TNL

นโยบายบริษัท (Company Policy)

เรื่อง : แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Security Guidelines)

เลขที่เอกสาร : PC-TNL-IT-001

แนวปฏิบัติในการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ ฉบับนี้ ผ่านการอนุมัติ โดยมติที่ประชุมคณะกรรมการบริษัท ครั้งที่ 4/2569 เมื่อวันที่ 10 สิงหาคม 2569 ให้มีผลบังคับใช้ตั้งแต่วันที่ 10 สิงหาคม 2569 เป็นต้นไป

ผู้จัดทำ	ผู้สอบทาน	ผู้อนุมัติ
กิตติชัย สัจจา	ปฐมพงษ์ โพธิ์พงษ์	
(นายกิตติชัย สัจจา)	(นายปฐมพงษ์ โพธิ์พงษ์)	(นายกิตติชัย ตรีรัชตพงษ์)

สารบัญ

ส่วนที่ 1 บทนำ

ด้วยบริษัท ธนูลักษณ์ จำกัด (มหาชน) และบริษัทในกลุ่ม (รวมเรียกว่า **"บริษัท"**) ตระหนักถึงความสำคัญของระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทต่อการให้บริการกับกรรมการบริษัท ผู้บริหาร พนักงาน และรวมถึงบุคคลภายนอกซึ่งได้รับอนุญาต ดังนั้น เพื่อให้การดำเนินธุรกรรมด้วยวิธีการทางอิเล็กทรอนิกส์ การปฏิบัติงานและบริหารงาน ได้อย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยเชื่อถือได้ และสามารถดำเนินงานได้อย่างต่อเนื่อง บริษัทจึงได้จัดทำนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และแนวในปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เพื่อเป็นแนวทางในการใช้งานเทคโนโลยีสารสนเทศ

ส่วนที่ 2 วัตถุประสงค์

1. เพื่อให้การดำเนินงานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทมีความมั่นคงปลอดภัย สามารถใช้งานได้อย่างต่อเนื่องและมีประสิทธิภาพ อันจะทำให้การดำเนินธุรกรรมมีความถูกต้อง เชื่อถือได้ตามมาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์
2. เพื่อกำหนดแนวทางปฏิบัติให้ผู้บริหาร ผู้ดูแลระบบ และเจ้าหน้าที่ผู้ใช้งานระบบ ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท
3. เพื่อป้องกันเจ้าหน้าที่ผู้ใช้งานและผู้เกี่ยวข้องไม่ให้กระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และกฎหมายอื่น ๆ ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

ส่วนที่ 3 คำนิยาม

คำนิยามที่ใช้ในแนวปฏิบัตินี้ ประกอบด้วย

"บริษัท"	หมายถึง	1. บริษัท ธนูลักษณ์ จำกัด (มหาชน) 2. บริษัท ออกซิเจน แอสเซ็ท จำกัด 3. บริษัท บริหารสินทรัพย์ ออกซิเจน จำกัด 4. บริษัท ทีเอ็นแอล อัลไลแอนซ์ จำกัด 5. บริษัท ออกซิเจน แอดไวเซอรี่ จำกัด รวมถึงนิติบุคคลอื่นที่บริษัทในกลุ่มดังกล่าวมีความสัมพันธ์กันในลักษณะเป็นผู้ถือหุ้นหรือเป็นหุ้นส่วนที่มีส่วนร่วมในการตัดสินใจเกี่ยวกับนโยบายการดำเนินงานในอีกนิติบุคคลหนึ่ง
"ผู้ใช้งาน"	หมายถึง	บุคคลที่ได้รับอนุญาตให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท โดยมีสิทธิและหน้าที่ตามที่บริษัทกำหนด
"ผู้บริหาร"	หมายถึง	ผู้บริหารบริษัท

