

ประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

ที่ สธ. ๓๓/๒๕๖๗

เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มี

ระบบเทคโนโลยีสารสนเทศ

(ฉบับที่ ๒)

อาศัยอำนาจตามความในข้อ ๓ (๑) แห่งประกาศคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ กจ. ๑๖/๒๕๖๑ เรื่อง หลักเกณฑ์ เงื่อนไขและวิธีการให้ความเห็นชอบผู้ให้บริการระบบเสนอขายโทเคนดิจิทัล ลงวันที่ ๓ กรกฎาคม พ.ศ. ๒๕๖๑ ประกอบกับข้อ ๖ (๗) (ง) (ฉ) และ (ช) แห่งประกาศคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ กจ. ๑๖/๒๕๖๑ เรื่อง หลักเกณฑ์ เงื่อนไขและวิธีการให้ความเห็นชอบผู้ให้บริการระบบเสนอขายโทเคนดิจิทัล ลงวันที่ ๓ กรกฎาคม พ.ศ. ๒๕๖๑ ซึ่งแก้ไขเพิ่มเติมโดยประกาศคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ กจ. ๗/๒๕๖๓ เรื่อง หลักเกณฑ์ เงื่อนไขและวิธีการให้ความเห็นชอบผู้ให้บริการระบบเสนอขายโทเคนดิจิทัล (ฉบับที่ ๔) ลงวันที่ ๒๔ มีนาคม พ.ศ. ๒๕๖๓ ข้อ ๓ (๑) ประกอบกับข้อ ๑๑ ข้อ ๑๗ ข้อ ๑๘ และข้อ ๑๙ แห่งประกาศคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ กธ. ๑๙/๒๕๖๑ เรื่อง หลักเกณฑ์ เงื่อนไขและวิธีการประกอบธุรกิจสินทรัพย์ดิจิทัล ลงวันที่ ๓ กรกฎาคม พ.ศ. ๒๕๖๑ และข้อ ๙ (๔) (๗) และ (๘) แห่งประกาศคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ กธ. ๑๙/๒๕๖๑ เรื่อง หลักเกณฑ์ เงื่อนไขและวิธีการประกอบธุรกิจสินทรัพย์ดิจิทัล ลงวันที่ ๓ กรกฎาคม พ.ศ. ๒๕๖๑ ซึ่งแก้ไขเพิ่มเติมโดยประกาศคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ กธ. ๒๓/๒๕๖๗ เรื่อง หลักเกณฑ์ เงื่อนไขและวิธีการประกอบธุรกิจสินทรัพย์ดิจิทัล (ฉบับที่ ๒๔) ลงวันที่ ๘ สิงหาคม พ.ศ. ๒๕๖๗ ข้อ ๕ (๑) ประกอบกับข้อ ๑๒ วรรคหนึ่ง (๖) (๑๑) และ (๑๒) และข้อ ๑๔ แห่งประกาศคณะกรรมการกำกับตลาดทุน ที่ ทธ. ๓๕/๒๕๕๖ เรื่อง มาตรฐานการประกอบธุรกิจ โครงสร้างการบริหารงาน ระบบงาน และการให้บริการของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสัญญาซื้อขายล่วงหน้า ลงวันที่ ๖ กันยายน พ.ศ. ๒๕๕๖ ข้อ ๔ (๑) ประกอบกับข้อ ๒๖ และข้อ ๓๒ แห่งประกาศคณะกรรมการกำกับตลาดทุน ที่ ทธ. ๓๐/๒๕๕๙ เรื่อง หลักเกณฑ์ในการประกอบ การเป็นศูนย์ซื้อขายสัญญาซื้อขายล่วงหน้า ลงวันที่ ๓ สิงหาคม พ.ศ. ๒๕๕๙ ข้อ ๕ (๑) ประกอบกับข้อ ๒๑ ข้อ ๒๗ วรรคหนึ่ง ข้อ ๓๗ และข้อ ๔๓ แห่งประกาศคณะกรรมการกำกับตลาดทุน

ที่ ทธ. ๓๑/๒๕๕๙ เรื่อง หลักเกณฑ์ในการประกอบการเป็นสำนักหักบัญชีสัญญาซื้อขายล่วงหน้า ลงวันที่ ๓ สิงหาคม พ.ศ. ๒๕๕๙ ข้อ ๕ (๑) ประกอบกับข้อ ๑๑ ข้อ ๑๗ วรรคหนึ่ง และข้อ ๓๓ แห่งประกาศคณะกรรมการกำกับตลาดทุน ที่ ทธ. ๓๒/๒๕๕๙ เรื่อง หลักเกณฑ์ เงื่อนไข และวิธีการในการประกอบการเป็นสำนักหักบัญชีหลักทรัพย์และศูนย์รับฝากหลักทรัพย์ ลงวันที่ ๓ สิงหาคม พ.ศ. ๒๕๕๙ และข้อ ๕ (๑) ประกอบกับข้อ ๓๑ (๑) และ (๔) วรรคหนึ่ง (ง) แห่งประกาศคณะกรรมการกำกับตลาดทุน ที่ ทจ. ๒๑/๒๕๖๒ เรื่อง ข้อกำหนดเกี่ยวกับการเสนอขายหลักทรัพย์ผ่านระบบคราวด์ฟันดิง ลงวันที่ ๑๒ เมษายน พ.ศ. ๒๕๖๒ และข้อ ๓๑ (๔/๑) แห่งประกาศคณะกรรมการกำกับตลาดทุน ที่ ทจ. ๒๑/๒๕๖๒ เรื่อง ข้อกำหนดเกี่ยวกับการเสนอขายหลักทรัพย์ผ่านระบบคราวด์ฟันดิง ลงวันที่ ๑๒ เมษายน พ.ศ. ๒๕๖๒ ซึ่งแก้ไขเพิ่มเติมโดยประกาศ คณะกรรมการกำกับตลาดทุน ที่ ทจ. ๑๔/๒๕๖๓ เรื่อง ข้อกำหนดเกี่ยวกับการเสนอขายหลักทรัพย์ ผ่านระบบคราวด์ฟันดิง (ฉบับที่ ๒) ลงวันที่ ๒๘ กุมภาพันธ์ พ.ศ. ๒๕๖๓ สำนักงานออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ให้ยกเลิกความใน (ง) ของ (๑) ในบทนิยามคำว่า “ผู้ประกอบการธุรกิจ” ของข้อ ๒ แห่งประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ สธ. ๓๘/๒๕๖๕ เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ ลงวันที่ ๒๘ กันยายน พ.ศ. ๒๕๖๕ และให้ใช้ความต่อไปนี้แทน

“(ง) การเป็นที่ปรึกษาการลงทุนที่มีการใช้เทคโนโลยีเพื่อการติดต่อหรือให้บริการแก่ลูกค้า”

ข้อ ๒ ให้ยกเลิกความใน (ญ) ของ (๑) ในบทนิยามคำว่า “ผู้ประกอบการธุรกิจ” ของข้อ ๒ แห่งประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ สธ. ๓๘/๒๕๖๕ เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ ลงวันที่ ๒๘ กันยายน พ.ศ. ๒๕๖๕ และให้ใช้ความต่อไปนี้แทน

“(ญ) การเป็นที่ปรึกษาสัญญาซื้อขายล่วงหน้าที่มีการใช้เทคโนโลยีเพื่อการติดต่อหรือให้บริการแก่ลูกค้า”

ข้อ ๓ ให้เพิ่มบทนิยามคำว่า “เทคโนโลยีเพื่อการติดต่อหรือให้บริการแก่ลูกค้า” ระหว่าง บทนิยามคำว่า “ผู้ประกอบการธุรกิจ” และคำว่า “เทคโนโลยีสารสนเทศ” ในข้อ ๒ แห่งประกาศ สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ สธ. ๓๘/๒๕๖๕ เรื่อง ข้อกำหนด ในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ ลงวันที่ ๒๘ กันยายน พ.ศ. ๒๕๖๕

“เทคโนโลยีเพื่อการติดต่อหรือให้บริการแก่ลูกค้า” หมายความว่า เทคโนโลยีหรือคอมพิวเตอร์ที่มีการใช้งานเพื่อดำเนินการอย่างหนึ่งอย่างใด ดังต่อไปนี้

- (๑) การติดต่อลูกค้า
- (๒) การจัดทำหรือนำส่งข้อมูลบริการหรือผลิตภัณฑ์ให้แก่ลูกค้า
- (๓) การประมวลผล วิเคราะห์ ออกผลลัพธ์หรือคำแนะนำ เพื่อให้ลูกค้าใช้ประกอบการตัดสินใจลงทุน”

ข้อ ๔ ให้ยกเลิกความในวรรคหนึ่งของข้อ ๔ แห่งประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ สธ. ๓๘/๒๕๖๕ เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ ลงวันที่ ๒๘ กันยายน พ.ศ. ๒๕๖๕ และให้ใช้ความต่อไปนี้แทน

“เพื่อประโยชน์ในการปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศนี้ ให้ผู้ประกอบการธุรกิจประเมินระดับความเสี่ยงเกี่ยวกับระบบเทคโนโลยีสารสนเทศซึ่งส่งผลต่อการดำเนินธุรกิจของผู้ประกอบการธุรกิจตามแบบ RLA (Risk Level Assessment) และจัดส่งผลการประเมินดังกล่าวต่อสำนักงานภายในไตรมาสที่ ๑ ของทุกปีปฏิทิน ทั้งนี้ ตามแบบและวิธีการที่กำหนดไว้บนเว็บไซต์ของสำนักงาน”

