**คู่มือในการจัดทำเอกสารประกอบคำขอความเห็นชอบ  
ผู้ให้บริการระบบเสนอขายโทเคนดิจิทัล (ICO Portal)**

รายการเอกสารประกอบคำขอ

ส่วนที่ 1 : ข้อมูลทั่วไปเกี่ยวกับบริษัท (Company’s Information)

ส่วนที่ 2 : คู่มือการทำหน้าที่เป็นผู้ให้บริการระบบเสนอขายโทเคนดิจิทัล (ICO Portal Operations Manual) ประกอบด้วย

* 1. ระบบงานในการกลั่นกรองโทเคนดิจิทัล (Due Diligence)
  2. ระบบการติดต่อและให้บริการกับผู้ลงทุน (Investor Onboarding)
  3. ระบบการเสนอขายและการจัดการค่าจองซื้อโทเคนดิจิทัล (Offering & Subscription Management)
  4. ระบบการจัดเก็บข้อมูลที่เกี่ยวกับการประกอบธุรกิจ (Record Keeping System)
  5. ระบบเทคโนโลยีสารสนเทศ (IT System)
  6. นโยบายด้านการบริหารความเสี่ยงและการป้องกันความขัดแย้งทางผลประโยชน์ (Risk Management and Conflict of Interest Policies)
  7. ระบบงานรองรับการประกอบธุรกิจได้อย่างต่อเนื่อง (BCP)
  8. ระบบงานในการกำกับดูแลการปฏิบัติงาน (Compliance System)
  9. ระบบการจัดการข้อร้องเรียนของผู้ลงทุน (Complaint Management System)

เอกสารแนบท้าย : แบบประเมินความพร้อมด้าน IT

**ส่วนที่ 1 : ข้อมูลทั่วไปเกี่ยวกับบริษัท (Company’s Information)**

**1.** **ลักษณะการประกอบธุรกิจ (Business Model)**

วัตถุประสงค์ เพื่อแสดงให้เห็นว่าบริษัทมีความรู้ความเข้าใจ มีคุณสมบัติและมีความพร้อมของระบบงาน รวมทั้งมีกลยุทธ์ในการประกอบธุรกิจให้ประสบความสำเร็จ

การจัดเตรียมเอกสารโปรดระบุลักษณะการประกอบธุรกิจของบริษัท โดยอย่างน้อยต้องครอบคลุมหัวข้อดังต่อไปนี้

* ความเป็นมาของบริษัท ความรู้ความชำนาญ ประสบการณ์ของผู้บริหารหรือผู้ถือหุ้นของผู้ประกอบธุรกิจ
* กลยุทธ์การทำธุรกิจ จุดแข็ง / จุดเด่นของบริษัท (อธิบายให้เห็นกลยุทธ์ในการทำธุรกิจของบริษัท)
* นโยบายการคิดค่าธรรมเนียมในการให้บริการ (Fees Policy)
* ลักษณะธุรกิจของผู้เสนอขายโทเคนดิจิทัลที่เป็นเป้าหมาย (Target Issuers)
* จำนวนบริษัทที่คาดว่าจะมีการออกเสนอขายต่อปี
* กลุ่มผู้ลงทุนเป้าหมาย (Target Investors)
* กรณีที่ประกอบธุรกิจอื่นอยู่ก่อนวันที่ขอรับอนุญาต อธิบายลักษณะธุรกิจอื่นที่บริษัทประกอบ และอธิบายถึงความเกี่ยวเนื่อง เป็นประโยชน์ หรือสนับสนุนการทำหน้าที่เป็น ICO Portal หรือรับรองว่าธุรกิจอื่นไม่มีลักษณะที่ก่อให้เกิดความขัดแย้งทางผลประโยชน์ หรือแสดงแนวทางการจัดการความขัดแย้งทางผลประโยชน์ที่มีประสิทธิภาพ

**2. โครงสร้างการถือหุ้น (Shareholding Structure)**

วัตถุประสงค์เพื่อแสดงให้เห็นถึงโครงสร้างการถือหุ้นของบริษัท

การจัดเตรียมเอกสาร

* นำส่งสำเนาบัญชีรายชื่อผู้ถือหุ้นของบริษัท ที่กระทรวงพาณิชย์รับรองเป็นเอกสารแนบ (อายุไม่เกิน 6 เดือน)
* แสดงโครงสร้างการถือหุ้นให้ครอบคลุมถึงผู้ถือหุ้นรายใหญ่ทางตรงและทางอ้อมทั้งหมด ตลอดจนถึงผู้ถือหุ้นรายใหญ่ชั้นสุดท้าย

**3. โครงสร้างองค์กรและขอบเขตหน้าที่ความรับผิดชอบ**

วัตถุประสงค์เพื่อแสดงให้เห็นถึงโครงสร้างการจัดการองค์กรที่ครอบคลุมงาน ICO Portal   
มีการถ่วงดุลและสอบยันการทำงานที่เหมาะสม (check and balance) และมีการกำหนดความรับผิดชอบของแต่ละฝ่ายงานที่ชัดเจนและครอบคลุมทุกกระบวนงานที่พึงมีในการประกอบธุรกิจ

การจัดเตรียมเอกสาร

* นำส่งสำเนาหนังสือรับรองบริษัท ซึ่งแสดงรายชื่อกรรมการและบุคคลผู้มีอำนาจในการจัดการบริษัทเป็นเอกสารแนบ
* แสดงโครงสร้างองค์กร โดยระบุชื่อผู้รับผิดชอบสูงสุดของแต่ละฝ่าย และจำนวนพนักงานของแต่ละฝ่าย (กรณียังไม่มีการจ้างผู้บริหารหรือพนักงานให้ระบุเป็นแผนงานได้)
* อธิบายขอบเขตหน้าที่และความรับผิดชอบของคณะกรรมการและฝ่ายงานที่เกี่ยวข้อง

**4. รายละเอียดเกี่ยวกับบุคลากร**

วัตถุประสงค์เพื่อแสดงให้เห็นถึงการมีบุคลากรในจำนวนที่เพียงพอกับการประกอบธุรกิจ ซึ่งมีความรู้ ความสามารถ และประสบการณ์เหมาะสมและสอดคล้องกับการปฏิบัติหน้าที่ และไม่มีประวัติในทางที่เสื่อมเสีย

การจัดเตรียมเอกสาร

* ระบุประวัติโดยสังเขปของคณะกรรมการและผู้บริหารที่เกี่ยวข้อง
* ระบุประวัติโดยสังเขปของทีมงานในส่วนงานที่ทำหน้าที่กลั่นกรองโทเคนดิจิทัล
* หากมีประสบการณ์ที่เกี่ยวข้องกับการออก ICO โปรดระบุรายละเอียดเกี่ยวกับประสบการณ์ดังกล่าว บทบาทของบุคลากร และความคืบหน้าของโครงการ

**ส่วนที่ 2 : คู่มือการทำหน้าที่เป็นผู้ให้บริการระบบเสนอขายโทเคนดิจิทัล** **(ICO Portal Operations Manual)**

|  |
| --- |
| **2.1 ระบบงานในการกลั่นกรองโทเคนดิจิทัล (Due Diligence)** |

**1. วิธีการ / ขั้นตอนในการติดต่อผู้ออกเสนอขายโทเคนดิจิทัล**

วัตถุประสงค์เพื่อแสดงให้เห็นว่าบริษัทมีการตรวจสอบคุณสมบัติของ issuer ในเบื้องต้นก่อนเริ่มให้บริการ

