันอยู่เสมอ รวมทั้งจัดให้วิธีปฏิบัติงานดังกล่าวอยู่ในสภาพที่พร้อมใช้งานและเข้าถึงได้

2. Funding portal ควรติดตามประสิทธิภาพการทำงานของระบบสารสนเทศและทรัพย์สินสารสนเทศประเภทอุปกรณ์ที่สำคัญให้ทำงานได้อย่างต่อเนื่องและมีประสิทธิภาพ เพื่อใช้เป็นข้อมูลในการประเมินสมรรถภาพและความเพียงพอ (capacity) ของระบบสารสนเทศ ทรัพย์สินสารสนเทศประเภทอุปกรณ์ และบุคลากร เพื่อให้สามารถรองรับแผนการปฏิบัติงานในอนาคตได้อย่างมีประสิทธิภาพด้วย

3. Funding portal ควรแบ่งแยกส่วนคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงาน (develop environment) และใช้งานจริง (production environment) ออกจากกัน และควบคุมให้มีการเข้าถึงเฉพาะผู้ที่เกี่ยวข้องในแต่ละส่วนเท่านั้น ทั้งนี้ การแบ่งแยกส่วนดังกล่าวอาจแบ่งโดยใช้เครื่องคอมพิวเตอร์คนละเครื่อง หรือแบ่งโดยการจัดเนื้อที่แยกไว้ต่างหากภายในเครื่องคอมพิวเตอร์เดียวกันก็ได้

5.6.2 การป้องกันภัยคุกคามจากโปรแกรมไม่ประสงค์ดี (protection from malware)

<u>ที่มา</u>

เพื่อให้มั่นใจว่าระบบสารสนเทศได้รับการป้องกันภัยคุกคามจากโปรแกรมไม่ประสงค์ดี

<u>แนวทางปฏิบัติ</u>

Funding portal ควรจัดให้มีการป้องกันและตรวจสอบโปรแกรมไม่ประสงค์ดี เช่น การตรวจสอบการติดตั้งซอฟต์แวร์ที่ไม่เหมาะสม การติดตั้งซอฟต์แวร์ตรวจสอบโปรแกรมไม่ประสงค์ดี เป็นต้น รวมทั้งแก้ไขเพื่อให้ระบบกลับมาใช้งานได้ตามปกติ (recovery) โดยขั้นต่ำควรกำหนดมาตรการ ดังนี้

1. ติดตั้งซอฟต์แวร์ตรวจสอบโปรแกรมไม่ประสงค์ดี และปรับปรุงให้เป็นปัจจุบันอย่างสม่ำเสมอ พร้อมทั้งกำหนดผู้มีหน้าที่รับผิดชอบให้รายงานและแก้ไขปัญหากรณีพบภัยคุกคาม

2. จัดให้มีการติดตามและกลั่นกรองข่าวสารเกี่ยวกับภัยคุกคาม เพื่อให้ทราบข้อเท็จจริง รวมทั้งแจ้งให้ผู้ที่เกี่ยวข้องได้ตระหนักถึงภัยคุกคามดังกล่าว

5.6.3 การสำรองข้อมูล (backup)

ที่มา

เพื่อป้องกันการสูญหายของข้อมูล

แนวทางปฏิบัติ

Funding portal ควรจัดให้มีนโยบายสำรองข้อมูลสำคัญทางธุรกิจ รวมถึงระบบปฏิบัติการ (operating system) แอพพลิเคชั่นระบบงานคอมพิวเตอร์ (application system) และชุดคำสั่งที่ใช้ทำงานให้ครบถ้วน ให้สามารถพร้อมใช้งานได้อย่างต่อเนื่อง โดยขั้นต่ำควรพิจารณา ดังนี้

1. กำหนดขั้นตอนหรือวิธีปฏิบัติในการสำรองข้อมูลเพื่อเป็นแนวทางให้แก่ผู้ปฏิบัติงาน โดยอย่างน้อยควรมีรายละเอียดเกี่ยวกับ

1.1 ข้อมูลที่สำรอง

1.2 ความถี่ในการสำรอง

1.3 ประเภทสื่อบันทึกข้อมูล

1.4 จำนวนที่สำรอง

1.5 ขั้นตอนและวิธีการสำรองโดยละเอียด

1.6 สถานที่และวิธีการเก็บรักษาสื่อบันทึกข้อมูลสำรอง ให้มีความปลอดภัย

1.7 กระบวนการกู้คืนข้อมูลในกรณีที่สูญหาย

2. กำหนดเป้าหมายในการกู้คืนข้อมูล เช่น กำหนดประเภทของข้อมูล และชุดข้อมูลล่าสุดที่จะกู้คืนได้ (recovery point objective : RPO)

3. จัดให้มีการทดสอบข้อมูลสำรองและกระบวนการกู้คืนข้อมูลอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าข้อมูลรวมทั้งโปรแกรมระบบต่าง ๆ ที่ได้สำรองไว้ มีความถูกต้องครบถ้วนและสามารถใช้งานได้ภายในระยะเวลาที่กำหนด

4. ในกรณีที่จำเป็นต้องจัดเก็บข้อมูลเป็นระยะเวลานาน ควรคำนึงถึงวิธีการนำข้อมูลกลับมาใช้งานในอนาคตด้วย เช่น กรณีที่จัดเก็บข้อมูลในสื่อบันทึกประเภทใด ต้องมีการเก็บอุปกรณ์และโปรแกรมที่เกี่ยวข้องสำหรับใช้อ่านสื่อบันทึกประเภทนั้นไว้ด้วยเช่นกัน เป็นต้น