ข้อ ๕ ให้ยกเลิกภาคผนวก ๑ คำศัพท์ ท้ายประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ สธ. ๓๘/๒๕๖๕ เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ ลงวันที่ ๒๘ กันยายน พ.ศ. ๒๕๖๕ และให้ใช้ภาคผนวก ๑ คำศัพท์ ท้ายประกาศนี้แทน

ข้อ ๖ ให้ยกเลิกภาคผนวก ๒ การกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ (Information Technology Governance) ท้ายประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ สธ. ๓๘/๒๕๖๕ เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ ลงวันที่ ๒๘ กันยายน พ.ศ. ๒๕๖๕ และให้ใช้ภาคผนวก ๒ การกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ (Information Technology Governance) ท้ายประกาศนี้แทน

ข้อ ๗ ให้ยกเลิกภาคผนวก ๓ การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Technology Security) ท้ายประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ สธ. ๓๘/๒๕๖๕ เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ ลงวันที่ ๒๘ กันยายน พ.ศ. ๒๕๖๕ และให้ใช้ภาคผนวก ๓ การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Technology Security) ท้ายประกาศนี้แทน

ข้อ ๘ ให้ยกเลิกภาคผนวก ๔ การตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology Audit) ท้ายประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ที่ สธ. ๓๘/๒๕๖๕ เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศลงวันที่ ๒๘ กันยายน พ.ศ. ๒๕๖๕ และให้ใช้ภาคผนวก ๔ การตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology Audit) ท้ายประกาศนี้แทน

ข้อ ๙ ประกาศนี้ให้ใช้บังคับตั้งแต่วันที่ ๑ มกราคม พ.ศ. ๒๕๖๘ เป็นต้นไป

ประกาศ ณ วันที่ ๒๑ พฤศจิกายน พ.ศ. ๒๕๖๗

พรอนงค์ บุชราตระกูล

เลขาธิการ

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

คำศัพท์

ส่วนที่ ๑ ขอบเขต

ให้ใช้คำอธิบายคำศัพท์ตามภาคผนวกนี้เพื่อประกอบการอธิบายคำย่อและความหมายของคำย่อ รวมถึงคำศัพท์ที่ปรากฏในภาคผนวกแนบท้ายประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ว่าด้วยข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ

ส่วนที่ ๒ คำอธิบายศัพท์

คำศัพท์

คำอธิบายศัพท์

“การใช้งานอุปกรณ์เคลื่อนที่” (mobile device)

การปฏิบัติงานที่มีการใช้อุปกรณ์เคลื่อนที่เพื่อเข้าถึงระบบ IT ที่มีนัยสำคัญ โดยผ่านการเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ภายในของผู้ประกอบธุรกิจโดยตรง

“การใช้งานอุปกรณ์ส่วนตัว”
(Bring Your Own Device : BYOD)

การใช้งานอุปกรณ์ส่วนตัวของบุคลากรเพื่อเข้าถึงระบบ IT รวมถึงการเข้าถึงระบบอีเมล และตารางการประชุม ของผู้ประกอบธุรกิจ ไม่ว่าจะกระทำผ่านแอปพลิเคชัน เว็บเบราว์เซอร์ หรือช่องทางใด ๆ

“การบริหารจัดการโครงการด้าน IT” (IT project management)

การจัดหา พัฒนา หรือแก้ไขเปลี่ยนแปลงระบบ IT ที่มีผลกระทบอย่างมีนัยสำคัญต่อการให้บริการ การดำเนินธุรกิจ หรือโครงสร้างพื้นฐาน (infrastructure) ด้าน IT

“การปฏิบัติงานจากเครือข่ายภายนอก”
(teleworking)

การปฏิบัติงานที่มีการเข้าถึงระบบ IT ที่มีนัยสำคัญโดยไม่ผ่านการเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ภายในของผู้ประกอบธุรกิจโดยตรง

“ซอฟต์แวร์”
(software)

ระบบหรือโปรแกรมคอมพิวเตอร์ดังนี้
(๑) ซอฟต์แวร์ระบบ (system software) เช่น ระบบปฏิบัติการ หรือโปรแกรมตรวจจับไวรัส เป็นต้น
(๒) ซอฟต์แวร์ประยุกต์ (application software) เช่น โปรแกรมประมวลผลคำ (word processor) หรือโปรแกรมสำหรับการประชุมออนไลน์ เป็นต้น

คำศัพท์**คำอธิบายศัพท์**

“ทรัพย์สินด้าน IT”

ฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูลที่เกี่ยวข้องกับการประกอบธุรกิจ โดยรวมถึงสิทธิในการใช้งานฮาร์ดแวร์และซอฟต์แวร์ เช่น สิทธิตามสัญญาอนุญาตใช้ซอฟต์แวร์ (software license) หรือสัญญาเช่าฮาร์ดแวร์ เป็นต้น

“บุคลากร”

บุคลากรของผู้ประกอบธุรกิจ

“บุคคลภายนอก”
(third party)

บุคคลภายนอกที่มีความเกี่ยวข้องกับผู้ประกอบธุรกิจดังนี้ แต่ไม่รวมถึงลูกค้าที่ใช้บริการหรือผลิตภัณฑ์ของผู้ประกอบธุรกิจ

(๑) ผู้ให้บริการงานด้าน IT

(๒) ผู้ที่มีการเชื่อมต่อกับระบบ IT ของผู้ประกอบธุรกิจ

(๓) ผู้ที่สามารถเข้าถึงข้อมูลสำคัญของผู้ประกอบธุรกิจหรือข้อมูลของลูกค้าที่อยู่ในรูปแบบอิเล็กทรอนิกส์และอยู่ภายใต้การควบคุมดูแลของผู้ประกอบธุรกิจ

“แบบ RLA”

(Risk Level
Assessment)

แบบการประเมินระดับความเสี่ยงเกี่ยวกับระบบเทคโนโลยีสารสนเทศซึ่งส่งผลต่อการดำเนินธุรกิจของผู้ประกอบธุรกิจที่กำหนดไว้บนเว็บไซต์ของสำนักงาน

“ประกาศที่
สธ. ๓๘/๒๕๖๕”

ประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ว่าด้วยข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ

“ผู้ประกอบธุรกิจ
ขนาดเล็ก”

ผู้ประกอบธุรกิจที่เข้าลักษณะเป็นผู้ประกอบธุรกิจขนาดเล็กตามที่กำหนดในแบบ RLA (Risk Level Assessment)

“ผู้ประกอบธุรกิจที่มี
ความเสี่ยงระดับต่ำ
ระดับปานกลาง หรือ
ระดับสูง”

ผู้ประกอบธุรกิจที่มีผลการประเมินตามแบบ RLA (Risk Level Assessment) อยู่ในระดับต่ำ ระดับปานกลาง หรือระดับสูง แล้วแต่กรณี

“ผู้ให้บริการงานด้าน IT”

บุคคลภายนอกซึ่งผู้ประกอบธุรกิจว่าจ้างหรือมอบหมายให้ปฏิบัติงานด้าน IT ซึ่งโดยปกติแล้วผู้ประกอบธุรกิจต้องดำเนินการเอง เช่น การมอบหมายงานทั้งหมดของฝ่ายเทคโนโลยีสารสนเทศให้แก่บริษัทในเครือ เป็นต้น

คำศัพท์**คำอธิบายศัพท์****“ภัยคุกคามทางไซเบอร์”**

การกระทำหรือการดำเนินการใด ๆ โดยมีขอบ โดยการใช้คอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือโปรแกรมคอมพิวเตอร์ ซึ่งมุ่งหมายให้เกิดความเสียหายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง รวมถึงภัยอันตรายที่อาจจะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

“ระบบ IT ที่มีนัยสำคัญ”
(critical system)

ระบบคอมพิวเตอร์หรือระบบเครือข่ายที่หากมีการหยุดชะงักจะส่งผลกระทบอย่างมีนัยสำคัญต่อการดำเนินงานหรือความต่อเนื่องในการดำเนินงาน ชื่อเสียงหรือฐานะของผู้ประกอบธุรกิจ หรือการใช้บริการของลูกค้า เช่น ระบบซื้อขาย ระบบสนับสนุนการปฏิบัติการ (back office system) ระบบจัดเก็บและบริหารจัดการข้อมูลลูกค้า ระบบจัดการลงทุน หรือระบบจัดเก็บทรัพย์สิน เป็นต้น

“เหตุการณ์ผิดปกติ
ด้าน IT” (IT incident)

เหตุการณ์ด้าน IT ที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) เช่น

- (๑) ระบบ IT ของผู้ประกอบธุรกิจถูกบุกรุกหรือโจมตี
- (๒) ความมั่นคงปลอดภัยด้าน IT ถูกคุกคาม
- (๓) ระบบ IT หยุดชะงัก ไม่สามารถให้บริการได้ เป็นต้น

“เหตุการณ์ด้าน
ความมั่นคงปลอดภัย
ของระบบ IT
อย่างมีนัยสำคัญ”

เหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ IT ที่เกิดขึ้นแล้วส่งผลกระทบดังนี้

- (๑) ทำให้ระบบ IT หรือข้อมูลที่จัดเก็บ ประมวลผล หรือส่งต่อ สูญเสียคุณสมบัติด้านความถูกต้องครบถ้วน (integrity) สภาพพร้อมใช้งาน (availability) หรือการดำรงไว้ซึ่งความลับ (confidentiality) อย่างมีนัยสำคัญ หรือ
- (๒) ทำให้เกิดการละเมิดหรือมีความเสี่ยงที่อาจทำให้เกิดการละเมิดต่อข้อกำหนดขององค์กรหรือกฎหมาย