การจัดเตรียมเอกสาร

* อธิบายแนวทางปฏิบัติในการติดต่อกับว่าที่ Issuer
* อธิบายขั้นตอนในการคัดเลือก issuer ก่อนที่จะเริ่มให้บริการกับ issuer แต่ละราย และการพิจารณาในเบื้องต้นว่า issuer มีคุณสมบัติตามนโยบายของบริษัทและตามที่ประกาศกำหนด เช่น เป็นบริษัทไทย ไม่มีส่วนเกี่ยวข้องกับธุรกิจที่ไม่ชอบด้วยกฎหมาย ไม่มีสถานะล้มละลาย กรรมการ ผู้บริหาร   
  ผู้มีอำนาจควบคุมไม่มีคุณสมบัติต้องห้าม เป็นต้น
* ระบุประเภทของเอกสาร หรือข้อมูลที่กำหนดให้ผู้ออกเสนอขายต้องจัดส่งให้บริษัทเพื่อใช้ตรวจสอบคุณสมบัติ

**2. การตรวจสอบคุณสมบัติของผู้ออกเสนอขาย**

วัตถุประสงค์เพื่อให้มั่นใจว่ามีการกำหนดวิธีการและขั้นตอนในการตรวจสอบคุณสมบัติของ issuer ตามที่หลักเกณฑ์กำหนดในประกาศว่าด้วยการเสนอขายโทเคนดิจิทัลต่อประชาชน

การจัดเตรียมเอกสาร

* อธิบายวิธีการตรวจสอบคุณสมบัติของผู้ออกเสนอขาย โดยระบุขั้นตอนและวิธีการในการตรวจสอบ เช่น การจัดทำ checklist ระบุเรื่องที่จะตรวจสอบ แนวทางในการพิจารณา ผู้รับผิดชอบในการตรวจสอบ และอำนาจในการตัดสินใจ
* ระบุประเภทของเอกสาร หรือข้อมูลที่กำหนดให้ผู้ออกเสนอขายต้องจัดส่งให้บริษัทเพื่อใช้ตรวจสอบคุณสมบัติของผู้ออกเสนอขาย และระบุแนวทาง วิธีการในการได้รับเอกสารข้างต้น   
  เช่น ให้ issuer จัดส่งโดยการ scan / hard copy โดยมีการเซ็นรับรองความถูกต้องของเอกสาร   
  หรือการกำหนดให้ issuer รับรองตนเอง
* ระบุแนวทางดำเนินการในกรณีที่ issuer ขาดคุณสมบัติหรือไม่สามารถปฏิบัติได้ตามแนวทาง  
  ที่กำหนด

**3. การตรวจสอบโครงการและโทเคนดิจิทัลที่ขออนุญาต**

วัตถุประสงค์เพื่อให้มั่นใจว่ามีการกำหนดวิธีการและขั้นตอนในการกลั่นกรองโครงการว่าแผนธุรกิจ  
มีความชัดเจน วัตถุประสงค์ เป้าหมาย แนวทางการดำเนินการโครงการหรือกิจการตามแผนธุรกิจ และบทบาทของโทเคนดิจิทัลในแผนธุรกิจมีความเหมาะสม การให้สิทธิแก่  
ผู้ถือโทเคนดิจิทัลเป็นไปได้และเป็นธรรม

การจัดเตรียมเอกสาร

* อธิบายวิธีการตรวจสอบลักษณะการประกอบธุรกิจ วัตถุประสงค์การเสนอขายของ issuer และลักษณะของโทเคนดิจิทัล เช่น
* การจัดทำ checklist ระบุเรื่องที่จะตรวจสอบ รวมถึงมีกระบวนการที่ทำให้แน่ใจว่าแผนธุรกิจเป็นไปได้ มีความชัดเจน และไม่ fraud หรือ scam
* การทำความรู้จัก issuer ซึ่งอาจทำโดยการสัมภาษณ์ผู้บริหาร การทำ company visit เพื่อแสดงได้ว่าผู้ออกเสนอขายมีการประกอบธุรกิจหรือโครงการธุรกิจที่ชัดเจน และไม่เป็นการระดมทุนเพื่อทำกิจการที่ไม่เหมาะสม หรือ scam
* การกำหนดเอกสารหรือข้อมูลที่ใช้ในการประกอบการพิจารณา
* ระบุแนวทางในการพิจารณาข้อมูลที่ได้รับ เช่น มีฝ่ายหรือคณะทำงานในการพิจารณาข้อมูลของ  
  ผู้ออกโทเคนดิจิทัล หรือมีการให้คะแนน บุคลากรที่พิจารณามีความรู้ ความเชี่ยวชาญในการตรวจสอบความเป็นไปได้ของ project หรือจ้างผู้เชี่ยวชาญภายนอกมาช่วยในการพิจารณาความถูกต้องของข้อมูล
* บรรยายวิธีคัดกรองลูกค้า จุดไหนที่จะ reject และจุดไหนที่จะรับเป็นลูกค้า รวมถึง methodologies ต่าง ๆ ในการคัดกรองโครงการ

**4. การตรวจสอบ smart contract ที่เกี่ยวข้อง**

วัตถุประสงค์เพื่อแสดงให้เห็นว่า ICO Portal มีความสามารถและระบบงานรองรับการตรวจสอบ smart contract

การจัดเตรียมเอกสาร

* อธิบายแนวทางในการตรวจสอบ smart contract ของ issuer โดยระบุวิธีการในการตรวจสอบ ระบุผู้รับผิดชอบในการตรวจสอบ เช่น ทีม IT ของบริษัท หรือจ้าง outsource (มีวิธีการคัดเลือก outsource อย่างไร ที่จะแน่ใจว่าน่าเชื่อถือ ระบุชื่อผู้ที่จะ outsource รวมถึง ผลงานของ outsource)
* กรณี ICO portal รับเขียน smart contract ให้แก่ issuer จะจัดให้มีการตรวจสอบโดยบุคคลอื่นที่เป็นอิสระอย่างไร

**5. การอนุมัติรับ issuer เพื่อให้เสนอขายผ่านบริษัท**

วัตถุประสงค์เพื่อแสดงให้เห็นถึงกลไกการอนุมัติให้เสนอขายโทเคนดิจิทัลผ่านบริษัท

การจัดเตรียมเอกสาร

* อธิบายขั้นตอนการอนุมัติในการให้ issuer ทำการเสนอขายโทเคนดิจิทัลผ่านบริษัท เช่น ผู้รับผิดชอบเสนอเรื่องต่อผู้บริหารหรือคณะกรรมการเพื่อขออนุมัติการเสนอขายผ่านบริษัท
* ระบุผู้อนุมัติ เช่น กรรมการผู้จัดการ หรือคณะกรรมการบริษัท

**6. การทำสัญญาระหว่างบริษัทและผู้ออกเสนอขาย**

วัตถุประสงค์เพื่อแสดงให้เห็นว่ามีการจัดทำข้อตกลงระหว่างกันที่รัดกุมและเป็นไปตามหลักเกณฑ์ที่กำหนด