“ผู้ดูแลระบบ”	หมายถึง	ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ หรือผู้ได้รับมอบหมายให้ควบคุมดูแลบริหารจัดการระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท
“สินทรัพย์”	หมายถึง	ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท เช่น คอมพิวเตอร์ อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่บริษัทซื้อมาเพื่อใช้งานอย่างถูกต้องตามกฎหมาย เป็นต้น
“การควบคุมการใช้งานสารสนเทศ”	หมายถึง	การควบคุมและจำกัดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท ที่เกี่ยวกับการให้บริการและข้อมูลตามความจำเป็นในการใช้งาน มีการป้องกันการลักลอบการเข้าถึงระบบโดยผู้ที่ไม่มีสิทธิทั้งจากภายในและภายนอกบริษัท
“ความมั่นคงปลอดภัยด้านสารสนเทศ”	หมายถึง	การคงไว้ซึ่งความลับ ความถูกต้องสมบูรณ์ และความพร้อมใช้งานของข้อมูลในระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท
“เหตุการณ์ด้านความมั่นคงปลอดภัย”	หมายถึง	เหตุการณ์ที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท หรือเหตุการณ์ที่สงสัยว่าจะเป็นจุดอ่อน หรือสร้างความเสียหายได้ในที่สุด ซึ่งส่งผลให้เป็นการละเมิดนโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัท เช่น การอนุญาตให้ผู้อื่นเข้าใช้งานระบบ การไม่กำหนดรหัสผ่านในการเข้าใช้งานระบบ การเปิดเผยเอกสารสำคัญให้บุคคลภายนอกล่วงรู้ โปรแกรมไม่พึงประสงค์ระบบถูกบุกรุกทางเครือข่าย หรือการเปิดเผยข้อมูลสำคัญโดยไม่ได้รับอนุญาต
“สถานการณ์ที่ไม่พึงประสงค์”	หมายถึง	สถานการณ์ที่ผู้ดูแลระบบไม่ต้องการให้เกิดขึ้นหรือสร้างความเสียหายกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท โดยผู้ดูแลระบบไม่ได้คาดการณ์ไว้ว่าจะเกิดขึ้น เช่น โปรแกรมไม่พึงประสงค์ โปรแกรมทำงานผิดพลาดหรือไม่ถูกต้อง ระบบถูกบุกรุกทางเครือข่าย ข้อมูลสำคัญถูกเปลี่ยนแปลงหรือสูญหาย หน้าเว็บไซต์ถูกเปลี่ยนแปลง การเปิดเผยข้อมูลสำคัญโดยไม่ได้รับอนุญาต ระบบถูกโจมตีจนไม่สามารถให้บริการได้ การหยุดชะงักของระบบคอมพิวเตอร์และเครือข่าย หรือเหตุการณ์อื่น ๆ ที่เป็นการละเมิดนโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ
“ฝ่ายเทคโนโลยีสารสนเทศ”	หมายถึง	หน่วยงาน และ/หรือ ผู้รับผิดชอบที่มีหน้าที่ดำเนินการเกี่ยวกับระบบเทคโนโลยีสารสนเทศและระบบงานคอมพิวเตอร์ เป็นศูนย์กลางเครือข่ายข้อมูลสารสนเทศของบริษัทในการศึกษาวิเคราะห์เพื่อพัฒนาระบบเทคโนโลยีสารสนเทศและระบบงานคอมพิวเตอร์ของบริษัทและปฏิบัติงานร่วมกันหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้อง
“ข้อมูลคอมพิวเตอร์”	หมายถึง	ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