เช่น

- ระบบ IT ของผู้ประกอบธุรกิจถูกบุกรุกหรือโจมตีสำเร็จ (successfully attacked หรือ system compromised)
- เหตุการณ์ DDoS ที่ส่งผลให้ระบบของผู้ประกอบธุรกิจเกิดการหยุดชะงัก
- ระบบ IT หยุดชะงัก ไม่สามารถให้บริการได้เป็นระยะเวลานานจนส่งผลกระทบต่อลูกค้าของผู้ประกอบธุรกิจในวงกว้าง

คำศัพท์คำอธิบายศัพท์

- เหตุการณ์ข้อมูลสำคัญของผู้ประกอบธุรกิจหรือข้อมูลส่วนบุคคลที่อยู่ภายใต้การควบคุมดูแลของผู้ประกอบธุรกิจรั่วไหล (data breach) ซึ่งส่งผลกระทบอย่างมีนัยสำคัญ
- เหตุการณ์ insider threat ทั้งด้วยเจตนา และไม่เจตนา จนเป็นเหตุให้ทรัพย์สินหรือข้อมูลของลูกค้าเสียหายหรือสูญหาย
- หน้าเว็บไซต์ของบริษัทโดนปลอมแปลง (website defacement) เป็นต้น

“ฮาร์ดแวร์” (hardware) อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย รวมถึงอุปกรณ์อื่น ๆ ที่เกี่ยวข้องกับระบบ IT ของผู้ประกอบธุรกิจ

“IT” เทคโนโลยีสารสนเทศ

“MFA” การยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication)

“non-disclosure agreement” ข้อตกลงในการไม่เปิดเผยข้อมูล

“privileged user” ผู้ใช้งานที่ได้รับสิทธิในการใช้งานในระดับสูง

การกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ (Information Technology Governance)

ขอบเขตการดำเนินการตามภาคผนวกนี้

ผู้ประกอบการที่มีความเสี่ยงระดับต่ำ ระดับปานกลาง หรือระดับสูง ให้ดำเนินการตามที่กำหนดในภาคผนวกนี้

การดำเนินการเกี่ยวกับการกำกับดูแลและบริหารจัดการด้าน IT

ส่วนที่ ๑ บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการของผู้ประกอบการ

ผู้ประกอบการต้องดำเนินการให้มีการควบคุมดูแลและบริหารจัดการความเสี่ยงด้าน IT ผ่านการกำกับดูแลโดยคณะกรรมการของผู้ประกอบการ เพื่อให้สอดคล้องกับระดับความเสี่ยงที่องค์กรยอมรับได้ โดยคำนึงถึงการบริหารและจัดการความเสี่ยงขององค์กร (enterprise risk) (ถ้ามี) ซึ่งอย่างน้อยต้องครอบคลุมในเรื่องดังนี้

๑.๑ การกำหนดกรอบการกำกับดูแลด้าน IT (IT governance framework) และการกำกับดูแลแผนงานด้าน IT ให้สอดคล้องกับแผนทางธุรกิจ และมีความเหมาะสมเพียงพอที่จะรองรับการเปลี่ยนแปลงด้าน IT และการเปลี่ยนแปลงการดำเนินธุรกิจในอนาคต

๑.๒ การจัดสรรทรัพยากรทางด้าน IT และทรัพยากรบุคคลที่ปฏิบัติงานด้าน IT ให้มีความเหมาะสมเพียงพอต่อการดำเนินธุรกิจ

๑.๓ การกำหนดนโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT ซึ่งมีการกำหนดเป็นลายลักษณ์อักษร โดยอย่างน้อยต้องครอบคลุมนโยบายตามที่กำหนดในส่วนของ ๒ ข้อ ๒.๒

๑.๔ การกำหนดขั้นตอนและวิธีปฏิบัติงานในการบริหารจัดการความเสี่ยงด้าน IT และการรักษาความมั่นคงปลอดภัยด้าน IT เพื่อให้เป็นไปตามนโยบายในข้อ ๑.๓ รวมถึงกำกับดูแลให้มีการนำไปปฏิบัติอย่างเหมาะสม

๑.๕ การสร้างความรู้และความตระหนักรู้ด้านความเสี่ยงด้าน IT แก่กรรมการและบุคลากรอย่างต่อเนื่อง และมีประสิทธิผล

๑.๖ การติดตาม ตรวจสอบ และรายงานผลการปฏิบัติงานเพื่อให้เป็นไปตามนโยบายในข้อ ๑.๓ ต่อคณะกรรมการของผู้ประกอบการ หรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบการ เฉพาะกรณีเป็นสาขาของธนาคารพาณิชย์ต่างประเทศ โดยมีการรายงานอย่างน้อยปีละ ๑ ครั้ง และในกรณีที่มีเหตุการณ์หรือการเปลี่ยนแปลงใด ๆ ซึ่งอาจส่งผลกระทบต่ออย่างมีนัยสำคัญต่อการปฏิบัติงานเพื่อให้เป็นไปตามนโยบายดังกล่าว ต้องมีการรายงานให้คณะกรรมการของผู้ประกอบการ หรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบการ เฉพาะกรณีเป็นสาขาของธนาคารพาณิชย์ต่างประเทศ ทราบโดยไม่ชักช้าด้วย

ส่วนที่ ๒ การกำกับดูแลและบริหารจัดการความเสี่ยงด้าน IT ในระดับองค์กร

๒.๑ ผู้ประกอบธุรกิจต้องจัดให้มีโครงสร้างการกำกับดูแลและบริหารจัดการความเสี่ยงด้าน IT โดยอย่างน้อยต้องมีลักษณะดังนี้

๒.๑.๑ ทำให้เกิดการถ่วงดุลอย่างเป็นอิสระ

๒.๑.๒ สอดคล้องตามหลักการแบ่งแยกหน้าที่ ๓ ระดับ (๓ Lines of Defense: ๓ LoDs) โดยมีการแบ่งแยกหน้าที่อย่างชัดเจนระหว่างการทำหน้าที่ด้าน IT ดังนี้

ระดับที่ ๑ (first line of defense) : การปฏิบัติงาน

ระดับที่ ๒ (second line of defense) : การบริหารความเสี่ยงและกำกับการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง

ระดับที่ ๓ (third line of defense) : การตรวจสอบ

๒.๒ ผู้ประกอบธุรกิจต้องจัดให้มีนโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT เป็นลายลักษณ์อักษร โดยต้องได้รับความเห็นชอบจากคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจ อย่างน้อยต้องครอบคลุมในเรื่องดังนี้

นโยบาย	เรื่องที่ต้องครอบคลุม
๒.๒.๑ <u>นโยบายการบริหารจัดการความเสี่ยงด้าน IT</u> (IT risk management policy)	(๑) บทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารจัดการความเสี่ยงด้าน IT (๒) การจัดให้มีกระบวนการบริหารจัดการความเสี่ยงด้าน IT เพื่อให้อยู่ในระดับที่องค์กรยอมรับได้
๒.๒.๒ <u>นโยบายการรักษาความมั่นคงปลอดภัยด้าน IT</u> (IT security policy)	(๑) โครงสร้างการบริหารงานเพื่อการรักษาความมั่นคงปลอดภัยด้าน IT (organization of information technology security) (๒) การบริหารจัดการบุคลากร และบุคคลภายนอก (๓) การบริหารจัดการทรัพย์สินด้าน IT (IT asset management) (๔) การรักษาความมั่นคงปลอดภัยของข้อมูล (data security) (๕) การควบคุมการเข้าถึงข้อมูลและระบบ IT (access control) (๖) การควบคุมการเข้ารหัส (cryptographic control) (๗) การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security) (๘) การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT (IT operations security) (๙) การรักษาความมั่นคงปลอดภัยเกี่ยวกับระบบเครือข่ายสื่อสาร (communication system security)

นโยบาย	เรื่องที่ต้องครอบคลุม
	(๑๐) การบริหารจัดการโครงการด้าน IT การจัดหา พัฒนาและบำรุงรักษาระบบ IT (IT project management, and system acquisition, development and maintenance) (๑๑) การบริหารจัดการเหตุการณ์ผิดปกติด้าน IT (IT incident management) (๑๒) แผนฉุกเฉินด้าน IT (IT contingency plan)

๒.๓ ผู้ประกอบธุรกิจต้องจัดให้มีการดำเนินการตามนโยบายในข้อ ๒.๒ ดังนี้

๒.๓.๑ สื่อสารนโยบายตามข้อ ๒.๒ ให้แก่บุคคลที่เกี่ยวข้อง^๑ รับทราบตามบทบาทหน้าที่ ความรับผิดชอบ และสิทธิการเข้าถึงข้อมูล ในลักษณะที่สามารถเข้าถึงได้ง่าย เพื่อให้บุคคลที่เกี่ยวข้องดังกล่าวเข้าใจและสามารถปฏิบัติตามนโยบายได้อย่างถูกต้อง

๒.๓.๒ กำหนดขั้นตอนและวิธีปฏิบัติงานให้เป็นไปตามนโยบายตามข้อ ๒.๒

๒.๓.๓ ในกรณีที่มีการเปลี่ยนแปลงนโยบายตามข้อ ๒.๒ ต้องสื่อสารให้บุคคลที่เกี่ยวข้องได้รับทราบอย่างทั่วถึง และต้องปรับปรุงขั้นตอนและวิธีปฏิบัติงานให้สอดคล้องกับการเปลี่ยนแปลงดังกล่าว

๒.๔ ผู้ประกอบธุรกิจต้องทบทวนหรือปรับปรุงนโยบายตามข้อ ๒.๒ อย่างน้อยปีละ ๑ ครั้ง และโดยไม่ชักช้าเมื่อมีเหตุการณ์ใด ๆ ซึ่งอาจส่งผลกระทบต่อการกำกับดูแลและบริหารจัดการความเสี่ยงด้าน IT อย่างมีนัยสำคัญ