การจัดเตรียมเอกสาร อธิบายขั้นตอนและวิธีการในการทำข้อตกลงระหว่างบริษัทและ issuer

* การจัดให้มีสัญญาหรือข้อตกลงที่เป็นมาตรฐานที่จะใช้กับทุก issuer
* สัญญาหรือข้อตกลงดังกล่าวผ่านการพิจารณาจาก compliance / ที่ปรึกษากฎหมาย โดยมีการตรวจสอบสัญญาหรือข้อตกลงกับข้อกำหนดของประกาศและกฎเกณฑ์ที่เกี่ยวข้องทั้งหมด
* ระบุผู้มีอำนาจลงนามในสัญญา หรือข้อตกลง

**7. การจัดเก็บเอกสารที่เกี่ยวข้องกับการกลั่นกรองโทเคนดิจิทัล**

วัตถุประสงค์เพื่อแสดงให้เห็นถึงกลไกการจัดเก็บเอกสารที่เกี่ยวข้องกับการปฏิบัติงาน

การจัดเตรียมเอกสาร

* อธิบายวิธีการในการจัดเก็บ เอกสารที่จะทำการจัดเก็บ มีการกำหนดผู้รับผิดชอบ มีการจัดทำ checklist เอกสารที่จะทำการจัดเก็บ เช่น working paper
* ระบุระยะเวลาในการจัดเก็บ

**8. การติดตามการเปิดเผยข้อมูลและเหตุการณ์สำคัญ**

วัตถุประสงค์เพื่อแสดงถึงมาตรการในการติดตามดูแลการเปิดเผยข้อมูลและการดำเนินการของ issuer ภายหลังการเสนอขาย

การจัดเตรียมเอกสาร อธิบายวิธีการ ขั้นตอนการติดตาม issuer หลังการเสนอขาย เช่น

* กำหนดทีมผู้รับผิดชอบในการติดตาม progress ของ issuer และ alert ทันทีเมื่อมีความผิดปกติเป็นเวลา 1 ปี
* มีการจัดทำข้อตกลงที่มีข้อกำหนดให้ issuer มีหน้าที่เปิดเผยข้อมูล รายงานความคืบหน้าโครงการ การรายงานความคืบหน้าในการใช้เงิน

|  |
| --- |
| **2.2 ระบบการติดต่อและให้บริการกับผู้ลงทุน (Investor Onboarding)** |

**1. การทำความรู้จักและพิสูจน์ตัวตนของผู้ลงทุน (KYC/CDD)**

วัตถุประสงค์เพื่อแสดงให้เห็นว่าบริษัทมีนโยบายและกระบวนการในการทำความรู้จักตัวตนผู้ลงทุนซึ่งเป็นไปตามมาตรฐานของสำนักงาน ปปง.

การจัดเตรียมเอกสาร อธิบายขั้นตอนในการทำความรู้จักผู้ลงทุน และการพิสูจน์ความมีตัวตนของ  
ผู้ลงทุน เช่น

* ระบุขั้นตอน วิธีการ ในการในการตรวจสอบ เช่น
  + การตรวจสอบ (verify) สำเนาบัตรประชาชน กับข้อมูลที่ผู้ลงทุนกรอกผ่านระบบ
  + การตรวจสอบข้อมูลจากฐานข้อมูลของ สำนักงาน ป.ป.ง. ว่าไม่เป็นบุคคลที่อยู่ใน list
  + การรับรองความถูกต้องของผู้รับผิดชอบในการ verify
  + เอกสารที่ใช้ประกอบการพิจารณาอื่น ๆ
* ระบุผู้รับผิดชอบในการตรวจสอบความมีตัวตนของผู้ลงทุน
* ระบุขั้นตอนการดำเนินการปฏิเสธการให้บริการ กรณี ข้อมูลที่มีไม่สามารถระบุตัวตนที่แท้จริง

**2. การจัดประเภทของผู้ลงทุน (ประกาศ กจ. 16/2561 ข้อ 21)**

วัตถุประสงค์เพื่อแสดงให้เห็นว่าบริษัทมีนโยบายและกระบวนการในการจัดประเภทผู้ลงทุน

การจัดเตรียมเอกสาร อธิบายขั้นตอน วิธีการในการจัดประเภทผู้ลงทุน

* ระบุผู้รับผิดชอบในการจัดประเภทผู้ลงทุน
* ระบุข้อกำหนด ขั้นตอน วิธีการในการจัดประเภทผู้ลงทุน เช่น
  + ประเภทเอกสาร หรือข้อมูลที่ใช้ในการแบ่งผู้ลงทุนที่ให้จัดส่งเพื่อจัดประเภทผู้ลงทุน
  + การสอบทานเอกสารหรือข้อมูลที่บริษัทได้รับ
  + การอนุมัติการจัดประเภทผู้ลงทุนระบุผู้อนุมัติ
* ระบุขั้นตอนการดำเนินการกรณีที่ผู้ลงทุนปฏิเสธที่จะให้ข้อมูล หรือข้อมูลไม่เพียงพอทำให้ไม่สามารถจัดประเภทผู้ลงทุนได้ โดยให้จัดเป็นผู้ลงทุนประเภทผู้ลงทุนรายบุคคล
* ระบุวิธีการแจ้งผลการจัดประเภทผู้ลงทุนและรายละเอียดข้อมูลที่แจ้ง

**3. การเปิดเผยข้อมูลต่อผู้ลงทุน (ประกาศ กจ. 16/2561 ข้อ 22)**

วัตถุประสงค์เพื่อแสดงให้เห็นว่าบริษัทมีการเปิดเผยข้อมูลต่อผู้ลงทุน เพื่อให้ผู้ลงทุนมีข้อมูล  
ในการตัดสินใจใช้บริการและพิจารณาความเสี่ยงที่เกี่ยวข้อง โดยเป็นไปตามหลักเกณฑ์ที่กำหนด

การจัดเตรียมเอกสาร

* อธิบายแนวทางในการเปิดเผยข้อมูลต่อผู้ลงทุนเกี่ยวกับ ICO Portal และการเสนอขายโทเคนดิจิทัล โดยระบุรายละเอียดข้อมูลที่เปิดเผยและช่องทางที่ใช้
* ระบุแนวทางในการให้ผู้ลงทุนลงนามรับทราบหรือยอมรับข้อตกลงในการใช้บริการและความเสี่ยงที่เกี่ยวข้อง เมื่อผู้ลงทุนผ่านการ KYC และจัดประเภทเรียบร้อยแล้ว

**4. การจัดให้ผู้ลงทุนทำแบบทดสอบความเข้าใจเกี่ยวกับการลงทุน (Knowledge Test)**

วัตถุประสงค์เพื่อแสดงให้เห็นว่าบริษัทมีการจัดให้ผู้ลงทุนทำแบบทดสอบความเข้าใจเกี่ยวกับการลงทุน

การจัดเตรียมเอกสาร อธิบายวิธีการ ขั้นตอน และรายละเอียดดังต่อไปนี้

* ระบุประเภทผู้ลงทุนที่จะต้องทำแบบทดสอบ และขั้นตอนที่มีการให้ผู้ลงทุนทำแบบทดสอบ
* อธิบายกระบวนการในการทำแบบทดสอบและการดำเนินการในกรณีที่มีผลการทดสอบผ่าน / ไม่ผ่าน
* โปรดนำส่งแบบทดสอบความเข้าใจ (knowledge test) ตัวอย่างเป็นเอกสารแนบ