5.6.4 การบันทึก จัดเก็บหลักฐานและติดตาม (logging and monitoring)

ที่มา

เพื่อบันทึกและจัดเก็บหลักฐานการใช้งานเกี่ยวกับระบบสารสนเทศอย่างครบถ้วนและเพียงพอสำหรับการสอบทานการใช้งานข้อมูลและระบบสารสนเทศตามหน้าที่ที่ผู้ปฏิบัติงานได้รับมอบหมาย

การตรวจสอบการเข้าใช้งานระบบสารสนเทศโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง การตรวจสอบและป้องกันการใช้งานระบบสารสนเทศที่มีความผิดปกติหรือไม่เป็นไปตามกฎหมายหรือหลักเกณฑ์ของทางการ และการตรวจสอบตัวตนของลูกค้า รวมทั้งเพื่อให้มีการติดตามและวิเคราะห์หลักฐานที่จัดเก็บ

แนวทางปฏิบัติ

1. Funding portal ควรจัดให้มีการบันทึกและจัดเก็บหลักฐาน (logs) ของระบบงานที่มีความสำคัญประเภทต่าง ๆ ดังต่อไปนี้

1.1 หลักฐานการเข้าถึงระบบปฏิบัติการ ฐานข้อมูล ระบบเครือข่าย คอมพิวเตอร์ (authentication log) โดยขั้นต่ำควรมีรายละเอียดเกี่ยวกับบัญชีผู้ใช้งาน วันเวลาที่เข้าใช้งาน และความพยายามในการเข้าใช้งาน โดยจัดเก็บเป็นระยะเวลาไม่น้อยกว่า 3 เดือน

1.2 หลักฐานการเข้าถึงและใช้งานระบบสารสนเทศ เช่น ระบบการจองซื้อ ระบบปฏิบัติการ back office หรือระบบงานอื่น ๆ ที่ funding portal กำหนด (application log) โดยขั้นต่ำต้องมีรายละเอียดเกี่ยวกับบัญชีผู้ใช้งาน หมายเลขประจำเครื่องที่สามารถระบุเครื่องที่ใช้งานได้ เช่น IP address เป็นต้น วันเวลาที่มีการใช้งาน ประเภทการดำเนินการ (transaction type) และรหัสอ้างอิงรายการ (reference ID) โดยจัดเก็บเป็นระยะเวลาไม่น้อยกว่า 2 ปี

2. Funding portal ควรจัดให้มีการป้องกันระบบการบันทึกและจัดเก็บหลักฐานการใช้งานระบบสารสนเทศที่มีความสำคัญ จากการถูกเปลี่ยนแปลงแก้ไข ทำความเสียหาย หรือเข้าถึงโดยไม่ได้รับอนุญาต

3. Funding portal ควรจัดให้มีการติดตามและวิเคราะห์หลักฐานที่ถูกจัดเก็บสำหรับการใช้งานระบบสารสนเทศที่มีความสำคัญ โดยให้สอดคล้องกับการประเมินความเสี่ยงขององค์กร และเป็นไปตามที่กำหนดไว้ในนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

5.6.5 การบริหารจัดการช่องโหว่ทางเทคนิค (technical vulnerability management)

ที่มา

เพื่อป้องกันภัยคุกคามจากช่องโหว่ทางเทคนิค

แนวทางปฏิบัติ

Funding portal ควรจัดให้มีการติดตามข้อมูลข่าวสารเกี่ยวกับช่องโหว่ทางเทคนิคที่อาจเป็นความเสี่ยงต่อระบบสารสนเทศของ funding portal อย่างทันต่อเหตุการณ์ รวมทั้งควรจัดให้มีการตรวจสอบหาช่องโหว่ดังกล่าว และมีมาตรการดำเนินการเพื่อปิดช่องโหว่หรือกำหนดแผนรองรับกรณีที่ระบบถูกบุกรุกผ่านช่องโหว่ดังกล่าว โดยขั้นต่ำควรกำหนดแนวทางดำเนินการดังนี้

1. กำหนดผู้มีหน้าที่รับผิดชอบในการติดตามและจัดการเกี่ยวกับช่องโหว่ทางเทคนิค โดยครอบคลุมถึงการประเมินความเสี่ยงของทรัพย์สินสารสนเทศที่เกี่ยวข้องซึ่งอาจได้รับผลกระทบจากช่องโหว่ดังกล่าว โดยเฉพาะทรัพย์สินสารสนเทศที่มีความเสี่ยงสูง การดำเนินการเพื่อปิดช่องโหว่ (patching) และการประสานงานกับบุคคลที่เกี่ยวข้อง

2. มีการประเมินความเสี่ยงของโปรแกรมเพื่อปิดช่องโหว่ (patches) โดยก่อนการติดตั้งโปรแกรมต้องมีการทดสอบและประเมินผลกระทบที่อาจเกิดจากการติดตั้งโปรแกรมดังกล่าว ทั้งนี้ กรณีที่ไม่มีโปรแกรมเพื่อปิดช่องโหว่ ให้ปฏิบัติตามคำแนะนำของบริษัทผู้ผลิตทรัพย์สินสารสนเทศที่เกี่ยวข้อง

3. มีการบันทึกและจัดเก็บหลักฐานเพื่อการตรวจสอบในการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับการจัดการช่องโหว่ทางเทคนิค

5.6.6 การตรวจสอบระบบสารสนเทศ (information systems audit)

ที่มา

เพื่อจัดให้มีการวางแผนการตรวจสอบระบบสารสนเทศอย่างเพียงพอเหมาะสม โดยการตรวจสอบดังกล่าวต้องส่งผลกระทบต่อการปฏิบัติงานน้อยที่สุด