^๑ “บุคคลที่เกี่ยวข้อง” หมายความว่า บุคลากร กรรมการ รวมถึงบุคคลภายนอก

การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Technology Security)

ขอบเขตการดำเนินการตามภาคผนวกนี้

๑. ผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ ระดับปานกลาง หรือระดับสูง ให้ดำเนินการตามที่กำหนดในภาคผนวกนี้
๒. ผู้ประกอบธุรกิจขนาดเล็ก ให้ดำเนินการรักษาความมั่นคงปลอดภัยด้าน IT ขั้นต้น อย่างน้อยในเรื่องดังนี้
 - ๒.๑ ส่วนที่ ๒ การบริหารจัดการบุคลากร และบุคคลภายนอก ข้อ ๒.๒ บุคคลภายนอก
 - ๒.๒ ส่วนที่ ๕ การควบคุมการเข้าถึงข้อมูลและระบบ IT (access control)
 - ๒.๓ ส่วนที่ ๘ การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT (IT operations security) ดังนี้
 - ข้อ ๘.๑ การบริหารจัดการการตั้งค่าระบบ (system configuration management)
 - ข้อ ๘.๔ การรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงาน (endpoint)
 - ข้อ ๘.๕ การกำหนดนโยบายและมาตรการรักษาความปลอดภัยสำหรับการใช้งานอุปกรณ์ส่วนตัว (bring your own device : BYOD)
 - ข้อ ๘.๙ การประเมินช่องโหว่ทางเทคนิค (technical vulnerability assessment)
 - ข้อ ๘.๑๐ การทดสอบการเจาะระบบงาน (penetration test)

ผู้ประกอบธุรกิจขนาดเล็ก ต้องจัดให้มีการทดสอบการเจาะระบบที่ครอบคลุมระบบงาน (application system) และระบบเครือข่ายที่มีช่องทางเชื่อมต่อกับเครือข่ายสาธารณะ (internet facing) อย่างน้อยทุก ๓ ปี และทุกครั้งที่มีการเปลี่ยนแปลงระบบดังกล่าวอย่างมีนัยสำคัญ สำหรับระบบอื่น ๆ ต้องจัดให้มีการประเมินความเสี่ยงจากการบุกรุกผ่านระบบเครือข่ายคอมพิวเตอร์ที่ใช้สื่อสารภายในองค์กร เพื่อกำหนดขอบเขตการทดสอบการเจาะระบบได้ตามความเหมาะสม

 - ข้อ ๘.๑๑ การบริหารจัดการโปรแกรมแก้ไขช่องโหว่ (patch management)- ๒.๔ ส่วนที่ ๑๑ การบริหารจัดการเหตุการณ์ผิดปกติด้าน IT (IT incident management) ดังนี้
 - ข้อ ๑๑.๓ รายงานเหตุการณ์ผิดปกติด้าน IT ต่อผู้มีหน้าที่รับผิดชอบเหตุการณ์ และสำนักงาน โดยไม่ชักช้าเมื่อทราบเหตุการณ์ดังกล่าว
 - ข้อ ๑๑.๔ วิเคราะห์สาเหตุที่แท้จริง (root cause) ของเหตุการณ์ผิดปกติด้าน IT เพื่อกำหนดแนวทางการแก้ไขและป้องกันไม่ให้เกิดเหตุการณ์ซ้ำในอนาคต
 - ข้อ ๑๑.๕ บันทึกข้อมูลที่เกี่ยวข้องกับการบริหารจัดการเหตุการณ์ผิดปกติด้าน IT และจัดเก็บข้อมูลดังกล่าวเป็นระยะเวลาไม่น้อยกว่า ๒ ปีนับแต่วันที่เกิดเหตุการณ์นั้น โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้สำนักงานสามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า

การดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้าน IT

ส่วนที่ ๑ โครงสร้างการบริหารงานเพื่อการรักษาความมั่นคงปลอดภัยด้าน IT (organization of information technology security)

ผู้ประกอบการต้องดำเนินการจัดให้มีโครงสร้างดังกล่าว โดยมีลักษณะอย่างน้อยดังนี้

๑.๑ กำหนดโครงสร้างภายในองค์กร (organizational structure) ในการปฏิบัติงานด้าน IT โดยมีรายละเอียดหน้าที่และความรับผิดชอบของบุคลากรเป็นลายลักษณ์อักษร

๑.๒ มีการสอบทานการปฏิบัติงานเพื่อป้องกันความเสี่ยงในการรักษาความมั่นคงปลอดภัยของระบบ IT ที่อาจเกิดขึ้นในการปฏิบัติงาน

ส่วนที่ ๒ การบริหารจัดการบุคลากร และบุคคลภายนอก

บุคลากรหรือบุคคลภายนอก	การบริหารจัดการ
๒.๑ บุคลากรที่เกี่ยวข้องหรือที่ใช้ระบบ IT ปฏิบัติงาน	ผู้ประกอบการต้องบริหารจัดการบุคลากรตามข้อ ๒.๑ อย่างเหมาะสม โดยดำเนินการอย่างน้อยดังนี้ (๑) มีกระบวนการคัดเลือกบุคลากรในการปฏิบัติหน้าที่ดังนี้ (๑.๑) คำนึงถึงความรู้ ความสามารถ และความเพียงพอในการปฏิบัติงาน (๑.๒) มีการตรวจสอบข้อมูลของบุคลากรก่อนการว่าจ้างอย่างเพียงพอ และสอดคล้องกับความเสี่ยงของตำแหน่งงานและหน้าที่ความรับผิดชอบ (๒) มีข้อกำหนดให้บุคลากรทำความเข้าใจ รับทราบ และลงนามยอมรับในเรื่องดังนี้ (๒.๑) บทบาทหน้าที่และความรับผิดชอบของบุคลากรดังกล่าวเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้าน IT (๒.๒) non-disclosure agreement (๓) สร้างความตระหนักรู้ถึงความเสี่ยงด้าน IT ให้แก่บุคลากรซึ่งสามารถเข้าถึงข้อมูลหรือระบบงานภายในองค์กร เพื่อให้บุคลากรดังกล่าวสามารถใช้งานระบบ IT ได้อย่างปลอดภัย (๔) กำหนดให้บุคลากรงดเว้นการใช้งานระบบ IT ในลักษณะที่อาจก่อให้เกิดความเสียหายแก่ผู้ประกอบการ ตลาดทุนโดยรวม หรือที่เป็น การกระทำผิดกฎหมาย หรือข้อกำหนดและจรรยาบรรณที่ผู้ประกอบการ กำหนดไว้ (ถ้ามี)

บุคลากรหรือบุคคลภายนอก	การบริหารจัดการ
	(๕) กำหนดมาตรการในการลงโทษบุคลากรที่มีพฤติกรรมฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายและมาตรการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT (๖) กำหนดขั้นตอนปฏิบัติเมื่อสิ้นสุดการจ้างงาน หรือเมื่อมีการเปลี่ยนแปลงตำแหน่งงาน เพื่อป้องกันการละเมิดหรือความเสียหายที่อาจเกิดขึ้นต่อทรัพย์สินด้าน IT
๒.๒ บุคคลภายนอก ในกรณีที่ผู้ประกอบการมีการดำเนินการอย่างใดอย่างหนึ่งดังนี้ ๒.๒.๑ ใช้บริการงานด้าน IT จากบุคคลภายนอก ๒.๒.๒ เชื่อมต่อระบบ IT กับบุคคลภายนอก ๒.๒.๓ อนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญของผู้ประกอบการหรือข้อมูลของลูกค้าที่อยู่ในรูปแบบอิเล็กทรอนิกส์และอยู่ภายใต้การควบคุมดูแลของผู้ประกอบการ	ผู้ประกอบการต้องบริหารจัดการบุคคลภายนอกตามข้อ ๒.๒.๑ , ๒.๒.๒ หรือ ๒.๒.๓ ดังนี้ (๑) ประเมินความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก รวมถึงผู้รับดำเนินการช่วง (subcontract) จากบุคคลภายนอก (ถ้ามี) (๒) กำหนดวิธีปฏิบัติและหลักเกณฑ์ในการคัดเลือกบุคคลภายนอก (๓) กำหนดบทบาท หน้าที่ และความรับผิดชอบของผู้ประกอบการและบุคคลภายนอกอย่างชัดเจนและเป็นลายลักษณ์อักษร (๔) กรณีบุคคลภายนอกซึ่งเป็นผู้ให้บริการงานด้าน IT รายที่มีนัยสำคัญตามผลการประเมินความเสี่ยงในข้อ ๒.๒ (๑) ข้อตกลงหรือสัญญาการให้บริการต้องระบุสิทธิให้ผู้ประกอบการ สำนักงาน และผู้ตรวจสอบภายนอกที่ได้รับการแต่งตั้งจากผู้ประกอบการหรือสำนักงาน สามารถเข้าตรวจสอบการดำเนินงานและการควบคุมภายในของบุคคลภายนอกดังกล่าวได้ หากมีเหตุจำเป็นทำให้ผู้ประกอบการไม่สามารถระบุสิทธิในการเข้าตรวจสอบตามวรรคหนึ่งไว้ในข้อตกลงหรือสัญญา ผู้ประกอบการต้องมีมาตรการประเมินหรือติดตามการดำเนินงานและการควบคุมภายในของบุคคลภายนอกให้รัดกุมเพียงพอสอดคล้องกับความเสี่ยงและความมีนัยสำคัญของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูล (๕) มี non-disclosure agreement สำหรับบุคคลภายนอกหรือผู้รับดำเนินการช่วงของบุคคลภายนอก ในกรณีที่บุคคลดังกล่าวสามารถเข้าถึงข้อมูลสำคัญของผู้ประกอบการหรือข้อมูลของลูกค้า