**5. ช่องทางในการติดต่อสื่อสารกับผู้ลงทุน**

วัตถุประสงค์เพื่อแสดงให้เห็นถึงแนวทางของบริษัทในการสื่อสารกับผู้ลงทุน

การจัดเตรียมเอกสาร

* ระบุช่องทาง วิธีการ ในการสื่อสารกับผู้ลงทุนเมื่อเกิดเหตุการณ์ต่าง ๆ เช่น เรื่องทั่วไป หรือเรื่องที่มีนัยสำคัญ
* ระบุแนวทาง วิธีการในการควบคุมดูแล
* ระบุระยะเวลาดำเนินการ เช่น ทันทีเมื่อได้รับแจ้งจาก issuer โดยมีการกำหนดขั้นตอน วิธีการ และผู้รับผิดชอบในการแจ้งต่อผู้ลงทุน

**6. ช่องทางสื่อสารทางอิเล็กทรอนิกส์ (ประกาศ กจ. 16/2561 ข้อ 25)**

วัตถุประสงค์เพื่อแสดงให้เห็นว่าบริษัทมีการจัดให้มีช่องทางสื่อสารทางอิเล็กทรอนิกส์เพื่อใช้ติดต่อสื่อสารระหว่างผู้ลงทุนด้วยกัน ผู้ลงทุนกับ ICO Portal หรือระหว่างผู้ลงทุนกับ  
ผู้ออกโทเคนดิจิทัล

การจัดเตรียมเอกสาร ระบุช่องทางและรูปแบบในการติดต่อสื่อสาร เพื่อให้เกิดการแลกเปลี่ยนข้อมูลกันระหว่างผู้ลงทุนด้วยกัน ระหว่างผู้ลงทุนกับ issuer หรือกับ ICO Portal เช่น ผ่าน webboard ของบริษัท

**7. การปรับปรุงข้อมูลผู้ลงทุนให้เป็นปัจจุบัน**

วัตถุประสงค์เพื่อแสดงให้เห็นว่าบริษัทมีนโยบายในการปรับปรุงข้อมูลผู้ลงทุนให้เป็นปัจจุบันตามความเหมาะสม

การจัดเตรียมเอกสาร ระบุรายละเอียดการดำเนินการปรับปรุงข้อมูลผู้ลงทุนและระยะเวลาในการปรับปรุงข้อมูลผู้ลงทุนแต่ละประเภท เช่น การปรับปรุงข้อมูลเมื่อผู้ลงทุนประสงค์จะลงทุนในโครงการเสนอขายโทเคนดิจิทัลเป็นครั้งที่ 2 ในระยะเวลาเกิน x เดือนนับจากการลงทุนครั้งแรกหรือการผ่านกระบวนการ KYC ครั้งล่าสุด เป็นต้น

|  |
| --- |
| **2.3 ระบบการเสนอขายและการจัดการค่าจองซื้อโทเคนดิจิทัล (Offering & Subscription Management)** |

**1. การเปิดเผยข้อมูลต่อผู้ลงทุน (ประกาศ กจ. 16/2561 ข้อ 27)**

วัตถุประสงค์เพื่อแสดงให้เห็นว่าบริษัทมีการเปิดเผยข้อมูลเกี่ยวกับการเสนอขายโทเคนดิจิทัล  
ที่ครบถ้วนเพียงพอ

การจัดเตรียมเอกสาร

* อธิบายขั้นตอนและวิธีการในการเปิดเผยข้อมูลต่อผู้ลงทุน ทั้งในช่วงก่อน ระหว่าง และหลังการเสนอขาย
* ระบุประเภทข้อมูลที่จะเปิดเผยให้ผู้ลงทุนทราบในแต่ละขั้นตอน / ช่วงเวลา
* ระบุกลไกที่ทำให้แน่ใจได้ว่าผู้ลงทุนรับทราบข้อมูลที่จำเป็น เช่น ข้อจำกัดในการลงทุนหรือ  
  ความเสี่ยง เป็นต้น

**2. การจัดการค่าจองซื้อ (ประกาศ กจ. 16/2561 ข้อ 28 – 31)**

วัตถุประสงค์เพื่อแสดงให้เห็นว่าบริษัทมีกระบวนการในการจัดการค่าจองซื้อที่รัดกุม ปลอดภัย   
และเป็นไปตามที่ประกาศกำหนด

การจัดเตรียมเอกสาร

* ระบุวิธีการจัดการค่าจองซื้อขณะเปิดเสนอขายโทเคนดิจิทัล
* กรณี จองซื้อด้วยคริปโทเคอร์เรนซี   
  - ระบุแนวทางการใช้ smart contract ในการบริหารจัดการค่าจองซื้อ   
  - อธิบายกระบวนการในการ ensure ว่าคริปโทเคอร์เรนซีที่นำมาลงทุนนั้นได้มาจาก licensed operator
* กรณีจองซื้อด้วยเงินบาท ให้ระบุชื่อผู้ที่ทำหน้าที่เก็บรักษาค่าจองซื้อ  
  - ระบุนโยบายของบริษัทว่ามีการเลือกผู้เก็บรักษาทรัพย์สินอย่างไร และมีการกำหนดคุณสมบัติในการคัดเลือกผู้ดูแลเงินค่าจองซื้ออย่างไร
* ระบุถึงการทำสัญญากำหนดหน้าที่ความรับผิดระหว่าง ICO portal กับผู้ดูแลรักษาเงินค่าจองซื้อ
* อธิบายขั้นตอน วิธีการ และระยะเวลาดำเนินการ ทั้งในกรณีที่การเสนอขายประสบความสำเร็จ (ยอดจองซื้อเกิน soft cap) และกรณีที่มีการจองซื้อไม่ครบตามจำนวนที่กำหนดหรือมีเหตุการณ์  
  ที่ทำให้ต้องยุติการเสนอขาย
* ระบุผู้รับผิดชอบในการดำเนินการในขั้นตอนต่าง ๆ

**3. การควบคุมมูลค่าการจองซื้อของผู้ลงทุนรายย่อย**

วัตถุประสงค์เพื่อแสดงให้เห็นว่าบริษัทมีระบบในการตรวจสอบและควบคุมมูลค่าการจองซื้อของ  
ผู้ลงทุนรายย่อยให้เป็นไปตามหลักเกณฑ์ที่กำหนด

การจัดเตรียมเอกสาร

* อธิบายถึงกลไกในการควบคุมมูลค่าเงินลงทุนของผู้ลงทุนรายย่อยให้ไม่เกิน 300,000 บาทต่อคนต่อโครงการ
* ระบุแนวทางในการควบคุมมูลค่าการระดมทุนจากผู้ลงทุนรายย่อยของโครงการให้ไม่เกิน 4 เท่าของส่วนผู้ถือหุ้นของ issuer หรือ 70% ของการระดมทุนทั้งหมด

|  |
| --- |
| **2.4 ระบบการจัดเก็บข้อมูลที่เกี่ยวกับการประกอบธุรกิจ (Record Keeping System)** |

วัตถุประสงค์เพื่อแสดงให้เห็นว่าบริษัทมีระบบในการจัดเก็บข้อมูลที่เกี่ยวข้องกับการประกอบธุรกิจ  
ในระยะเวลาที่เหมาะสม เพื่อให้สำนักงานหรือหน่วยงานกำกับดูแลอื่นสามารถตรวจสอบได้ และมีมาตรการในการรักษาความลับของข้อมูล