“ศูนย์สารสนเทศ”	หมายถึง	ห้องเครื่องแม่ข่าย (Server Room) ห้องเครือข่าย (Network Room)
“ระบบคอมพิวเตอร์”	หมายถึง	อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
“ระบบเครือข่ายสื่อสาร”	หมายถึง	ระบบที่สามารถใช้ในการติดต่อสื่อสาร การเชื่อมโยง หรือการส่งข้อมูลสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของบริษัท ซึ่งการเชื่อมโยงเป็นได้ทั้งในรูปแบบใช้สายและแบบไร้สาย โดยระบบเครือข่ายสื่อสาร ได้แก่ ระบบเครือข่ายระยะใกล้ (Local Area Network: LAN) ระบบเครือข่ายระยะไกล (Wide Area Network: WAN) และระบบอินเทอร์เน็ต (Internet)
“ระบบเครือข่ายสื่อสารระยะใกล้”	หมายถึง	เครือข่ายที่เชื่อมโยงกันในพื้นที่ใกล้เคียงกัน
“ระบบเครือข่ายสื่อสารระยะไกล”	หมายถึง	เครือข่ายเชื่อมโยงกันในระยะทางที่ห่างไกล
“ระบบอินเทอร์เน็ต”	หมายถึง	ระบบเครือข่ายสื่อสารที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ของบริษัท เข้ากับระบบเครือข่ายสื่อสารอินเทอร์เน็ตทั่วโลก
“สารสนเทศ”	หมายถึง	ข้อมูลที่ผ่านการประมวลผลการจัดระเบียบ ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ
“ระบบเทคโนโลยีสารสนเทศและการสื่อสาร”	หมายถึง	ระบบงานของบริษัท ที่ประกอบด้วย ระบบคอมพิวเตอร์ ระบบฐานข้อมูล ระบบเครือข่ายสื่อสาร เจ้าหน้าที่ผู้ใช้ระบบ เจ้าหน้าที่ผู้พัฒนาระบบ เจ้าหน้าที่ผู้จัดการดูแลระบบ และผู้บริหารของบริษัท นำมาทำงานร่วมกัน เพื่อกำหนดวัตถุประสงค์ รวบรวมจัดเก็บขอมูล ประมวลผลข้อมูล และส่งผลลัพธ์หรือสารสนเทศที่ได้ให้ผู้ใช้ระบบและผู้บริหารของบริษัทสามารถนำมาใช้ประโยชน์ในการวางแผน เพื่อช่วยสนับสนุนการปฏิบัติงาน การตัดสินใจ การบริหาร การวิเคราะห์ และติดตามผลการดำเนินงานของหน่วยงานระดับต่าง ๆ ของบริษัท
“รหัสผ่าน” (Password)	หมายถึง	ตัวอักษร อักขระ หรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศและการสื่อสาร
“การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ”	หมายถึง	การดำเนินการรักษาความมั่นคง ปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท ประกอบด้วย คุณสมบัติพื้นฐาน 3 ประการ ได้แก่ การรักษาความลับ บูรณภาพ และความพร้อมใช้งาน
“การรักษาความลับ” (Confidentiality)	หมายถึง	การเก็บรักษาข้อมูลไว้เป็นความลับและจะมีเพียงผู้มีสิทธิเท่านั้นที่จะสามารถเข้าถึงข้อมูลเหล่านั้นได้

