

## คำศัพท์

### ส่วนที่ 1 ขอบเขต

ให้ใช้คำอธิบายคำศัพท์ตามภาคผนวกนี้เพื่อประกอบการอธิบายคำย่อและความหมายของคำย่อ รวมถึงคำศัพท์ที่ปรากฏในภาคผนวกแนบท้ายประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ว่าด้วยข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ

### ส่วนที่ 2 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)

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

“การปฏิบัติงานจากเครือข่ายภายนอก” (teleworking)

การปฏิบัติงานที่มีการเข้าถึงระบบ IT ที่มีนัยสำคัญโดยไม่ผ่านการเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ภายในของผู้ประกอบธุรกิจโดยตรง

“ซอฟต์แวร์” (software)

ระบบหรือโปรแกรมคอมพิวเตอร์ดังนี้

(1) ซอฟต์แวร์ระบบ (system software) เช่น ระบบปฏิบัติการ หรือโปรแกรมตรวจจับไวรัส เป็นต้น

(2) 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)	บุคคลภายนอกที่มีความเกี่ยวข้องกับผู้ประกอบธุรกิจนี้ แต่ไม่รวมถึงลูกค้าที่ใช้บริการหรือผลิตภัณฑ์ของผู้ประกอบธุรกิจ <ol style="list-style-type: none"> <li>(1) ผู้ให้บริการงานด้าน IT</li> <li>(2) ผู้ที่มีการเชื่อมต่อกับระบบ IT ของผู้ประกอบธุรกิจ</li> <li>(3) ผู้ที่สามารถเข้าถึงข้อมูลสำคัญของผู้ประกอบธุรกิจหรือข้อมูลของลูกค้าที่อยู่ในรูปแบบอิเล็กทรอนิกส์และอยู่ภายใต้การควบคุมดูแลของผู้ประกอบธุรกิจ</li> </ol>
“แบบ RLA” (Risk Level Assessment)	แบบการประเมินระดับความเสี่ยงเกี่ยวกับระบบเทคโนโลยีสารสนเทศซึ่งส่งผลกระทบต่อการดำเนินธุรกิจของผู้ประกอบธุรกิจที่กำหนดไว้บนเว็บไซต์ของสำนักงาน
“ประกาศที่ สธ. 38/2565”	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)

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

“เหตุการณ์ผิดปกติ  
ด้าน IT” (IT incident)

เหตุการณ์ด้าน IT ที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) เช่น

- (1) ระบบ IT ของผู้ประกอบธุรกิจถูกบุกรุกหรือโจมตี
- (2) ความมั่นคงปลอดภัยด้าน IT ถูกคุกคาม
- (3) ระบบ IT หยุดชะงัก ไม่สามารถให้บริการได้ เป็นต้น

“เหตุการณ์ด้าน  
ความมั่นคงปลอดภัย  
ของระบบ IT  
อย่างมีนัยสำคัญ”

เหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ IT ที่เกิดขึ้นแล้วส่งผลกระทบดังนี้

- (1) ทำให้ระบบ IT หรือข้อมูลที่จัดเก็บ ประมวลผล หรือส่งต่อ สูญเสียคุณสมบัติด้านความถูกต้องครบถ้วน (integrity) สภาพพร้อมใช้งาน (availability) หรือการธำรงไว้ซึ่งความลับ (confidentiality) อย่างมีนัยสำคัญ หรือ
- (2) ทำให้เกิดการละเมิดหรือมีความเสี่ยงที่อาจทำให้เกิดการละเมิดต่อข้อกำหนดขององค์กรหรือกฎหมาย

เช่น

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

**คำศัพท์****คำอธิบายศัพท์**

	<ul style="list-style-type: none"> <li>- เหตุการณ์ข้อมูลสำคัญของผู้ประกอบการหรือข้อมูลส่วนบุคคลที่อยู่ภายใต้การควบคุมดูแลของผู้ประกอบการรั่วไหล (data breach) ซึ่งส่งผลกระทบต่ออย่างมีนัยสำคัญ</li> <li>- เหตุการณ์ insider threat ทั้งด้วยเจตนา และไม่เจตนา จนเป็นเหตุให้ทรัพย์สินหรือข้อมูลของลูกค้าเสียหายหรือสูญหาย</li> <li>- หน้าเว็บไซต์ของบริษัทโดนปลอมแปลง (website defacement) เป็นต้น</li> </ul>
“ฮาร์ดแวร์” (hardware)	อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย รวมถึงอุปกรณ์อื่น ๆ ที่เกี่ยวข้องกับระบบ IT ของผู้ประกอบการ
“IT”	เทคโนโลยีสารสนเทศ
“MFA”	การยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication)
“non-disclosure agreement”	ข้อตกลงในการไม่เปิดเผยข้อมูล
“privileged user”	ผู้ใช้งานที่ได้รับสิทธิในการใช้งานในระดับสูง