การจัดเตรียมเอกสาร โปรดนำส่งนโยบายในการบริหารจัดการและจัดเก็บข้อมูล โดยระบุ

* ประเภทของข้อมูลที่จัดเก็บ
* รูปแบบในการจัดเก็บ
* ระยะเวลาในการจัดเก็บข้อมูลแต่ละประเภท
* ผู้รับผิดชอบในการดำเนินการที่เกี่ยวกับการจัดเก็บข้อมูล
* การกำหนดผู้เข้าถึงข้อมูลในแต่ละประเภท
* ขั้นตอน วิธีการ และการขออนุมัติในการเข้าถึงข้อมูล และการจัดเก็บหลักฐานการเข้าถึงข้อมูล

|  |
| --- |
| **2.5 ระบบเทคโนโลยีสารสนเทศ (IT System)** |

โปรดกรอกแบบประเมินความพร้อมด้าน IT ที่แนบท้ายคู่มือฉบับนี้

|  |
| --- |
| **2.6 นโยบายด้านการบริหารความเสี่ยงและการป้องกันความขัดแย้งทางผลประโยชน์  (Risk Management and Conflict of Interest Policies)** |

**1. นโยบายด้านการบริหารความเสี่ยง**

วัตถุประสงค์เพื่อแสดงให้เห็นว่าบริษัทมีการบริหารและจัดการความเสี่ยงที่อาจเกิดขึ้นทุกด้านอย่างรัดกุม

การจัดเตรียมเอกสาร

* อธิบายกระบวนการบริหารและจัดการความเสี่ยงของบริษัท โดยระบุกระบวนการประเมิน  
  ความเสี่ยง ผู้มีหน้าที่รับผิดชอบจัดทำการประเมินความเสี่ยง ผู้มีอำนาจอนุมัติ และระบุรอบระยะเวลาทบทวนความเสี่ยง
* กำหนดวิธีการประเมินความเสี่ยงและกำหนดระดับความเสี่ยงที่บริษัทยอมรับได้ (risk appetite)
* จัดทำการประเมินความเสี่ยงที่เกี่ยวข้องกับการประกอบธุรกิจของบริษัททั้งหมด โดยต้องครอบคลุมความเสี่ยงอย่างรอบด้าน (เช่น ความเสี่ยงด้านธุรกิจ (business risk) ด้านระบบเทคโนโลยีสารสนเทศและความปลอดภัยทางไซเบอร์ (IT and cyber risk) ด้านการดำเนินงาน (operational risk) ด้านการเงิน (financial risk) ด้านการตลาด (market risk) ด้านการป้องกันและปราบปราม  
  การฟอกเงิน (anti-money laundering) ด้านการปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้อง (legal and compliance risk) เป็นต้น) และกำหนดกระบวนการจัดการและการติดตามความเสี่ยง (risk management & monitoring) ในแต่ละด้าน เพื่อให้สามารถควบคุมและบริหารจัดการความเสี่ยง  
  ให้อยู่ในระดับที่ยอมรับได้

**2. มาตรการป้องกันความขัดแย้งทางผลประโยชน์**

วัตถุประสงค์เพื่อแสดงให้เห็นว่าบริษัทมีการประเมินความขัดแย้งทางผลประโยชน์ (conflict of interests) ที่เกี่ยวข้องกับการประกอบธุรกิจ และมีการกำหนดนโยบายเพื่อป้องกันหรือบรรเทาความขัดแย้งทางผลประโยชน์นั้น

การจัดเตรียมเอกสาร

* ระบุความขัดแย้งทางผลประโยชน์ที่อาจเกิดขึ้น ซึ่งรวมถึงแต่ไม่จำกัดเพียงความขัดแย้งระหว่างผลประโยชน์ของผู้ลงทุนและบริษัท/พนักงานของบริษัท/หรือผู้เกี่ยวข้องกับบริษัท
* อธิบายมาตรการป้องกันหรือบริหารจัดการความขัดแย้งทางผลประโยชน์ดังกล่าว รวมทั้งแนวทางในการเปิดเผยข้อมูลเกี่ยวกับความขัดแย้งทางผลประโยชน์ที่มี

|  |
| --- |
| **2.7 ระบบงานรองรับการประกอบธุรกิจได้อย่างต่อเนื่อง (BCP)** |

วัตถุประสงค์เพื่อแสดงให้เห็นว่าบริษัทมีมาตรการรองกับเพื่อให้สามารถดำเนินธุรกิจได้อย่างต่อเนื่องเมื่อเกิดเหตุการณ์ไม่ปกติหรือฉุกเฉิน

การจัดเตรียมเอกสาร

* อธิบายแผน BCP ของบริษัท โดยระบุมาตรการ วิธีการ และระยะเวลาในการดำเนินการในกรณีเกิดเหตุการณ์ไม่ปกติเพื่อให้ระบบงานที่สำคัญยังคงดำเนินต่อไปได้
* ระบุแนวทางในการทดสอบแผน BCP เพื่อให้มั่นใจว่าเมื่อเกิดเหตุการณ์ไม่ปกติ บริษัทสามารถดำเนินการตามแนวทางที่กำหนดไว้ได้อย่างมีประสิทธิภาพ

|  |
| --- |
| **2.8 ระบบงานในการกำกับดูแลการปฏิบัติงาน (Compliance System)** |

วัตถุประสงค์เพื่อแสดงให้เห็นว่าบริษัทมีกระบวนการตรวจสอบและกำกับดูแลการปฏิบัติงานของบริษัทและพนักงานให้เป็นไปอย่างถูกต้องตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง รวมไปถึงข้อบังคับของบริษัท

การจัดเตรียมเอกสาร

* อธิบายขอบเขตหน้าที่ของส่วนงานกำกับดูแลการปฏิบัติงานหรือผู้ที่รับผิดชอบในการทำหน้าที่กำกับดูแลการปฏิบัติงาน วิธีการหรือขั้นตอนปฏิบัติงาน ความรับผิดชอบและการดำเนินการกรณีตรวจพบกรณีการกระทำผิดและการรายงานต่อหน่วยงานกำกับดูแลหรือผู้ที่เกี่ยวข้อง
* แสดงสายการบังคับบัญชาของฝ่ายงานกำกับดูแลการปฏิบัติงาน

|  |
| --- |
| **2.9 ระบบการจัดการข้อร้องเรียนของผู้ลงทุน (Complaint Management System)** |

วัตถุประสงค์เพื่อให้มั่นใจว่าบริษัทมีระบบในการจัดการเกี่ยวกับเรื่องร้องเรียนของผู้ลงทุนที่มีประสิทธิภาพ

การจัดเตรียมเอกสาร

* ระบุช่องทางในการรับเรื่องร้องเรียนและวิธีการร้องเรียนผ่านแต่ละช่องทาง
* ระบุผู้รับผิดชอบในการรับ / ดำเนินการเกี่ยวกับเรื่องร้องเรียน
* ระบุขั้นตอนในการดำเนินการเพื่อหาข้อยุติเกี่ยวกับเรื่องร้องเรียน ระยะเวลาที่ใช้ในการดำเนินการ การแจ้งผลการดำเนินการต่อผู้ร้องเรียน และการรายงานเกี่ยวกับเรื่องร้องเรียนต่อผู้บริหาร / กรรมการบริษัท / หน่วยงานกำกับดูแล
* ระบุแนวทางในการจัดเก็บเรื่องร้องเรียนและระยะเวลาในการจัดเก็บ



**แบบประเมินความพร้อมในการเริ่มต้นประกอบกิจการ  
ส่วนการบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กร   
และการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ**

|  |
| --- |
| **ส่วนที่ 1 ข้อมูลทั่วไป** |

1.1 ชื่อองค์กร/บริษัท  
(ภาษาไทย)     
(ภาษาอังกฤษ)

1.2 ที่อยู่  
 (ภาษาไทย)     
 (ภาษาอังกฤษ)

1.3 หมายเลขโทรศัพท์     หมายเลขโทรสาร

1.4 Website

1.5 ชื่อผู้ประสานงาน (Contact Person)     โทรศัพท์   
 Email

|  |
| --- |
| **ส่วนที่ 2 ระบบงานที่ประสงค์จะขอรับความเห็นชอบในครั้งนี้** |

1.