แนวทางปฏิบัติ

1. Funding portal ควรจัดให้มีการวางแผนการตรวจสอบระบบสารสนเทศให้สอดคล้องกับความเสี่ยงที่ได้ประเมินไว้

2. Funding portal ควรกำหนดขอบเขตการตรวจสอบทางเทคนิค (technical audit test) ให้ครอบคลุมจุดเสี่ยงที่สำคัญ และควรควบคุมการตรวจสอบดังกล่าวไม่ให้กระทบต่อการปฏิบัติงานตามปกติ

3. ในกรณีที่การตรวจสอบระบบสารสนเทศมีโอกาสกระทบต่อความพร้อมใช้งานของระบบ (system availability) funding portal ควรแจ้งกำหนดการล่วงหน้าเพื่อลดผลกระทบที่เกิดขึ้นจากการดำเนินการ

5.7 การรักษาความมั่นคงปลอดภัยด้านการสื่อสารและระบบเครือข่ายคอมพิวเตอร์ (Communications Security)

5.7.1 การบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ (network security management)

ที่มา

เพื่อป้องกันการกระทำที่มีความเสี่ยงต่อข้อมูลสารสนเทศในระบบเครือข่ายคอมพิวเตอร์ และป้องกันโครงสร้างพื้นฐานที่สนับสนุนระบบเครือข่ายคอมพิวเตอร์

แนวทางปฏิบัติ

1. Funding portal ควรจัดให้มีการบริหารจัดการและควบคุมระบบเครือข่ายคอมพิวเตอร์อย่างมั่นคงปลอดภัย โดยขั้นต่ำควรมีการดำเนินการดังนี้

1.1 กำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้เฉพาะบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

1.2 มีวิธีการที่สามารถระบุถึงอุปกรณ์ที่เชื่อมต่อบนเครือข่ายได้อย่างชัดเจน เช่น IP address และประเภทของอุปกรณ์ เป็นต้น

2. มีการควบคุมการเชื่อมต่อกับระบบเครือข่ายสาธารณะ (public network) และระบบเครือข่ายไร้สาย (wireless network) อย่างรัดกุม เพื่อป้องกันการรั่วไหลหรือเปลี่ยนแปลงแก้ไขข้อมูลที่ส่งผ่านระบบเครือข่ายดังกล่าว

3. Funding portal ควรจัดทำข้อตกลงการใช้บริการระบบเครือข่ายคอมพิวเตอร์ (network services agreements) กับผู้ให้บริการภายนอก โดยมีเนื้อหาครอบคลุมถึงวิธีการบริหารจัดการคุณภาพการให้บริการ รวมทั้งกระบวนการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายคอมพิวเตอร์

4. Funding portal ควรจัดให้มีการแบ่งแยกระบบเครือข่ายคอมพิวเตอร์ตามความเหมาะสม โดยระบุขอบเขต (domain) ของระบบเครือข่ายย่อยอย่างชัดเจน และจัดให้มีกระบวนการควบคุมการเข้าถึงขอบเขตดังกล่าวโดยสอดคล้องเหมาะสมกับระดับความต้องการด้านการรักษาความมั่นคงปลอดภัยของแต่ละขอบเขตที่ถูกจัดแบ่ง

5.7.2 การควบคุมการรับส่งข้อมูลสารสนเทศ (information transfer)

ที่มา

เพื่อรักษาความมั่นคงปลอดภัยในการรับส่งข้อมูลสารสนเทศผ่านระบบเครือข่ายภายในองค์กร และระหว่างระบบเครือข่ายภายในองค์กรกับระบบเครือข่ายภายนอก

แนวทางปฏิบัติ

1. Funding portal ควรจัดให้มีนโยบายและหลักปฏิบัติเพื่อปกป้องข้อมูลสารสนเทศที่รับส่งผ่านระบบและอุปกรณ์ในการสื่อสารทุกประเภท โดยมีเนื้อหาขั้นต่ำครอบคลุมถึง

1.1 แนวปฏิบัติที่ดีในการรับส่งข้อมูลสารสนเทศผ่านช่องทางการสื่อสารอิเล็กทรอนิกส์ประเภทต่าง ๆ

1.2 นำเทคนิคการเข้ารหัสข้อมูลมาใช้ในการรับส่งข้อมูลสารสนเทศที่เป็นความลับและมีความสำคัญผ่านช่องทางการสื่อสารบางประเภทที่ต้องการการรักษาความมั่นคงปลอดภัย เช่น การใช้งานระบบ cloud computing เป็นต้น

2. Funding portal ควรจัดให้พนักงานและผู้ให้บริการภายนอก มีการทำสัญญารักษาความลับหรือไม่เปิดเผยข้อมูลที่มีความสำคัญ โดยขั้นต่ำต้องมีเนื้อหาครอบคลุมถึง

2.1 การระบุความเป็นเจ้าของข้อมูลสำคัญทางธุรกิจ ทรัพย์สินทางปัญญาและวิธีป้องกันการรั่วไหลของข้อมูล

2.2 การป้องกันการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต ต้องจัดให้มีการลงนามผู้รับผิดชอบ

2.3 การกำหนดขั้นตอนการขออนุญาตเข้าถึงข้อมูลหรือกำหนดสิทธิการเข้าถึงข้อมูลตามที่ได้ลงนาม

2.4 การกำหนดสิทธิการเข้าถึงข้อมูลเพื่อตรวจสอบหรือติดตามการใช้งานข้อมูลที่มีความสำคัญ

2.5 การกำหนดกระบวนการแจ้งเตือนและรายงานผู้เกี่ยวข้องหากพบการรั่วไหลหรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