บุคลากรหรือบุคคลภายนอก	การบริหารจัดการ
	(๖) กำกับดูแล ติดตาม และบริหารจัดการความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก โดยต้องสอดคล้องกับระดับความเสี่ยงและระดับความมั่นคงสำคัญของบุคคลภายนอก (๗) รักษาความมั่นคงปลอดภัยด้าน IT จากการให้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก ที่สอดคล้องกับการรักษาความมั่นคงปลอดภัยด้าน IT ของผู้ประกอบการธุรกิจ หรือสอดคล้องกับมาตรฐานสากลที่ได้รับการยอมรับโดยทั่วไป (๘) เตรียมความพร้อมรับมือต่อเหตุการณ์ผิดปกติด้าน IT ที่อาจเกิดขึ้น และมีผลกระทบอย่างมีนัยสำคัญ เพื่อให้สามารถให้บริการหรือดำเนินธุรกิจได้อย่างต่อเนื่อง

ส่วนที่ ๓ การบริหารจัดการทรัพย์สินด้าน IT (IT asset management)

ผู้ประกอบการต้องจัดให้มีการบริหารจัดการทรัพย์สินด้าน IT เพื่อนำไปใช้ดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้าน IT ได้อย่างเหมาะสม ครบถ้วนและเป็นปัจจุบัน ดังนี้

- ๓.๑ จัดทำทะเบียนรายการทรัพย์สินด้าน IT ประเภทฮาร์ดแวร์ ซอฟต์แวร์ รวมถึงสิทธิในการใช้งานฮาร์ดแวร์และซอฟต์แวร์
- ๓.๒ กำหนดบุคคลหรือหน่วยงานซึ่งรับผิดชอบทรัพย์สินด้าน IT แต่ละรายการ
- ๓.๓ จัดให้มีการบำรุงรักษาทรัพย์สินด้าน IT อย่างสม่ำเสมอ

ส่วนที่ ๔ การรักษาความมั่นคงปลอดภัยของข้อมูล (data security)

ผู้ประกอบการต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลเพื่อให้ข้อมูลมีความถูกต้องครบถ้วน และมีสภาพพร้อมใช้งาน รวมถึงสามารถรักษาความลับของข้อมูลได้อย่างเหมาะสม ดังนี้

- ๔.๑ การกำหนดบุคคลหรือหน่วยงานซึ่งเป็นเจ้าของข้อมูล
- ๔.๒ การจัดชั้นความลับของข้อมูล (data classification) และแนวทางการรักษาความปลอดภัยของข้อมูลที่สอดคล้องตามชั้นความลับ โดยครอบคลุมข้อมูลดังนี้
 - ๔.๒.๑ ข้อมูลที่อยู่บนอุปกรณ์ที่ใช้ปฏิบัติงาน (data at endpoint)
 - ๔.๒.๒ ข้อมูลที่อยู่ระหว่างการรับส่งผ่านเครือข่าย (data in transit)
 - ๔.๒.๓ ข้อมูลที่อยู่บนระบบงานและสื่อบันทึกข้อมูล (data at rest)
- ๔.๓ การจัดให้มีแนวทางในการนำเข้า ประมวลผล และทำลายข้อมูลอย่างปลอดภัย
- ๔.๔ การจัดทำทะเบียนทรัพย์สินด้าน IT ประเภทข้อมูล (data inventory) ให้ครบถ้วนและเป็นปัจจุบัน

ส่วนที่ ๕ การควบคุมการเข้าถึงข้อมูลและระบบ IT (access control)

ผู้ประกอบธุรกิจต้องจัดให้มีการควบคุมการเข้าถึงข้อมูลและระบบ IT อย่างมีประสิทธิภาพ เพื่อให้สามารถป้องกันการเข้าถึงและเปลี่ยนแปลงแก้ไขโดยผู้ไม่มีสิทธิหรือไม่ได้รับอนุญาต ดังนี้

๕.๑ จัดให้มีแนวทางการบริหารจัดการบัญชีผู้ใช้งานและสิทธิการเข้าถึง โดยมีการทบทวนปรับปรุงสิทธิให้เหมาะสมอย่างสม่ำเสมอ สอดคล้องกับหน้าที่ความรับผิดชอบ รวมถึงมีกระบวนการเพิกถอนสิทธิเมื่อสิ้นสุดความจำเป็นต้องใช้งาน

๕.๒ จัดให้มีกระบวนการยืนยันตัวตนผู้ใช้งาน (authentication) ที่เหมาะสมกับความเสี่ยง และป้องกันการปฏิเสธความรับผิดชอบ

๕.๓ กำหนดมาตรการควบคุม จำกัด และติดตามการใช้งานบัญชี privileged user (privileged user management) ดังนี้

๕.๓.๑ มี MFA เมื่อเข้าใช้งานและเปลี่ยนรหัสผ่านสำหรับระบบปฏิบัติการและระบบฐานข้อมูลที่เกี่ยวข้องกับระบบ IT ที่มีความสำคัญ

๕.๓.๒ กรณีผู้ประกอบธุรกิจมีข้อจำกัดสำหรับ MFA สามารถใช้วิธีการอื่นใดที่เทียบเท่าทดแทน และจัดให้มีการประเมินความเสี่ยงและพิจารณาแนวทางควบคุมความเสี่ยงก่อนดำเนินการเพื่อขออนุมัติยกเว้น (exception)

๕.๓.๓ มีการควบคุมและติดตามตรวจสอบการใช้งานบัญชี privileged user อย่างเข้มงวด

ส่วนที่ ๖ การควบคุมการเข้ารหัส (cryptographic control)

ผู้ประกอบธุรกิจต้องจัดให้มีการควบคุมการเข้ารหัสที่เชื่อถือได้และเป็นไปตามมาตรฐานสากล โดยกำหนดวิธีการเข้ารหัสข้อมูล (encryption) และการบริหารจัดการกุญแจเข้ารหัส (key management) อย่างปลอดภัยเพื่อให้มั่นใจได้ว่า การดำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และความถูกต้องแท้จริง (authenticity) ของข้อมูลมีความเหมาะสมและมีประสิทธิภาพ ดังนี้

๖.๑ กำหนดวิธีการเข้ารหัสที่ปลอดภัย

๖.๒ กำหนดการบริหารจัดการกุญแจเข้ารหัส โดยจัดให้มีมาตรการการควบคุมตั้งแต่การสร้างและติดตั้งกุญแจเข้ารหัส การจัดเก็บและสำรองกุญแจเข้ารหัส ไปจนถึงการเพิกถอนหรือทำลายกุญแจเข้ารหัส

๖.๓ กำหนดมาตรการการควบคุมกุญแจเข้ารหัสที่ให้บริการโดยบุคคลภายนอก ซึ่งต้องตรวจสอบเพื่อให้มั่นใจได้ว่ากุญแจการเข้ารหัสที่สร้างขึ้นไม่มีการนำมาใช้ร่วมกับบุคคลอื่น

๖.๔ กำหนดกระบวนการรองรับกรณีเกิดการรั่วไหลของกุญแจเข้ารหัส

ส่วนที่ ๗ การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security)

ผู้ประกอบธุรกิจต้องจัดให้มีการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อมของทรัพย์สินด้าน IT พร้อมทั้งมีระบบการป้องกัน และกระบวนการบำรุงรักษาฮาร์ดแวร์และระบบสาธารณูปโภค (facilities)

ที่เกี่ยวข้องกับ IT เพื่อให้สามารถป้องกันความเสียหายต่อทรัพย์สินด้าน IT ที่จัดเก็บอยู่ในศูนย์คอมพิวเตอร์หลัก ศูนย์คอมพิวเตอร์สำรอง และศูนย์คอมพิวเตอร์จากบุคคลภายนอก (co-location)

ส่วนที่ ๘ การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT (IT operations security)

ผู้ประกอบการธุรกิจต้องมีมาตรการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT เพื่อให้การปฏิบัติงานเกี่ยวกับการประมวลผลข้อมูลมีความถูกต้องและมั่นคงปลอดภัย โดยต้องครอบคลุมการบริหารจัดการอย่างน้อยในเรื่องดังนี้

๘.๑ การบริหารจัดการการตั้งค่าระบบ (system configuration management) โดยมีกระบวนการในการควบคุมการตั้งค่าระบบ และสอบทานการตั้งค่าระบบอย่างสม่ำเสมอ เพื่อให้การตั้งค่าระบบเป็นไปอย่างถูกต้องและปลอดภัย

๘.๒ การบริหารจัดการการเปลี่ยนแปลง (change management) อย่างรัดกุมเพียงพอ เพื่อให้การเปลี่ยนแปลงเป็นไปตามวัตถุประสงค์ที่กำหนดไว้อย่างถูกต้องครบถ้วน และป้องกันการเปลี่ยนแปลงโดยไม่ได้รับอนุญาต

๘.๓ การบริหารจัดการขีดความสามารถของระบบ IT (capacity management) โดยจัดให้มีมาตรฐานและวิธีปฏิบัติเรื่องการจัดการขีดความสามารถ การติดตามประสิทธิภาพการทำงานของระบบ และการประเมินแนวโน้มการใช้ทรัพยากรด้าน IT เพื่อให้สามารถรองรับการดำเนินธุรกิจในปัจจุบัน และสามารถวางแผนการจัดสรรทรัพยากรให้รองรับการใช้งานในอนาคตได้อย่างมีประสิทธิภาพ