2.

3.

|  |
| --- |
| **ส่วนที่ 3 เอกสารประกอบการพิจารณา** |

โปรดจัดส่งเอกสารประกอบการพิจารณาดังต่อไปนี้

|  |
| --- |
| **1. นโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ** |
| รายชื่อเอกสาร :  1. |
| **2. แผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศ ระยะสั้น และระยะยาว** |
| รายชื่อเอกสาร :  1. |
| **3. แผนผังองค์กรหน่วยงานเทคโนโลยีสารสนเทศ** |
| รายชื่อเอกสาร :  1. |
| **4. เอกสารคำบรรยายลักษณะงาน (Job Description) ของพนักงานเทคโนโลยีสารสนเทศ** |
| รายชื่อเอกสาร :  1. |
| **5. ขั้นตอน/ช่องทาง/รายชื่อ สำหรับการติดต่อสำนักงาน หน่วยงานกำกับดูแลด้านสารสนเทศ และหน่วยงานของผู้ให้บริการ** |
| รายชื่อเอกสาร :  1. |
| **6. กระบวนการบริหารจัดการบัญชีผู้ใช้งานในระบบงาน** |
| รายชื่อเอกสาร :  1. |
| **7. กระบวนการการสำรองข้อมูล และทดสอบสื่อสำรองข้อมูล** |
| รายชื่อเอกสาร :  1. |
| **8. กระบวนการในการปฏิบัติงานประจำวันของเจ้าหน้าที่สารสนเทศ (Batch Operation)** |
| รายชื่อเอกสาร :  1. |
| **9. กระบวนการการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยระบบสารสนเทศ (Security Incident Response)** |
| รายชื่อเอกสาร :  1. |
| **10. กระบวนการการจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ** |
| รายชื่อเอกสาร :  1. |
| **11. กระบวนการบันทึก จัดเก็บ และ สอบทานบันทึกเหตุการณ์ของระบบสารสนเทศ (Log)** |
| รายชื่อเอกสาร :  1. |
| **12. นโยบายบริหารความต่อเนื่องทางธุรกิจ (BCM) และแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ** |
| รายชื่อเอกสาร :  1. |
| **13. รายชื่อผู้รับดำเนินการในงานที่เกี่ยวกับระบบสารสนเทศของผู้ประกอบธุรกิจ (ถ้ามี)** |
| รายชื่อเอกสาร :  1. |
| **14. นโยบายการดำเนินการในงานที่เกี่ยวกับระบบสารสนเทศโดยบุคคลอื่น (IT Outsourcing) (ถ้ามี)** |
| รายชื่อเอกสาร :  1. |
| **15. ทะเบียนทรัพย์สินสารสนเทศของบริษัท (ทั้งในส่วนของทรัพย์สินประเภทข้อมูล ระบบ และอุปกรณ์)** |
| รายชื่อเอกสาร :  1. |
| **16. แนวทางในการจัดระดับความสำคัญข้อมูลหรือระดับชั้นความลับของข้อมูล (Data Classification)** |
| รายชื่อเอกสาร :  1. |
| **17. คู่มือ เอกสารมาตรฐาน หรือข้อกำหนดในการใช้งานอุปกรณ์เคลื่อนที่ (หากมีการใช้งานเพื่อเข้าถึงข้อมูล / ระบบงาน)** |
| รายชื่อเอกสาร :  1. |
| **18. แนวทาง หรือวิธีการปฏิบัติงานจากเครือข่ายภายนอกบริษัท หรือมีการใช้งานจากเครือข่ายภายนอกบริษัทผ่านอุปกรณ์เคลื่อนที่ (หากมีการใช้งานเพื่อเข้าถึงข้อมูล / ระบบงาน)** |
| รายชื่อเอกสาร :  1. |
| **19. เอกสารสิทธิการใช้งานมาตรฐาน (Authorization Matrix)** |
| รายชื่อเอกสาร :  1. |
| **20. แผนผังโครงสร้างระบบเครือข่าย (Network Diagram)** |
| รายชื่อเอกสาร :  1. |

|  |
| --- |
| **ส่วนที่ 4 การควบคุมที่ประเมิน** |

โปรดอธิบายกระบวนการหรือแนวปฏิบัติในการควบคุมด้านเทคโนโลยีสารสนเทศ ดังต่อไปนี้

|  |
| --- |
| หมายเหตุ : หากมีข้อสงสัยในรายละเอียดของข้อปฏิบัติ สามารถศึกษาได้จากประกาศสำนักงาน ก.ล.ต. ที่ สธ. 37/2559 เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ และ ประกาศแนวปฏิบัติที่ นป. 3/2559 เรื่อง แนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศ ได้จาก   * <http://capital.sec.or.th/webapp/nrs/data/7038s.pdf> * <http://capital.sec.or.th/webapp/nrs/data/7041s.pdf> * <http://capital.sec.or.th/webapp/nrs/data/7040s.pdf> * <http://capital.sec.or.th/webapp/nrs/data/7042s.pdf> |