2.6 การกำหนดมาตรการดำเนินการกรณีละเมิดหรือยกเลิกสัญญา รวมทั้งข้อกำหนดในการคืนหรือทำลายข้อมูลที่มีความสำคัญเมื่อสิ้นสุดสัญญา

5.8 <u>การจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ (System Acquisition, Development and Maintenance)</u>

5.8.1 การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (security requirements of information systems)

<u>ที่มา</u>

เพื่อกำหนดให้กระบวนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นส่วนหนึ่งของระบบสารสนเทศของทั้งภายในองค์กรและที่เกี่ยวข้องกับการให้บริการภายนอกผ่านเครือข่ายสาธารณะ ตลอดช่วงอายุการใช้งานระบบสารสนเทศ (entire life cycle) ได้แก่ กระบวนการจัดหา กระบวนการพัฒนาระบบ (system development life cycle) การใช้งาน และการดูแลรักษา

<u>แนวทางปฏิบัติ</u>

Funding portal ควรระบุข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศไว้เป็นส่วนหนึ่งเมื่อจัดให้มีระบบสารสนเทศใหม่หรือเมื่อปรับปรุงระบบเก่า

5.8.2 การรักษาความมั่นคงปลอดภัยในกระบวนการพัฒนาระบบสารสนเทศ (security in development and support process)

<u>ที่มา</u>

เพื่อให้การพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศประมวลผลเป็นไปได้อย่างถูกต้องครบถ้วนและเป็นไปตามความต้องการของผู้ใช้งาน (change management) รวมถึงการรักษาไว้ซึ่งความมั่นคงปลอดภัยของระบบสารสนเทศตลอดช่วงการพัฒนาระบบงานสารสนเทศ (system development life cycle)

<u>แนวทางปฏิบัติ</u>

1. Funding portal ควรจัดให้มีการควบคุมการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศตลอดทุกขั้นตอนตามการควบคุมที่ได้กำหนดไว้ เช่น

1.1 มีการประเมินผลกระทบที่อาจเกิดขึ้นจากการเปลี่ยนแปลง

1.2 มีการกำหนดวิธีปฏิบัติให้คำขอให้แก้ไขหรือพัฒนามาจากผู้ที่มีสิทธิและอนุมัติคำขอโดยผู้มีอำนาจ ควรกำหนดให้มีการควบคุมผลข้างเคียงที่อาจเกิดขึ้นเนื่องจากมีการแก้ไข มีการตรวจรับจากผู้มีอำนาจภายหลังการแก้ไขหรือพัฒนาแล้วเสร็จก่อนโอนย้ายระบบงาน รวมทั้งมีการจัดเก็บรายละเอียดของคำขอไว้ เป็นต้น

1.3 กำหนดวิธีปฏิบัติในกรณีที่มีการแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ในกรณีฉุกเฉิน และบันทึกเหตุผลความจำเป็นและขออนุมัติจากผู้มีอำนาจทุกครั้ง

1.4 ปรับปรุงเอกสารประกอบระบบงานทั้งหมดหลังจากที่ได้มีการแก้ไขเปลี่ยนแปลง เพื่อให้ทันสมัยอยู่เสมอ เช่น เอกสารประกอบรายละเอียดโครงสร้างข้อมูล คู่มือระบบงาน ทะเบียนรายชื่อผู้มีสิทธิใช้งาน ขั้นตอนการทำงานของโปรแกรม และต้องจัดเก็บเอกสารดังกล่าวในที่ปลอดภัยและสะดวกต่อการใช้งาน

1.5 จัดเก็บโปรแกรม version ก่อนการเปลี่ยนแปลงไว้ใช้งาน หรือมีกระบวนการถอยกลับสู่สภาพเดิม (fall-back) ของระบบงาน ในกรณีระบบงานผิดพลาดหรือไม่สามารถใช้งานได้

1.6 มีการสื่อสารให้กับบุคคลที่เกี่ยวข้องได้รับทราบและสามารถปฏิบัติงานได้อย่างถูกต้อง

1.7 บันทึกและจัดเก็บหลักฐานทั้งหมด (audit trail) ที่เกี่ยวข้องกับการเปลี่ยนแปลงเพื่อใช้ประกอบในกรณีที่มีการตรวจสอบ

2. Funding portal ควรจัดให้มีการทดสอบระบบสารสนเทศที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลง เพื่อให้มั่นใจว่าการทำงานมีประสิทธิภาพ การประมวลผลถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน พร้อมทั้งปรับปรุงแผนบริหารความต่อเนื่องทางธุรกิจ (business continuity plan) ให้สอดคล้องกับการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศดังกล่าว

3. Funding portal ควรจัดให้มีการดูแล ติดตาม และควบคุมการปฏิบัติงานของผู้ให้บริการพัฒนาระบบงานสารสนเทศจากภายนอก (outsourced system development) ให้เป็นไปตามข้อกำหนดของสัญญา

5.9 การใช้บริการจากผู้ให้บริการภายนอก (Supplier Relationship)

5.9.1 การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศจากผู้ให้บริการภายนอก (information security in supplier relationships)

ที่มา

เพื่อป้องกันทรัพย์สินสารสนเทศของ funding portal จากการเข้าถึงโดยผู้ให้บริการภายนอกอย่างไม่เหมาะสม

แนวทางปฏิบัติ

1. Funding portal ควรจัดให้มีนโยบายเกี่ยวกับการใช้บริการจากผู้ให้บริการภายนอกอย่างเป็นลายลักษณ์อักษร เพื่อลดความเสี่ยงจากการเข้าถึงทรัพย์สินสารสนเทศของ funding portal อย่างไม่เหมาะสม ทั้งนี้ นโยบายดังกล่าวควรมีเนื้อหาขั้นต่ำครอบคลุมประเด็นดังต่อไปนี้