“บูรณภาพ” (Integrity)	หมายถึง	การรับรองว่าข้อมูลจะไม่ถูกกระทำการใด ๆ อันมีผลให้เกิดการเปลี่ยนแปลงหรือแก้ไขจากผู้ซึ่งไม่มีสิทธิไม่ว่าการกระทำนั้นจะมีเจตนาหรือไม่ก็ตาม
“ความพร้อมใช้งาน” (Availability)	หมายถึง	การรับรองได้ว่าข้อมูลหรือระบบเทคโนโลยีสารสนเทศและการสื่อสารทั้งหลายพร้อมที่จะให้บริการในเวลาที่ต้องการใช้งาน
“ชุดคำสั่งไม่พึงประสงค์” (Malware)	หมายถึง	ชุดคำสั่งที่มีผลทำให้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร เกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
“จดหมายอิเล็กทรอนิกส์” (E-mail)	หมายถึง	ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายสื่อสารที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ เช่น SMTP, POP3 หรือ IMAP
“ผู้ใช้งานที่มีสิทธิการเข้าถึงระดับสูงสุด”	หมายถึง	ผู้ใช้งานระบบ (หรือบัญชีผู้ใช้) ที่มีสิทธิการเข้าถึงระดับสูงสุดภายในระบบเทคโนโลยีสารสนเทศ เครือข่าย หรือแอปพลิเคชันหนึ่ง ๆ ซึ่งสามารถกระทำการสำคัญที่มีผลกระทบอย่างมากต่อความมั่นคง ความพร้อมใช้งาน และความลับของระบบได้
“ปัญญาประดิษฐ์” (AI)	หมายถึง	เทคโนโลยีที่สามารถจำลองกระบวนการคิดของมนุษย์ เช่น การเรียนรู้ การตัดสินใจ การสร้างเนื้อหา เป็นต้น
“เครื่องมือ AI สาธารณะ”	หมายถึง	ระบบ AI ที่เปิดให้บุคคลทั่วไปใช้งาน เช่น ChatGPT, Google Gemini, Claude, Perplexity, Copilot เป็นต้น
“ข้อมูลอ่อนไหว” (Sensitive Data)	หมายถึง	ข้อมูลที่เป็นความลับทางธุรกิจ ข้อมูลลูกค้า ข้อมูลส่วนบุคคล ฯลฯ
“ข้อมูลส่วนบุคคลที่สามารถระบุตัวตนได้” (PII)	หมายถึง	ข้อมูลที่ใช้ระบุตัวบุคคลใดบุคคลหนึ่งได้ ซึ่งรวมถึงข้อมูลที่สามารถระบุตัวบุคคลได้ไม่ว่าจะใช้เพียงข้อมูลเดียวหรือเมื่อใช้ร่วมกับข้อมูลอื่น ตัวอย่าง : ชื่อ ที่อยู่ หมายเลขโทรศัพท์ ที่อยู่อีเมล หมายเลขประกันสังคม หมายเลขหนังสือเดินทาง หมายเลขใบขับขี่ บัตรประจำตัวที่ออกโดยรัฐบาล (หมายเลขประจำตัวผู้เสียภาษี) วันเกิด เชื้อชาติ สถานที่เกิด เป็นต้น
“การประเมินความเสี่ยง” (Risk Assessment)	หมายถึง	กระบวนการวิเคราะห์ ตรวจสอบ และประเมินความเสี่ยงที่อาจเกิดขึ้นกับระบบ ICT ของบริษัท เช่น ความเสี่ยงจากการโจมตีทางไซเบอร์ ความล้มเหลวของระบบเครือข่าย การรั่วไหลของข้อมูล หรือการหยุดชะงักของบริการทางไอที เพื่อหาแนวทางในการจัดการและลดผลกระทบที่อาจเกิดขึ้น

ส่วนที่ 4 โครงสร้างด้านความปลอดภัยเทคโนโลยีสารสนเทศ

เพื่อให้มีการกำหนดกรอบการบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศของบริษัทตั้งแต่เริ่มต้น รวมถึงการควบคุมการปฏิบัติงานเพื่อให้มีความมั่นคงปลอดภัย บริษัทจึงได้กำหนดผู้เกี่ยวข้องและหน้าที่ในการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศของบริษัท ดังนี้

4.1 ฝ่ายเทคโนโลยีสารสนเทศ

1) กำหนดแผน เป้าหมาย และระเบียบปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัท โดยครอบคลุมถึงงบประมาณและจำนวนบุคลากรให้สอดคล้องกับแผนกลยุทธ์ของบริษัท
2) ระเบียบปฏิบัติที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ซึ่งหมายรวมถึงนโยบาย มาตรฐาน แนวปฏิบัติ และคู่มือเพื่อการดำเนินงานการรักษาความลับของข้อมูล (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และความมั่นคงของระบบ (Availability)
3) การบริหารความเสี่ยงและการวิเคราะห์ความเสี่ยงที่อาจทำให้ระบบเกิดปัญหา กระทบกับการดำเนินธุรกิจของบริษัท
4) มีการกำกับดูแลระบบเทคโนโลยีสารสนเทศที่มั่นใจได้ว่ามาตรการที่วางไว้สามารถดำเนินการได้อย่างมีประสิทธิภาพ และมีการบริหารเฝ้าระวังการโจมตีระบบและภัยต่าง ๆ ที่อาจเกิดขึ้นกับระบบ รวมทั้งวางแผนบริหารความต่อเนื่องทางธุรกิจเพื่อกู้ระบบยามฉุกเฉิน
5) เตรียมพร้อมรับสถานการณ์และเรียนรู้เทคนิคใหม่ ๆ ทางด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ
6) ประเมินความต้องการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศ ความคุ้มค่า รวมทั้งจัดหาและพัฒนาระบบเทคโนโลยีสารสนเทศให้สอดคล้องกับกลยุทธ์ของบริษัท
7) ดูแลทรัพยากรด้านเทคโนโลยีสารสนเทศของบริษัท ให้สามารถสนับสนุนการปฏิบัติงานภายในอย่างมีประสิทธิภาพ