| **สิ่งที่พิจารณา** | **รายละเอียดการปฏิบัติ** | **เอกสารอ้างอิง** |
| --- | --- | --- |
| 1. มีการจัดทำนโยบายและมาตรการการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ | | |
| 1.1. นโยบายควรได้รับอนุมัติจากคณะกรรมการหรือผู้มีหน้าที่ที่ได้รับมอบหมาย |  |  |
| 1.2. นโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศครอบคลุมหัวข้อสำคัญตามประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ สธ. 37/2559 โดยประกอบไปด้วยหัวข้อดังต่อไปนี้ |  |  |
| 1.2.1. การควบคุมการเข้าถึงระบบงาน ข้อมูล และสิ่งอำนวยความสะดวกในการประมวลผลข้อมูล (Information Processing Facilities) |  |  |
| 1.2.2. การบริหารทรัพย์สินสารสนเทศ |  |  |
| 1.2.3. การรักษาความปลอดภัยการสื่อสารข้อมูลและเครือข่ายสื่อสาร |  |  |
| 1.2.4. การควบคุมการเข้ารหัส |  |  |
| 1.2.5. การป้องกันภัยคุกคามด้านเทคโนโลยีสารสนเทศ (Threat and Vulnerability Management) |  |  |
| 1.2.6. การรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ |  |  |
| 1.2.7. การรักษาความมั่นคงปลอดภัยทางกายภาพ |  |  |
| 1.2.8. การใช้งานผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ (IT Outsourcing) และการใช้งานใช้งานระบบสารสนเทศร่วมกันบนระบบเครือข่ายคอมพิวเตอร์เพื่อการประมวลผลตามความต้องการของผู้ใช้งาน (Cloud Computing) |  |  |
| 1.2.9. บทบาทหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ |  |  |
| 1.2.10. การใช้งานทรัพยากรสารสนเทศที่ยอมรับได้สำหรับพนักงาน (Acceptable IT usage policy) |  |  |
| 1.3. มีนโยบายมีรายละเอียดการสื่อสารด้านนโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศไปยังบุคลากรภายในองค์กร |  |  |
| 2. มีการจัดทำแผนกลยุทธ์หรือแผนการดำเนินงานด้านเทคโนโลยีสารสนเทศที่ครอบคลุมการจัดหาและพัฒนาระบบงานสำคัญ เทคโนโลยีสนับสนุนและระบบรักษาความมั่นคงปลอดภัย | | |
| 2.1. แผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศได้รับอนุมัติจากคณะกรรมการหรือผู้มีหน้าที่ที่ได้รับมอบหมาย |  |  |
| 2.2. แผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศประกอบไปด้วยแผนการดำเนินงานสำคัญ ได้แก่ |  |  |
| 2.2.1. แผนการจัดหาและพัฒนาระบบงาน ระยะเวลาการดำเนินงาน งบประมาณ หน่วยงานผู้รับผิดชอบ |  |  |
| 2.2.2. แผนการจัดหาและพัฒนา หรือ แผนการปรับปรุงด้านเทคโนโลยีสนับสนุน และระบบรักษาความมั่นคงปลอดภัยสารสนเทศ |  |  |
| 2.2.3. แผนการพัฒนาบุคคลากรด้านเทคโนโลยีสารสนเทศ |  |  |
| 3. มีการจัดทำโครงสร้างการบริหารงานด้านเทคโนโลยีสารสนเทศ และกำหนดบทบาทหน้าที่ความรับผิดชอบด้านการสนับสนุนการปฏิบัติงานอย่างชัดเจน | | |
| 3.1. แผนผังโครงสร้างองค์กรด้านเทคโนโลยีสารสนเทศ แสดงและกำหนดบทบาทหน้าที่ความรับผิดชอบในงานสำคัญ ได้แก่ |  |  |
| 3.1.1. งานบริหารจัดการด้านเทคโนโลยีสารสนเทศ |  |  |
| 3.1.2. งานพัฒนาและบำรุงรักษาระบบงาน |  |  |
| 3.1.3. งานปฏิบัติการด้านเทคโนโลยีสารสนเทศประจำวัน |  |  |
| 3.1.4. งานบริหารจัดการด้านโครงสร้างพื้นฐาน เครื่องแม่ข่าย และ ระบบปฏิบัติการ และเครือข่ายสื่อสาร |  |  |
| 3.1.5. งานรักษาความมั่นคงปลอดภัยสารสนเทศ |  |  |
| 3.2. เอกสารคำบรรยายลักษณะงาน มีการจัดทำคำบรรยายลักษณะงาน (Job Description) ที่ระบุถึงบทบาทหน้าที่ แนวการปฏิบัติหน้าที่ และความรับผิดชอบ |  |  |
| 3.3. แผนผังองค์กรหน่วยงานเทคโนโลยีสารสนเทศ และ เอกสารคำบรรยายลักษณะงาน แสดงถึงการแบ่งแยกหน้าที่ความรับผิดชอบ อย่างเหมาะสม |  |  |
| 4. มีการจัดทำรายละเอียดหน่วยงานหรือบุคลากรทั้งภายในและภายนอกบริษัทที่รับผิดชอบด้านความมั่นคงปลอดภัย ด้านกำกับดูแล และด้านสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศ รวมทั้งช่องทางการติดต่อเพื่อใช้ในกรณีที่มีปัญหา หรือเหตุการณ์สำคัญ | | |
| 4.1 มีการกำหนดรายชื่อผู้รับผิดชอบด้านเทคโนโลยีสารสนเทศเมื่อเกิดเหตุด้านความมั่นคงปลอดภัยสารสนเทศอย่างชัดเจน |  |  |
| 4.1.1 บุคลากรผู้รับผิดชอบด้านเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ |  |  |
| 4.1.2 ผู้ติดต่อและช่องทางติดต่อของหน่วยงานกำกับดูแล |  |  |
| 4.1.3 บริษัทผู้ให้บริการที่เกี่ยวข้อง |  |  |
| 5. มีการจัดทำขั้นตอนการปฏิบัติงานทางด้านสารสนเทศในกิจกรรมสำคัญ | | |
| 5.1. กระบวนการการบริหารจัดการบัญชีผู้ใช้งานในระบบงาน ควรประกอบไปด้วย  - ขั้นตอนการบริหารบัญชีผู้ใช้งาน และ รหัสผ่าน  - การอนุมัติ แก้ไขเปลี่ยนแปลง และยกเลิกการใช้งานระบบงาน หรือการเข้าถึงข้อมูล  - การสอบทานความเหมาะสมของสิทธิการเข้าใช้งานและการเข้าถึงข้อมูล  - การบริหารจัดการผู้ใช้งานที่มีสิทธิสูงในระบบงาน  - การจัดเก็บบันทึกเหตุการณ์และการสอบทานบันทึกเหตุการณ์ |  |  |
| 5.2. กระบวนการการสำรองและกู้คืนข้อมูล ควรประกอบไปด้วย  - กลยุทธ์การสำรองข้อมูล ประกอบด้วย ประเภทข้อมูล ความถี่การสำรองข้อมูล ที่สอดคล้องกับระยะเวลาการกู้คืน (Recovery Time Objective: RTO) และ ระยะเวลาการสูญหายของข้อมูลที่ยอมรับได้ (Recovery Point Objective: RPO)  - ระยะเวลาการจัดเก็บข้อมูล  - การบริหารจัดการสื่อบันทึกข้อมูล การเข้ารหัส สถานที่จัดเก็บสื่อบันทึกข้อมูล และระยะเวลาการใช้งาน  - การทดสอบความพร้อมสื่อบันทึกข้อมูลและการกู้คืนข้อมูล  - ขั้นตอนการกู้คืนข้อมูลและระบบงานในรายละเอียด |  |  |
| 5.3. กระบวนการในการปฏิบัติงานประจำวันของเจ้าหน้าที่สารสนเทศ (Batch Operation) โดยกระบวนการควรประกอบไปด้วย  - ขั้นตอนการปฏิบัติงานประจำวัน (Daily Tasks)  - กระบวนการการตรวจสอบความครบถ้วนถูกต้องในผลการปฏิบัติงานประจำวัน  - การติดตามผลการแก้ไขในกรณีที่อาจมีข้อผิดพลาดจากการปฏิบัติงานประจำวันเกิดขึ้น |  |  |