1.1 กำหนดข้อตกลงเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและกระบวนการควบคุมอย่างเป็นลายลักษณ์อักษร และมีการลงนามร่วมกันระหว่าง funding portal และผู้ให้บริการภายนอก

ทั้งนี้ funding portal ต้องมั่นใจว่าผู้ให้บริการภายนอกมีหน้าที่รับผิดชอบในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศเสมือนกับ funding portal ดำเนินการด้วยตนเอง

1.2 กำหนดหน้าที่ความรับผิดชอบของผู้ให้บริการภายนอก

1.3 ระบุประเภทข้อมูลสารสนเทศที่อนุญาตให้ผู้บริการภายนอกเข้าถึง เพื่อให้การกำหนดมาตรการควบคุมและติดตามการเข้าถึงข้อมูลเป็นไปอย่างเหมาะสม ภายใต้หลักความจำเป็นในการรู้ข้อมูล (need-to-know basis)

1.4 จัดให้มีขั้นตอนและกระบวนการติดตามควบคุมการเข้าถึงสารสนเทศอย่างเหมาะสม

1.5 มีการรักษาความมั่นคงปลอดภัยในกรณีที่มีการเคลื่อนย้ายหรือถ่ายโอนข้อมูลสารสนเทศ

1.6 มีการควบคุมความครบถ้วนถูกต้องของข้อมูลและการประมวลผลข้อมูลที่ได้รับจากผู้ให้บริการภายนอก

1.7 กำหนดกระบวนการควบคุมอย่างเป็นมาตรฐานเพื่อติดตามการทำงานของผู้ให้บริการภายนอก

2. ข้อตกลงเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศควรมีเนื้อหาขั้นต่ำดังนี้

2.1 รายละเอียดของข้อมูลที่จำเป็นต้องใช้หรือเข้าถึงโดยผู้ให้บริการภายนอก รวมทั้งวิธีการเข้าถึงข้อมูลดังกล่าว

2.2 การจัดแบ่งประเภทข้อมูลที่สอดคล้องกับนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

2.3 มีมาตรการดำเนินการเพื่อให้มั่นใจได้ว่าข้อมูลที่เป็นความลับหรือมีความสำคัญ ทรัพย์สินทางปัญญา และลิขสิทธิ์ของ funding portal ได้รับการคุ้มครองอย่างปลอดภัยตามกฎหมายและหลักเกณฑ์ของทางการที่เกี่ยวข้อง

2.4 กำหนดหน้าที่ความรับผิดชอบของผู้ให้บริการภายนอกในการปฏิบัติงานภายใต้การควบคุมต่าง ๆ เช่น กำหนดเงื่อนไขการเข้าถึงข้อมูลของผู้ใช้บริการ ติดตามตรวจสอบการปฏิบัติงานของผู้ให้บริการภายนอกให้เป็นไปตามข้อตกลงของผู้ใช้บริการ กำหนดให้ผู้ให้บริการภายนอกรายงานผลการปฏิบัติงานให้ผู้ใช้บริการทราบเมื่อร้องขอ การแก้ไขปัญหาต่าง ๆ ภายในระยะเวลาที่กำหนด รวมทั้งการปฏิบัติงานให้เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของผู้ใช้บริการ

2.5 แนวทางการใช้งานข้อมูลสารสนเทศอย่างถูกต้องเหมาะสม

2.6 แนวทางการแก้ไขปัญหากรณีที่เกิดข้อผิดพลาดจากการปฏิบัติหน้าที่

2.7 รายชื่อและช่องทางสำหรับติดต่อบุคคลหรือหน่วยงานอื่น ๆ ที่เกี่ยวข้องโดยเฉพาะอย่างยิ่งบุคคลหรือหน่วยงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

2.8 สิทธิในการเข้าตรวจสอบกระบวนการปฏิบัติงานของผู้ให้บริการภายนอก รวมทั้งควบคุมให้มีการปฏิบัติงานเป็นไปตามข้อตกลงที่ได้กำหนดไว้ ทั้งนี้ ในกรณีที่ผู้ให้บริการภายนอกประกอบธุรกิจในต่างประเทศและมีข้อจำกัดในการเข้าตรวจสอบการปฏิบัติงานดังกล่าว funding portal ควรมีมาตรการเพื่อให้มั่นใจได้ว่ามีการควบคุมผู้ให้บริการภายนอกให้ปฏิบัติงานเป็นไปตามข้อตกลงที่ได้กำหนดไว้อย่างเหมาะสม

2.9 ผู้ให้บริการภายนอกยินยอมให้สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์เข้าตรวจสอบการปฏิบัติงานของผู้ให้บริการ เรียกดู หรือตรวจสอบเอกสารหลักฐานที่เกี่ยวข้องได้

2.10 ข้อกำหนดเพิ่มเติมเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ กรณีที่ผู้ให้บริการภายนอกมอบหมายการปฏิบัติงานให้กับบุคคลอื่นต่อ (sub-contracting to another supplier)

5.9.2 การใช้บริการ cloud computing กับระบบสารสนเทศที่มีความสำคัญ

<u>ที่มา</u>

เพื่อกำหนดมาตรการรักษาความมั่นคงปลอดภัยสำหรับการใช้บริการ cloud computing กับระบบสารสนเทศที่มีความสำคัญ