๘.๔ การรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงาน (endpoint) ให้สามารถป้องกันการโจมตีด้วยรูปแบบต่าง ๆ หรือภัยจากโปรแกรมไม่ประสงค์ดี (malware) เพื่อลดความเสี่ยงจากการถูกโจมตีระบบ IT ขององค์กร หรือถูกใช้เป็นช่องทางในการโจมตีหน่วยงานอื่น และป้องกันการรั่วไหลของข้อมูลสำคัญหรือการเข้าใช้งานระบบ IT โดยไม่ได้รับอนุญาต

๘.๕ การกำหนดนโยบายและมาตรการรักษาความปลอดภัยสำหรับการปฏิบัติงานจากเครือข่ายภายนอก (teleworking) การใช้งานอุปกรณ์เคลื่อนที่ (mobile device) และรวมถึงการใช้งานอุปกรณ์ส่วนตัว (Bring Your Own Device: BYOD) โดยพิจารณาความเสี่ยงที่เกี่ยวข้อง และจัดให้มีมาตรการควบคุมอย่างเหมาะสม

๘.๖ การสำรองข้อมูล (data backup) ที่สำคัญด้วยวิธีการและความถี่ที่เหมาะสม เพื่อให้ข้อมูลสำรองมีสภาพพร้อมใช้งานสอดคล้องกับเป้าหมายการกู้คืนระบบ IT ในกรณีที่ระบบ IT และข้อมูลหลักเกิดเหตุขัดข้องหรือได้รับความเสียหาย โดยต้องมีการทดสอบข้อมูลสำรองและกระบวนการกู้คืนข้อมูลอย่างน้อยปีละ ๑ ครั้ง

๘.๗ การจัดเก็บข้อมูลบันทึกเหตุการณ์การใช้งานเกี่ยวกับระบบ IT (log) อย่างครบถ้วนและเพียงพอ เพื่อให้สามารถใช้เป็นหลักฐานการทำธุรกรรมทางอิเล็กทรอนิกส์ และสามารถติดตามและตรวจสอบการเข้าถึงและใช้งานข้อมูลและระบบ IT ย้อนหลังได้ ตามที่กฎหมายกำหนด

๘.๘ การติดตามดูแลระบบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (security monitoring) โดยมีกระบวนการหรือเครื่องมือป้องกันและตรวจจับเหตุการณ์ผิดปกติด้าน IT หรือภัยคุกคามทางไซเบอร์ที่อาจส่งผล

กระทบต่อความมั่นคงปลอดภัยต่อระบบ IT ที่มีนัยสำคัญ

๘.๙ การประเมินช่องโหว่ทางเทคนิค (technical vulnerability assessment) ของระบบ IT ที่เหมาะสมกับระดับความเสี่ยงเพื่อให้ทราบถึงช่องโหว่ และสามารถดำเนินการแก้ไขและป้องกันภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นได้อย่างทันท่วงที โดยการประเมินช่องโหว่ทางเทคนิคครอบคลุมระบบ IT ที่มีนัยสำคัญ และระบบ IT ที่เชื่อมต่อกับเครือข่ายสาธารณะ (internet facing) ทุกระบบอย่างน้อยปีละ ๑ ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญของระบบดังกล่าว เช่น การเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ IT หรือการเพิ่มเติมฟังก์ชันสำคัญของระบบ IT เป็นต้น

๘.๑๐ การทดสอบการเจาะระบบ (penetration test)

๘.๑๐.๑ ผู้ประกอบธุรกิจต้องจัดให้มีการทดสอบการเจาะระบบดังนี้

ระบบงาน	การทดสอบ
(๑) ระบบงาน (application system) และระบบเครือข่ายที่มีการเชื่อมต่อกับเครือข่ายสาธารณะ (internet facing)	(๑.๑) อย่างน้อยปีละ ๑ ครั้ง และ (๑.๒) ทุกครั้งที่มีการเปลี่ยนแปลงระบบดังกล่าวอย่างมีนัยสำคัญ
(๒) ระบบอื่น ๆ นอกจาก (๑)	จัดให้มีการประเมินความเสี่ยงจากการบุกรุกผ่านระบบเครือข่ายคอมพิวเตอร์ที่ใช้สื่อสารภายในองค์กร เพื่อกำหนดขอบเขตการทดสอบการเจาะระบบและทดสอบการเจาะระบบตามความเหมาะสม

๘.๑๐.๒ การทดสอบการเจาะระบบข้างต้น ต้องดำเนินการโดยผู้เชี่ยวชาญภายในหรือภายนอกที่เป็นอิสระจากเจ้าของระบบ

๘.๑๐.๓ ในกรณีที่มีการตรวจพบช่องโหว่ ผู้ประกอบธุรกิจต้องดำเนินการแก้ไข และป้องกันภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นอย่างทันท่วงที เพื่อขจัดความเสี่ยงจากช่องโหว่ดังกล่าว

๘.๑๐.๔ ผู้ประกอบธุรกิจต้องจัดเก็บรายงานการดำเนินการตามข้อ ๘.๑๐ เป็นระยะเวลาไม่น้อยกว่า ๒ ปีนับแต่วันที่จัดทำเอกสารนั้น โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้สำนักงานสามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า

๘.๑๐.๕ ผู้ประกอบธุรกิจต้องนำส่งรายงานผลการทดสอบการเจาะระบบโดยไม่ชักช้าเมื่อได้รับการแจ้งจากสำนักงาน

๘.๑๑ การบริหารจัดการโปรแกรมแก้ไขช่องโหว่ (patch management) โดยจัดให้มีกระบวนการควบคุมการติดตั้งโปรแกรมแก้ไขช่องโหว่บนระบบและอุปกรณ์ เพื่อลดความเสี่ยงที่จะถูกโจมตีในอนาคต

ส่วนที่ ๙ การรักษาความมั่นคงปลอดภัยเกี่ยวกับระบบเครือข่ายสื่อสาร (communication system security)

ผู้ประกอบการต้องมีการรักษาความมั่นคงปลอดภัยเกี่ยวกับระบบเครือข่ายสื่อสารอย่างเหมาะสม เพื่อให้ระบบเครือข่ายสื่อสารและข้อมูลที่ได้รับส่งผ่านระบบเครือข่ายสื่อสารมีความมั่นคงปลอดภัย สามารถป้องกันการบุกรุกหรือภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น รวมทั้งพร้อมให้บริการได้อย่างต่อเนื่อง

ส่วนที่ ๑๐ การบริหารจัดการโครงการด้าน IT (IT project management) การจัดหา พัฒนา และบำรุงรักษา ระบบ IT (system acquisition, development and maintenance)

ผู้ประกอบการต้องมีการบริหารจัดการโครงการด้าน IT และมีการจัดหา พัฒนา รวมถึงบำรุงรักษา ระบบ IT เพื่อให้มั่นใจว่ามีการรักษาความมั่นคงปลอดภัยตลอดวงจรชีวิตของระบบ IT (entire life cycle) ดังนี้

การดำเนินการ	รายละเอียด
๑๐.๑ บริหารจัดการโครงการด้าน IT (IT project management)	กำหนดกรอบการบริหารจัดการโครงการ (project management framework) เพื่อให้การบริหารจัดการโครงการด้าน IT ที่มีนัยสำคัญ เป็นไปอย่างมีประสิทธิภาพ สามารถส่งมอบโครงการได้อย่างถูกต้อง ครบถ้วนตามแผนงานและบรรลุวัตถุประสงค์ตามเป้าหมายที่กำหนดไว้
๑๐.๒ จัดหาระบบ IT (system acquisition)	จัดให้มีหลักเกณฑ์ในการจัดหาระบบ IT และผู้ให้บริการ เพื่อให้มั่นใจว่าระบบที่จัดหาสามารถตอบสนองความต้องการทางธุรกิจและความต้องการด้านความมั่นคงปลอดภัย IT โดยคำนึงถึงความยืดหยุ่นในการเปลี่ยนแปลงผู้ให้บริการ การเปลี่ยนแปลงเทคโนโลยี รวมถึงการเปลี่ยนแปลงต่าง ๆ ที่เกี่ยวข้องกับการดำเนินธุรกิจอย่างมีนัยสำคัญ
๑๐.๓ พัฒนาระบบ IT (system development)	จัดให้มีมาตรการควบคุมเกี่ยวกับการพัฒนาระบบ IT ในการออกแบบ พัฒนา ทดสอบระบบ และนำระบบขึ้นใช้งานจริง เพื่อให้มั่นใจว่าระบบมีความถูกต้อง มั่นคงปลอดภัย เชื่อถือได้ พร้อมใช้งาน และมีความยืดหยุ่นเพียงพอจะรองรับการใช้งานได้สอดคล้องกับแผนการดำเนินธุรกิจ โดยต้องดำเนินการอย่างน้อยดังนี้ (๑) มีการกำหนดรายละเอียดความต้องการของระบบ (requirement) และคุณสมบัติทางเทคนิค (technical specification) ของระบบที่พัฒนา ดังนี้ (๑.๑) ความมั่นคงปลอดภัย (security) (๑.๒) สภาพพร้อมใช้งาน (availability) (๑.๓) ขีดความสามารถที่รองรับ (capacity)