| 5.4. กระบวนการการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยระบบสารสนเทศ (Security Incident Response) โดยกระบวนการควรประกอบไปด้วย  - กำหนดผู้มีหน้าที่รับผิดชอบ รวมถึงช่องทางการติดต่อ  - การระบุสถานการณ์ด้านความมั่นคงปลอดภัย และแผนการรับมือกับสถานการณ์  - กำหนดเกณฑ์การจัดระดับความสำคัญ และ วิธีการรายงานไปยังผู้ที่เกี่ยวข้องตามระดับความสำคัญ  - การบันทึกข้อมูล จัดทำรายงานและสรุปผลจากเหตุการณ์  - การทดสอบและซักซ้อมแผนการรับมือ |  |  |
| 5.5. มีกระบวนการการแก้ไขเปลี่ยนแปลงโปรแกรม โดยกระบวนการควรประกอบไปด้วย  - การร้องขอ สอบทาน และ อนุมัติแก้ไขเปลี่ยนแปลงระบบงาน  - การทดสอบระบบงาน  - การทดสอบด้านความปลอดภัย  - การนำระบบงานเข้าสู่การใช้งาน  - การควบคุมโปรแกรมต้นฉบับ |  |  |
| 5.6. กระบวนการบันทึก จัดเก็บ และ สอบทานบันทึกเหตุการณ์ของระบบสารสนเทศ (Log) โดยกระบวนการควรประกอบไปด้วย  - ข้อกำหนดด้านการจัดเก็บบันทึกเหตุการณ์ของระบบสารสนเทศ เช่น ประเภทบันทึกเหตุการณ์ ระบบสารสนเทศ ระยะเวลาการจัดเก็บ  - การรักษาความปลอดภัยของบันทึกเหตุการณ์ที่จัดเก็บ และการใช้งานระบบจัดเก็บบันทึกเหตุการณ์กลาง (Centralized log server)  - ผู้มีหน้าที่ในการตั้งค่าการจัดเก็บ และ ผู้มีหน้าที่ในการตรวจสอบบันทึกเหตุการณ์  - กระบวนการตรวจสอบและวิเคราะห์บันทึกเหตุการณ์ |  |  |
| 6. มีการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศในการรองรับเหตุการณ์ฉุกเฉิน | | |
| 6.1. มีการจัดเตรียมแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ  - ขอบเขตแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศครอบคลุมระบบงานสำคัญที่เกี่ยวข้องในการให้บริการ (Mission Critical System)  - แนวทางสอดคล้องกับแผนการบริหารความต่อเนื่องในการดำเนินธุรกิจ ผลการประเมินผลกระทบทางธุรกิจ และเป้าหมายการกู้คืนระบบให้บริการ  - กำหนดสถานการณ์ฉุกเฉิน ครอบคลุมเหตุการณ์อันอาจจะเกิดขึ้น และเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ - บทบาทหน้าที่ความรับผิดชอบ และอำนาจการประกาศใช้แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ  - บทบาทหน้าที่ความรับผิดชอบ และอำนาจการประกาศใช้แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ  - ขั้นตอนการดำเนินงานตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ  - การซักซ้อมแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ  - ขั้นตอนการนำระบบงานกลับสู่การทำงานปกติ |  |  |
| 7. มีการจัดทำนโยบายเพื่อรองรับในกรณีที่ผู้ประกอบธุรกิจแต่งตั้งบุคคลอื่นเป็นผู้รับดำเนินการในงานที่เกี่ยวกับระบบสารสนเทศของผู้ประกอบธุรกิจ (ถ้ามี) | | |
| 7.1. มีการจัดทำรายชื่อบริษัทผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ |  |  |
| 7.2. มีการจัดทำสัญญาและข้อตกลงการใช้บริการ ที่ครอบคลุมเรื่องสำคัญ ได้แก่  - ขอบเขตและเงื่อนไขการให้บริการ  - มาตรฐานความปลอดภัยเทคโนโลยีสารสนเทศ  - ข้อตกลงการรักษาความลับและการไม่เปิดเผยข้อมูล  - การรักษาความต่อเนื่องในการให้บริการ (Optional) |  |  |
| 8. มีการจัดทำทะเบียนทรัพย์สินสารสนเทศของบริษัท (ทั้งในส่วนของทรัพย์สินประเภทข้อมูล, ระบบ และ อุปกรณ์) โดยมีการกำหนดผู้รับผิดชอบ | | |
| 8.1. มีการจัดทำรายการทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศ (Optional) ประกอบด้วย  - เครื่องแม่ข่ายและระบบประมวลผล  - Workstation และ อุปกรณ์เคลื่อนที่  - สื่อบันทึกข้อมูล  - อุปกรณ์เครือข่าย และ ระบบรักษาความปลอดภัยเครือข่าย  - ระบบงาน ซอฟต์แวร์ และ ลิขสิทธิ์  - อุปกรณ์ด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องอื่น ๆ |  |  |
| 8.2. มีการรวบรวมรายการข้อมูลและการจัดชั้นความลับของข้อมูล (Optional) ประกอบด้วย  - ทะเบียนข้อมูล  - ระดับความสำคัญ  - เจ้าของข้อมูล  - มาตรการควบคุมและรักษาความปลอดภัยข้อมูล |  |  |
| 9. มีการควบคุมสิทธิการใช้งานและการเข้าถึงข้อมูลสารสนเทศของผู้ใช้งานอย่างเหมาะสม | | |
| 9.1. มีการกำหนดสิทธิการเข้าถึงระบบงานสำคัญ สอดคล้องกับบทบาทหน้าที่ความรับผิดชอบ ได้แก่  - จัดทำตารางสิทธิ์ ระบบงานสำคัญ (Mission Critical System) ที่กำหนดสิทธิการใช้งานตามระดับหน้าที่ความรับผิดชอบ  - การควบคุมบัญชีผู้ใช้งานที่มีสิทธิการใช้งานระดับสูง  - การแบ่งแยกหน้าที่และการตรวจสอบการดำเนินงาน (Maker Checker) |  |  |
| 10. มีมาตรการรักษาความปลอดภัยเครือข่าย และระบบสารสนเทศ | | |
| 10.1. มีการจัดทำมาตรการรักษาความปลอดภัยเครือข่ายและเทคโนโลยีสารสนเทศ ประกอบด้วย  - การแบ่งแยกเครือข่าย ได้แก่ เครือข่ายสำหรับเครื่องแม่ข่ายระบบงานสำคัญ เครือข่ายผู้ใช้งานทั่วไป เครือข่ายดีเอ็มซี (DMZ) เครือข่ายภายนอก  - มีการติดตั้งอุปกรณ์ควบคุมการเข้าถึงเครือข่าย (Network Firewall) เพื่อควบคุมการเข้าถึงเครือข่ายจากบุคคลผู้ไม่พึงประสงค์  - มีการติดตั้งอุปกรณ์วิเคราะห์พฤติกรรมจากข้อมูลจราจรเครือข่าย (Network Traffic Analyzer) เพื่อตรวจสอบและยับยั้งความพยายามในการบุกรุกระบบ เช่น IDS/IPS หรือ Web Application Firewall: WAF (กรณีมีการใช้งาน ระบบงานเพื่อการให้บริการทำธุรกรรมผ่านเครือข่ายอินเตอร์เน็ต)  - มีการติดตั้งระบบคัดกรองโปรแกรมไม่พึงประสงค์ (Content Screening) เช่น ระบบป้องกันไวรัสระดับองค์กร และระบบป้องกันไวรัสที่เครื่องผู้ใช้งาน  - มีการจัดทำแนวทางการตรวจสอบ ติดตาม และรายงานผลเหตุการณ์ผิดปกติ ที่เกิดขึ้นและตรวจจับได้บนอุปกรณ์รักษาความมั่นคงปลอดภัยเครือข่าย |  |  |