<u>แนวทางปฏิบัติ</u>

ในกรณีที่ใช้บริการ cloud computing กับระบบสารสนเทศที่มีความสำคัญ funding portal ควรจัดให้มีข้อกำหนดเกี่ยวกับการใช้งาน โดยขั้นต่ำควรมีรายละเอียด ดังนี้

1. กำหนดข้อตกลงระหว่างผู้ให้บริการและผู้ใช้บริการ โดยมีลักษณะดังนี้

1.1 ผู้ใช้บริการถือเป็นเจ้าของข้อมูลสารสนเทศ

1.2 กำหนดประเภทบริการที่จะใช้ cloud computing

1.3 ต้องระบุข้อตกลงในการควบคุมการเข้าถึงข้อมูล เช่น วิธีการเข้าใช้งานระบบ วิธีการกำหนดสิทธิการใช้งาน การติดตามการแก้ปัญหา การรายงานข้อผิดพลาด ประสิทธิภาพ และสภาพโดยรวมของระบบ อย่างชัดเจน

1.4 กำหนดบทบาทหน้าที่ความรับผิดชอบของผู้ให้บริการในด้านการสำรองข้อมูล กระบวนการแก้ไขปัญหา ระดับการให้บริการ (service level agreement) ระยะเวลาในการกลับคืนสู่สภาพการดำเนินงานปกติของระบบสารสนเทศ (recovery time objectives : RTO) และกำหนดเป้าหมายในการกู้คืนข้อมูล เช่น กำหนดประเภทของข้อมูล และชุดข้อมูลล่าสุดที่จะกู้คืนได้ (recovery point objective : RPO) อย่างชัดเจน

1.5 กำหนดเงื่อนไขความรับผิดชอบในกรณีที่ผู้ให้บริการไม่สามารถให้บริการตามสัญญาที่กำหนด

1.6 กำหนดให้เนื้อหาหรือเอกสารที่เกี่ยวข้องกับข้อตกลงมีการระบุรายละเอียดที่เกี่ยวข้องกับนโยบายการป้องกันการรั่วไหลของข้อมูลที่อาจเกิดขึ้นจากผู้ให้บริการ

1.7 ผู้ให้บริการไม่มีสิทธิเข้าถึงและไม่เปิดเผยข้อมูลของผู้ใช้บริการ เว้นแต่จะแจ้งและได้รับความยินยอมจากผู้ใช้บริการ หรือแจ้งให้ทราบหากเป็นไปตามกฎหมายของประเทศที่ผู้ให้บริการไปตั้งศูนย์ข้อมูล (cloud server hosting country) หรือเป็นไปตามกฎหมายเกี่ยวกับความมั่นคงของประเทศผู้ให้บริการ (origin country)

1.8 Funding portal ควรมีมาตรการเพื่อให้มั่นใจได้ว่าผู้ให้บริการจัดให้มีการตรวจสอบขั้นตอนการปฏิบัติงานอย่างน้อยปีละ 1 ครั้ง จากผู้ตรวจสอบอิสระ

1.9 มีข้อกำหนดเมื่อสิ้นสุดการใช้บริการ (exit plan) เช่น กำหนดระยะเวลารักษาข้อมูลและวิธีการทำลายข้อมูลเพื่อให้มั่นใจว่าไม่สามารถกู้คืนข้อมูลกลับมาได้

1.10 ในกรณีที่ผู้ให้บริการมีการใช้บริการจากผู้ให้บริการภายนอก (subcontract of the cloud provider) ให้ถือว่าบริการดังกล่าวเป็นส่วนหนึ่งของผู้ให้บริการด้วย

2. การติดตาม ประเมิน และทบทวนการให้บริการของผู้ให้บริการ

2.1 ควรติดตามตรวจสอบประสิทธิภาพของการให้บริการ รวมทั้งมาตรการด้านความมั่นคงปลอดภัยให้สอดคล้องกับข้อกำหนดตามสัญญาต่าง ๆ หรือข้อตกลงในการให้บริการ

2.2 ควรประเมินความเพียงพอของระบบงานของผู้ให้บริการ (capacity planning) อย่างสม่ำเสมอ

2.3 ควรทบทวนเงื่อนไขการบริการในกรณีที่มีการเปลี่ยนแปลง เพื่อให้มั่นใจได้ว่าการให้บริการยังคงสอดคล้องกับการใช้งานและนโยบายด้านความมั่นคงปลอดภัยของระบบสารสนเทศของ funding portal

2.4 ควรทบทวนคุณสมบัติของผู้ให้บริการอย่างต่อเนื่อง เช่น การตรวจสอบความมั่นคงในฐานะทางการเงิน กระบวนการปฏิบัติงาน และประสิทธิภาพการปฏิบัติงาน เป็นต้น

3. ผู้ใช้บริการควรกำหนดแนวปฏิบัติเกี่ยวกับการโอนย้ายข้อมูล (data migration) ไปยังผู้ให้บริการรายใหม่อย่างชัดเจน ในกรณีที่มีการเปลี่ยนผู้ให้บริการ ทั้งนี้ เพื่อให้มั่นใจได้ว่าข้อมูลสารสนเทศยังคงมีความครบถ้วนถูกต้อง และพร้อมใช้งานอยู่เสมอ

5.10 <u>การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Incident Management)</u>

<u>ที่มา</u>

เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศได้รับการดำเนินการอย่างถูกต้อง มีประสิทธิภาพ ในช่วงระยะเวลาที่เหมาะสม

<u>แนวทางปฏิบัติ</u>

1. Funding portal ควรจัดให้มีขั้นตอนและกระบวนการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ โดยขั้นต่ำควรมีการกำหนดขั้นตอนและกระบวนการดังต่อไปนี้