การดำเนินการ	รายละเอียด
	(๒) มีการแบ่งแยกบทบาทหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องในการพัฒนาระบบ เพื่อให้มีการสอบทานก่อนนำระบบขึ้นไปให้บริการจริง (๓) มีการแบ่งแยกสภาพแวดล้อมของระบบงานที่ใช้สำหรับการพัฒนา (development) และการทดสอบ (testing) ออกจากระบบงานที่ให้บริการจริง (production) (๔) มีกระบวนการหรือเครื่องมือควบคุมการพัฒนาชุดคำสั่งคอมพิวเตอร์ให้มีความปลอดภัย (๕) มีการทดสอบระบบ IT ที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลง เพื่อให้มั่นใจได้ว่าระบบดังกล่าวสามารถประมวลผลได้อย่างถูกต้อง ครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน (๖) มีมาตรการควบคุมความถูกต้องครบถ้วนของการแปลงข้อมูล (data conversion) (๗) มีมาตรการรักษาความมั่นคงปลอดภัย และความลับของข้อมูลสำคัญที่นำไปใช้ในการทดสอบ (๘) มีการทดสอบประสิทธิภาพ (performance test) ของระบบที่เกี่ยวข้องกับการให้บริการหรือการทำธุรกรรมทางอิเล็กทรอนิกส์ เมื่อมีการพัฒนาหรือเปลี่ยนแปลงระบบอย่างมีนัยสำคัญ เพื่อให้มั่นใจว่าระบบดังกล่าวสามารถรองรับปริมาณการใช้งานได้สอดคล้องกับความต้องการทางธุรกิจ (๙) ในกรณีที่มีการมอบหมายให้บุคคลภายนอกเป็นผู้พัฒนาหรือแก้ไขเปลี่ยนแปลงระบบ IT ผู้ประกอบธุรกิจต้องจัดให้มีการติดตาม และควบคุมการดำเนินการให้เป็นไปตามข้อตกลงในการมอบหมายงาน (๑๐) มีกระบวนการขออนุมัติจากผู้บริหารหรือคณะกรรมการที่ได้รับมอบหมายจากผู้ประกอบธุรกิจ ก่อนนำระบบขึ้นใช้งานจริง
๑๐.๔ แก้ไขเปลี่ยนแปลงระบบ IT (system change)	(๑) มีการประเมินผลกระทบ และจัดลำดับความสำคัญของการเปลี่ยนแปลง (๒) มีกระบวนการขออนุมัติการเปลี่ยนแปลง (change request) โดยต้องได้รับการอนุมัติจากหน่วยงานเจ้าของระบบ (system

การดำเนินการ	รายละเอียด
	owner) เป็นลายลักษณ์อักษร เพื่อให้มั่นใจได้ว่าการเปลี่ยนแปลงได้รับการพิจารณาความจำเป็นอย่างเหมาะสมแล้ว (๓) มีการทดสอบระบบก่อนนำไปตั้งค่า หรือนำไปติดตั้งบนระบบที่ให้บริการจริง เพื่อลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้น (๔) มีกระบวนการขออนุมัติจากผู้บริหารหรือคณะกรรมการที่ได้รับมอบหมายจากผู้ประกอบธุรกิจ ก่อนนำระบบขึ้นใช้งานจริง (๕) มีกระบวนการหรือเครื่องมือควบคุมการเปลี่ยนแปลงรุ่น (version) ของชุดคำสั่งคอมพิวเตอร์ (source code version control) และรองรับการถอยกลับสู่สภาพเดิม (fallback) (๖) ปรับปรุงรายละเอียดประกอบระบบงานที่ได้มีการแก้ไขเปลี่ยนแปลง เพื่อให้เป็นปัจจุบัน

ส่วนที่ ๑๑ การบริหารจัดการเหตุการณ์ผิดปกติด้าน IT (IT incident management)

ผู้ประกอบธุรกิจต้องมีการบริหารจัดการเหตุการณ์ผิดปกติด้าน IT อย่างเหมาะสมและทันท่วงที ดังนี้

๑๑.๑ จัดให้มีช่องทางรับแจ้งเหตุการณ์ผิดปกติด้าน IT จากบุคลากร ผู้ใช้บริการ และผู้ที่เกี่ยวข้อง

๑๑.๒ กำหนดแผน หรือขั้นตอนการบริหารจัดการเหตุการณ์ผิดปกติด้าน IT

๑๑.๓ รายงานเหตุการณ์ผิดปกติด้าน IT ต่อผู้มีหน้าที่รับผิดชอบเหตุการณ์ และสำนักงาน โดยไม่ชักช้า

เมื่อทราบเหตุการณ์ดังกล่าว

๑๑.๔ วิเคราะห์สาเหตุที่แท้จริง (root cause) ของเหตุการณ์ผิดปกติด้าน IT เพื่อกำหนดแนวทางการแก้ไข และป้องกันไม่ให้เกิดเหตุการณ์ซ้ำในอนาคต

๑๑.๕ บันทึกข้อมูลที่เกี่ยวข้องกับการบริหารจัดการเหตุการณ์ผิดปกติด้าน IT และจัดเก็บข้อมูลดังกล่าวเป็นระยะเวลาไม่น้อยกว่า ๒ ปีนับแต่วันที่เกิดเหตุการณ์นั้น โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้สำนักงานสามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า

๑๑.๖ ทดสอบและทบทวนขั้นตอนปฏิบัติหรือแผนการบริหารจัดการเหตุการณ์ผิดปกติด้าน IT อย่างน้อยปีละ ๑ ครั้ง โดยต้องครอบคลุมถึงการทดสอบการบริหารจัดการเหตุการณ์ด้านภัยคุกคามทางไซเบอร์ (cyber security drill) และจัดให้มีการรายงานผลการทดสอบและทบทวนต่อคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจ

ส่วนที่ ๑๒ แผนฉุกเฉินด้าน IT (IT contingency plan)

ผู้ประกอบการต้องจัดทำแผนฉุกเฉินด้าน IT เพื่อรองรับเหตุการณ์ผิดปกติด้าน IT ซึ่งส่งผลกระทบให้ไม่สามารถให้บริการได้ตามปกติ หรือไม่สามารถดำเนินธุรกิจอย่างต่อเนื่อง โดยต้องกู้คืนระบบให้กลับคืนสู่สภาพปกติภายในระยะเวลาที่เหมาะสมได้ ดังนี้

๑๒.๑ จัดให้มีคณะทำงานหรือหน่วยงานที่รับผิดชอบในการจัดทำแผนฉุกเฉินด้าน IT

๑๒.๒ กระบวนการจัดทำแผนฉุกเฉินด้าน IT ต้องครอบคลุมการดำเนินการ ดังนี้

๑๒.๒.๑ ประเมินความเสี่ยง (risk analysis) เพื่อให้สามารถระบุเหตุการณ์ความเสี่ยงที่อาจทำให้กระบวนการและระบบ IT หยุดชะงัก ไม่สามารถให้บริการได้ตามปกติ หรือไม่สามารถดำเนินธุรกิจอย่างต่อเนื่อง

๑๒.๒.๒ วิเคราะห์ผลกระทบทางธุรกิจ (business impact analysis) จากเหตุการณ์ความเสี่ยงตาม ข้อ ๑๒.๒.๑ เพื่อกำหนดระยะเวลาเป้าหมายในการกู้คืนระบบ IT (Recovery Time Objective: RTO) ระยะเวลาเป้าหมายสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective: RPO) และระยะเวลาสูงสุดที่ยอมให้กระบวนการทางธุรกิจหยุดชะงัก (Maximum Tolerable Downtime: MTD) อย่างเหมาะสม

๑๒.๒.๓ จัดทำแผนฉุกเฉินด้าน IT อย่างเป็นลายลักษณ์อักษร ซึ่งได้รับความเห็นชอบจากคณะกรรมการของผู้ประกอบการหรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบการ

๑๒.๓ จัดให้มีระบบ IT สำรอง และทรัพยากรที่จำเป็น เพื่อให้สามารถกู้คืนระบบได้ตามระยะเวลาเป้าหมายที่กำหนดไว้

๑๒.๔ สื่อสารให้บุคลากรที่เกี่ยวข้องมีความเข้าใจและสามารถปฏิบัติตามแผนฉุกเฉินด้าน IT อย่างเหมาะสม

๑๒.๕ ทบทวนและทดสอบการปฏิบัติตามแผนฉุกเฉินด้าน IT อย่างน้อยปีละ ๑ ครั้ง และเมื่อมีเหตุจำเป็นที่ควรได้รับการทบทวนและทดสอบดังกล่าว โดยรายงานผลการทบทวนและทดสอบต่อคณะกรรมการของผู้ประกอบการหรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบการ

๑๒.๖ กำหนดกระบวนการดำเนินงาน เพื่อรับมือเหตุการณ์การใช้ทรัพยากรด้าน IT หรือการใช้ประสิทธิภาพของระบบงานเกินขีดจำกัดของตัวชี้วัดที่กำหนดไว้ เช่น การจำกัดการให้บริการบางช่องทาง หรือตัดการเชื่อมต่อกับผู้ให้บริการหรือบุคคลภายนอกที่มีผลกระทบต่อระบบ IT เป็นต้น

๑๒.๗ จัดให้มีรายละเอียดในการติดต่อ ดังนี้ เพื่อให้สามารถประสานงานในการรายงานเหตุการณ์ผิดปกติด้าน IT หรือขอความช่วยเหลือจากหน่วยงานภายนอกที่เกี่ยวข้องได้อย่างมีประสิทธิภาพ โดยต้องปรับปรุงข้อมูลดังกล่าวให้เป็นปัจจุบันอยู่เสมอ

๑๒.๗.๑ รายชื่อหน่วยงานกำกับดูแลและบุคคลภายนอกที่ให้บริการหรือที่มีการเชื่อมต่อกับระบบ IT ของผู้ประกอบการ

๑๒.๗.๒ ช่องทางในการติดต่อ และรายชื่อผู้ที่เกี่ยวข้องของหน่วยงานกำกับดูแลหรือบุคคลภายนอกตามข้อ ๑๒.๗.๑