1.1 จัดให้มีบุคคลหรือหน่วยงานเพื่อทำหน้าที่รับแจ้งเหตุการณ์ (point of contact) และรายงานเหตุการณ์ต่อคณะผู้บริหารหรือผู้เกี่ยวข้องให้ทราบและดำเนินการต่อไป (escalation)

1.2 การดำเนินการเพื่อตอบสนองต่อเหตุการณ์ที่เกิดขึ้นอย่างมีประสิทธิภาพ เพื่อทำให้เหตุการณ์คลี่คลายหรือกลับสู่ภาวะปกติอย่างรวดเร็ว

1.3 การรายงานให้สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์รับทราบถึงสถานการณ์และผลการบริหารจัดการ

2. Funding portal ควรจัดให้มีการรายงานสถานการณ์ที่เกิดขึ้นอย่างรวดเร็วและทันต่อเหตุการณ์ ผ่านบุคคลหรือหน่วยงานที่ทำหน้าที่รับแจ้งเหตุการณ์ (point of contact) โดยให้ดำเนินการดังนี้

2.1 รายงานสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์เมื่อมีเหตุการณ์ที่ส่งผลกระทบต่อระบบสารสนเทศที่มีความสำคัญ ประเภทดังต่อไปนี้

(1) ระบบหยุดชะงัก (system disruption)

(2) มีการบุกรุก เข้าถึง หรือใช้งานระบบโดยไม่ได้รับอนุญาต (system compromised)

(3) ส่งผลกระทบต่อชื่อเสียงของ funding portal (harm to reputation) เช่น ถูกปลอมแปลงหน้าเว็บไซต์ของบริษัท (website defacement)

โดยให้รายงาน ดังนี้

- รายงานโดยไม่ชักช้าเมื่อทราบเหตุการณ์ โดยมีเนื้อหาครอบคลุมถึงวันเวลา ประเภทเหตุการณ์ เหตุการณ์ และผลกระทบที่คาดว่าจะเกิดขึ้น ทั้งนี้ อาจแจ้งโดยวาจาหรือผ่านระบบรับส่งข้อความผ่านทางอิเล็กทรอนิกส์ (electronic messaging) ตามความเหมาะสม
- รายงานภายในวันทำการถัดไปหลังทราบเหตุการณ์เป็นลายลักษณ์อักษร โดยมีเนื้อหาครอบคลุมถึงวันเวลา ประเภทเหตุการณ์ เหตุการณ์ ผลกระทบที่เกิดขึ้น การดำเนินการแก้ไขปัญหา และความคืบหน้าในการแก้ไขปัญหา
- รายงานเมื่อเหตุการณ์ยุติหรือแก้ไขปัญหาแล้วเสร็จ เป็นลายลักษณ์อักษร โดยมีเนื้อหาครอบคลุมถึงวันเวลา ประเภทเหตุการณ์ เหตุการณ์ ผลกระทบที่เกิดขึ้น การดำเนินการแก้ไขปัญหา ผลการแก้ไขปัญหา ระยะเวลาในการแก้ไข สาเหตุที่เกิดปัญหา และแนวทางป้องกันในอนาคต

2.2 Funding portal ควรแจ้งบุคคลที่เกี่ยวข้อง เช่น ลูกค้า ทราบโดยไม่ชักช้า ในกรณีที่เหตุการณ์ส่งผลกระทบต่อบุคคลดังกล่าว

2.3 Funding portal ควรจัดให้มีการรายงานความคืบหน้าในการบริหารจัดการสถานการณ์และผลการบริหารจัดการเป็นระยะ และเมื่อเหตุการณ์ยุติแล้ว

5.11 <u>การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Aspects of Business Continuity Management)</u>

<u>ที่มา</u>

เพื่อให้การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศเป็นส่วนหนึ่งของการบริหารความต่อเนื่องทางธุรกิจ (business continuity management) ของ funding portal ทั้งนี้ เพื่อให้ระบบสารสนเทศอยู่ในสภาพที่พร้อมใช้งานอยู่เสมอ

<u>แนวทางปฏิบัติ</u>

1. Funding portal ควรคำนึงถึงความมั่นคงปลอดภัยของระบบสารสนเทศในการบริหารความต่อเนื่องทางธุรกิจเมื่อเกิดสถานการณ์ที่ไม่พึงประสงค์หรือไม่คาดคิด

2. Funding portal ควรกำหนดระยะเวลาในการกลับคืนสู่สภาพการดำเนินงานปกติของระบบสารสนเทศ (recovery time objectives : RTO) พร้อมทั้งจัดลำดับการกู้คืนระบบงานสารสนเทศที่มีความสำคัญทุกระบบ ให้เหมาะสมกับผลกระทบที่อาจเกิดขึ้น ทั้งนี้ ระยะเวลาในการกู้คืนดังกล่าวควรปฏิบัติได้อย่างมีประสิทธิภาพ

3. Funding portal ควรจัดให้มีการสำรองระบบสารสนเทศ เพื่อให้อยู่ในสภาพพร้อมใช้งานหรือสอดคล้องกับ recovery time objectives ที่กำหนด

4. Funding portal ควรจัดให้มีรายชื่อและช่องทางสำหรับติดต่อ (contact person) ของหน่วยงานกำกับดูแลและหน่วยงานผู้ให้บริการที่สนับสนุนการทำงานระบบสารสนเทศของบริษัท เพื่อให้สามารถติดต่อประสานงาน หรือขอความช่วยเหลือในกรณีเกิดเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ พร้อมทั้งปรับปรุงรายชื่อและช่องทางสำหรับติดต่อดังกล่าวให้เป็นปัจจุบัน