[แนบท้ายประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ สธ. ๓๘/๒๕๖๕ ซึ่งแก้ไขเพิ่มเติม
โดยประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ สธ. ๓๓/๒๕๖๗ (ฉบับที่ ๒)]

การตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology Audit)

ให้ผู้ประกอบธุรกิจดำเนินการตามที่กำหนดในภาคผนวกนี้

การดำเนินการ	รายละเอียดในการดำเนินการ
๑. การจัดให้มีผู้ตรวจสอบ	ผู้ตรวจสอบตามข้อ ๑. ต้องมีลักษณะดังนี้ ๑.๑ มีความเป็นอิสระจากผู้ทำหน้าที่ด้าน IT ในระดับ ดังนี้ ๑.๑.๑ ระดับที่ ๑ (first line of defense) : การปฏิบัติงาน ๑.๑.๒ ระดับที่ ๒ (second line of defense) : การบริหารความเสี่ยงและกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง ๑.๒ ในกรณีที่เป็นการตรวจสอบด้าน IT ตั้งแต่วันที่ ๑ มกราคม พ.ศ. ๒๕๖๗ เป็นต้นไป ผู้ตรวจสอบต้องผ่านการรับรองและมีวุฒิบัตรอย่างหนึ่งอย่างใดดังนี้ ๑.๒.๑ Certified Information Systems Auditor (CISA) ๑.๒.๒ Certified Information Security Manager (CISM) ๑.๒.๓ Certified Information Systems Security Professional (CISSP) ๑.๒.๔ ISO/IEC ๒๗๐๐๑ Lead Auditor ๑.๒.๕ ใบรับรองอื่นตามที่กำหนดเพิ่มเติมบนเว็บไซต์ของสำนักงาน
๒. การวางแผนและกำหนดขอบเขตการตรวจสอบ	ทบทวนแผนงานและขอบเขตการตรวจสอบให้สอดคล้องกับความเสี่ยงด้าน IT และประกาศที่ สธ. ๓๘/๒๕๖๕ โดยต้องดำเนินการอย่างน้อยปีละ ๑ ครั้ง และเมื่อมีเหตุจำเป็นที่ควรได้รับการทบทวนดังกล่าว
๓. การตรวจสอบด้าน IT ตามแผนงานและขอบเขตที่กำหนด	๓.๑ จัดให้มีการตรวจสอบและรายงานผลการตรวจสอบด้าน IT โดยมีรายละเอียดดังนี้ ๓.๑.๑ กรณีเป็นผู้ประกอบธุรกิจขนาดเล็ก ต้องจัดให้มีการตรวจสอบด้าน IT ที่ครอบคลุมหลักเกณฑ์ทั้งหมดที่บังคับใช้กับผู้ประกอบธุรกิจขนาดเล็ก แบบเต็มรูปแบบ (full scope) อย่างน้อยทุก ๓ ปี ตามรอบปีที่สำนักงานกำหนด ๓.๑.๒ กรณีเป็นผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ ต้องจัดให้มีการตรวจสอบด้าน IT ที่ครอบคลุมหลักเกณฑ์ทั้งหมดที่บังคับใช้กับผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ แบบเต็มรูปแบบ (full scope) อย่างน้อยทุก ๓ ปี ตามรอบปีที่สำนักงานกำหนด ทั้งนี้ กรณีที่เกิดเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ IT อย่างมีนัยสำคัญ ผู้ประกอบธุรกิจขนาดเล็กและผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ ต้องจัดให้มีการดำเนินการตรวจสอบด้าน IT แบบเต็มรูปแบบ (full scope) ภายในปีที่เกิดเหตุการณ์ดังกล่าว กรณีที่มิเหตุจำเป็นทำให้ผู้ประกอบธุรกิจขนาดเล็กหรือผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ ไม่สามารถดำเนินการตรวจสอบด้าน IT แบบเต็มรูปแบบ (full scope) ภายใน

การดำเนินการ	รายละเอียดในการดำเนินการ
	ปีที่เกิดเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ IT อย่างมีนัยสำคัญ ผู้ประกอบธุรกิจต้องดำเนินการดังต่อไปนี้ ภายใน ๔ เดือน นับแต่วันที่ทราบเหตุการณ์ดังกล่าว (๑) รายงานเหตุจำเป็นที่ทำให้ไม่สามารถดำเนินการตรวจสอบด้าน IT แบบเต็มรูปแบบ (full scope) ได้ภายในปีที่เกิดเหตุการณ์ดังกล่าว และแผนการตรวจสอบด้าน IT ต่อคณะกรรมการของผู้ประกอบธุรกิจ หรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจเฉพาะกรณีเป็นสาขาของธนาคารพาณิชย์ต่างประเทศ รวมทั้งรายงานเหตุจำเป็นดังกล่าวต่อสำนักงาน และ (๒) ดำเนินการตรวจสอบด้าน IT แบบเต็มรูปแบบ (full scope) ๓.๑.๓ กรณีเป็นผู้ประกอบธุรกิจที่มีความเสี่ยงระดับปานกลาง ต้องจัดให้มีการตรวจสอบด้าน IT ที่ครอบคลุมหลักเกณฑ์ทั้งหมดที่บังคับใช้กับผู้ประกอบธุรกิจที่มีความเสี่ยงระดับปานกลาง แบบเต็มรูปแบบ (full scope) อย่างน้อยปีละ ๑ ครั้ง ๓.๑.๔ กรณีเป็นผู้ประกอบธุรกิจที่มีความเสี่ยงระดับสูง ต้องจัดให้มีการตรวจสอบด้าน IT ที่ครอบคลุมหลักเกณฑ์ทั้งหมดที่บังคับใช้กับผู้ประกอบธุรกิจที่มีความเสี่ยงระดับสูง แบบเต็มรูปแบบ (full scope) อย่างน้อยปีละ ๑ ครั้ง ๓.๒ จัดให้มีการบันทึกข้อมูลเกี่ยวกับการตรวจสอบ เช่น กระดาษทำการ (working paper) และหลักฐานประกอบการตรวจ เป็นต้น เป็นระยะเวลาไม่น้อยกว่า ๒ ปีนับแต่วันที่จัดทำรายงานและแผนดังกล่าว โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้สำนักงานสามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า
๔. การจัดให้มีแผนการปรับปรุงแก้ไขข้อบกพร่องจากการตรวจสอบด้าน IT และการติดตามความคืบหน้า	จัดให้มีแผนการปรับปรุงแก้ไขข้อบกพร่องจากการตรวจสอบด้าน IT ตามข้อ ๓. ที่เหมาะสมกับความเสี่ยงจากข้อบกพร่อง และติดตามความคืบหน้าในการดำเนินการตามแผนดังกล่าว
๕. การจัดทำและรายงานผลการตรวจสอบ	๕.๑ เสนอรายงานผลการตรวจสอบตามข้อ ๓. และแผนการปรับปรุงแก้ไขข้อบกพร่องต่อคณะกรรมการของผู้ประกอบธุรกิจ คณะกรรมการตรวจสอบของผู้ประกอบธุรกิจ หรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจเฉพาะกรณีเป็นสาขาของธนาคารพาณิชย์ต่างประเทศ โดยไม่ชักช้า

การดำเนินการ	รายละเอียดในการดำเนินการ
	๕.๒^๑ รายงานผลการตรวจสอบและแผนการปรับปรุงแก้ไขข้อบกพร่องที่ผ่านการพิจารณาจากคณะกรรมการของผู้ประกอบธุรกิจ คณะกรรมการตรวจสอบของผู้ประกอบธุรกิจ หรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจเฉพาะกรณีเป็นสาขาของธนาคารพาณิชย์ต่างประเทศ ตามข้อ ๕.๑ ต่อสำนักงาน ตามรูปแบบและวิธีการที่กำหนดไว้บนเว็บไซต์ของสำนักงาน ภายใน ๓ เดือน นับแต่วันสิ้นปีปฏิทินของปี ดำเนินการตรวจสอบตามข้อ ๓. เว้นแต่ในกรณีที่เป็นผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลที่มีหน้าที่ต้องรายงานผลการตรวจสอบตามประกาศคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ กร. ๑๙/๒๕๖๑ เรื่อง หลักเกณฑ์ เงื่อนไขและวิธีการประกอบธุรกิจสินทรัพย์ดิจิทัล ลงวันที่ ๓ กรกฎาคม พ.ศ. ๒๕๖๑ ให้ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลปฏิบัติตามประกาศดังกล่าว ๕.๓ จัดเก็บรายงานผลการตรวจสอบและแผนการปรับปรุงแก้ไขข้อบกพร่องเป็นระยะเวลาไม่น้อยกว่า ๒ ปี นับแต่วันที่จัดทำรายงานและแผนดังกล่าว โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้สำนักงานสามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า

^๑ เว้นแต่กรณีเป็นผู้ประกอบธุรกิจที่เป็นธนาคารพาณิชย์ตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน บริษัทประกันชีวิตตามกฎหมายว่าด้วยการประกันชีวิต หรือสถาบันการเงินที่จัดตั้งขึ้นตามกฎหมายอื่น ซึ่งได้รับใบอนุญาตประกอบธุรกิจหลักทรัพย์ดังนี้ โดยไม่ได้มีการประกอบธุรกิจหลักทรัพย์ประเภทอื่น โดยให้ได้รับยกเว้นการดำเนินการตามข้อ ๕.๒

๑. การเป็นนายหน้าซื้อขายหลักทรัพย์ การค้าหลักทรัพย์ และการจัดจำหน่ายขายหลักทรัพย์อันเป็นตราสารแห่งหนี้ หรือ
๒. กิจการการยืมและให้ยืมหลักทรัพย์