แบบสำรวจความคิดเห็น

เรื่อง การออกหลักเกณฑ์และแนวทางปฏิบัติเกี่ยวกับการเสนอขายหลักทรัพย์

ผ่านระบบหรือเครือข่ายอิเล็กทรอนิกส์ (Crowdfunding)

ข้อมูลทั่วไป

ชื่อผู้ตอบ_____ตำแหน่ง_____

ชื่อบริษัท/ องค์กร_____

อาชีพ/ ประเภทธุรกิจ_____

โทรศัพท์_____โทรสาร_____

E-mail address_____

สถานะของผู้ให้ความคิดเห็น

- ☐ ผู้สนใจประกอบธุรกิจเป็นผู้ให้บริการระบบหรือเครือข่ายอิเล็กทรอนิกส์ (funding portal)
- ☐ ผู้สนใจออกและเสนอขายหลักทรัพย์ผ่านระบบหรือเครือข่ายอิเล็กทรอนิกส์
- ☐ บริษัทหลักทรัพย์
- ☐ อื่น ๆ (ระบุ)_____

ความเห็นและข้อเสนอแนะ

1. ความเห็นเกี่ยวกับหลักการในการออกหลักเกณฑ์เกี่ยวกับการเสนอขายหลักทรัพย์ผ่านระบบหรือเครือข่ายอิเล็กทรอนิกส์ ดังนี้

1.1 การกระทำที่อาจก่อให้เกิดความขัดแย้งทางผลประโยชน์หรือการดำเนินธุรกิจเพื่อให้เป็นไปตามมาตรฐานของผู้ให้บริการระบบหรือเครือข่ายอิเล็กทรอนิกส์ (funding portal)

☐ เห็นด้วย ☐ ไม่เห็นด้วย

ความเห็นและข้อเสนอแนะ_____

_____

_____

1.2 การจัดเก็บข้อมูลของสมาชิกที่ติดต่อหรือใช้บริการผ่านระบบหรือเครือข่ายอิเล็กทรอนิกส์ของผู้ให้บริการระบบหรือเครือข่ายอิเล็กทรอนิกส์

☐ เห็นด้วย ☐ ไม่เห็นด้วย

ความเห็นและข้อเสนอแนะ_____

_____

_____

1.3 ระบบในการกำกับดูแลการปฏิบัติงานของผู้ให้บริการระบบหรือเครือข่ายอิเล็กทรอนิกส์

☐ เห็นด้วย ☐ ไม่เห็นด้วย

ความเห็นและข้อเสนอแนะ_____

_____

_____

1.4 การจัดทำงบการเงินประจำปีของผู้ให้บริการระบบหรือเครือข่ายอิเล็กทรอนิกส์

☐ เห็นด้วย ☐ ไม่เห็นด้วย

ความเห็นและข้อเสนอแนะ_____

_____

_____

1.5 การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของผู้ให้บริการระบบหรือเครือข่ายอิเล็กทรอนิกส์

☐ เห็นด้วย ☐ ไม่เห็นด้วย

ความเห็นและข้อเสนอแนะ_____

_____

_____

2. ความเห็นเกี่ยวกับหลักการในการออกแนวทางปฏิบัติเกี่ยวกับการเสนอขายหลักทรัพย์ผ่านระบบหรือเครือข่ายอิเล็กทรอนิกส์ ดังนี้

2.1 การเปิดเผยข้อมูลของบริษัทที่เสนอขายหลักทรัพย์และการสิ้นสุดการเปิดเผยข้อมูลของการเสนอขายหลักทรัพย์ผ่านระบบหรือเครือข่ายอิเล็กทรอนิกส์

☐ เห็นด้วย ☐ ไม่เห็นด้วย

ความเห็นและข้อเสนอแนะ_____

_____

_____

2.2 การประกอบธุรกิจอื่นของผู้ให้บริการระบบหรือเครือข่ายอิเล็กทรอนิกส์

☐ เห็นด้วย ☐ ไม่เห็นด้วย

ความเห็นและข้อเสนอแนะ_____

_____

_____

2.3 หลักทรัพย์ที่ห้ามเสนอขายผ่านระบบหรือเครือข่ายอิเล็กทรอนิกส์

☐ เห็นด้วย ☐ ไม่เห็นด้วย

ความเห็นและข้อเสนอแนะ_____

_____

_____

2.4 การโฆษณาและการส่งเสริมการขาย

☐ เห็นด้วย ☐ ไม่เห็นด้วย

ความเห็นและข้อเสนอแนะ_____

_____

_____

2.5 การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของผู้ให้บริการระบบหรือเครือข่ายอิเล็กทรอนิกส์

☐ เห็นด้วย ☐ ไม่เห็นด้วย

ความเห็นและข้อเสนอแนะ_____

_____

_____

3. ความเห็นและข้อเสนอแนะอื่น ๆ_____

_____

_____

_____

_____

กรุณาส่งแบบสำรวจความคิดเห็นกลับไปที่

ฝ่ายนโยบายและพัฒนาธุรกิจตัวกลาง

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

ชั้น 25 เลขที่ 333/3 ถนนวิภาวดีรังสิต

แขวงจอมพล เขตจตุจักร กรุงเทพฯ 10900

หรือ โทรสาร 0-2695-9763 หรือ e-mail: kornwara@sec.or.th

วันสุดท้ายของการแสดงความคิดเห็น วันที่ 12 กุมภาพันธ์ 2559

***** สำนักงานขอขอบคุณท่านที่ได้ให้ความร่วมมือในการแสดงความคิดเห็นในครั้งนี้ *****