4.2 พนักงานทุกคนของบริษัท

1) ปฏิบัติตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างเคร่งครัด
2) รักษาความลับของข้อมูลสารสนเทศของบริษัท และไม่เปิดเผยรหัสผ่านเข้าใช้ระบบของตนเอง
3) รายงานเหตุการณ์ละเมิดความปลอดภัยสารสนเทศ และปัญหาทางด้านความปลอดภัย เมื่อเกิดเหตุการณ์ดังกล่าวให้กับฝ่ายเทคโนโลยีสารสนเทศทราบ
4) ใช้งานข้อมูลและทรัพย์สินทางข้อมูลของบริษัทอย่างรับผิดชอบ และใช้ข้อมูลสำหรับงานที่ตนเองรับผิดชอบหรือได้รับอนุญาตเท่านั้น

4.3 หน่วยงานหรือบุคคลภายนอกที่เข้ามาปฏิบัติงานในบริษัท หรือทำงานให้กับบริษัท

1) ปฏิบัติตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างเคร่งครัด
2) รักษาความลับของข้อมูลสารสนเทศของบริษัท และไม่เปิดเผยรหัสผ่านเข้าใช้ระบบของตนเอง
3) รายงานเหตุการณ์ละเมิดความปลอดภัยสารสนเทศ และปัญหาทางด้านความปลอดภัย เมื่อเกิดเหตุการณ์ดังกล่าวให้กับฝ่ายเทคโนโลยีสารสนเทศทราบ

4) ใช้งานข้อมูลและทรัพย์สินทางข้อมูลของบริษัทอย่างรับผิดชอบ และใช้ข้อมูลสำหรับงานที่ตนเองรับผิดชอบหรือได้รับอนุญาตเท่านั้น

ส่วนที่ 5 แนวปฏิบัติในการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศบริษัท

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทมี 11 หมวด ดังนี้

หมวดที่ 1 การเข้าถึงและการควบคุมการใช้งานสารสนเทศและระบบเทคโนโลยีสารสนเทศและการสื่อสาร

เพื่อป้องกันไม่ให้บุคคลที่ไม่ได้รับอนุญาตเข้าถึงข้อมูล ระบบ หรือทรัพยากรทางเทคโนโลยี ซึ่งครอบคลุมทั้งด้านเทคนิคและการบริหารจัดการ ดังนี้

1.1 การควบคุมการเข้าถึงสิทธิของผู้ใช้งาน

1) มีการกำหนดสิทธิของผู้ใช้งานในการเข้าถึงระบบ โดยพิจารณาจากหน้าที่ความรับผิดชอบในการเข้าถึงและการใช้งานข้อมูลของผู้ใช้งานแต่ละกลุ่มงาน
2) ผู้ดูแลระบบจะกำหนดสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารนั้น ๆ ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้งาน และหน้าที่ความรับผิดชอบของผู้ใช้งานเป็นไปตามระเบียบที่บริษัท กำหนด และทบทวนสิทธิอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง หรือในกรณีฝ่ายทรัพยากรบุคคลมีการแจ้งย้าย เปลี่ยนตำแหน่งงานใหม่ ออกจากงาน เกษียณ หรือในกรณีที่หน่วยงานต้นสังกัด ยื่นทำขอต่อฝ่ายเทคโนโลยีสารสนเทศเพื่อให้มีสิทธิหรือยกเลิกสิทธิต่าง ๆ ในการใช้งานอนุญาต
3) ผู้ดูแลระบบจะกำหนดสิทธิบัญชีรายชื่อผู้ใช้งานรายใหม่และรหัสผ่านสำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร และยกเลิกสิทธิของผู้ใช้งานเมื่อมีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบ เมื่อสิ้นสุดการเป็นพนักงาน หรือสิ้นสุดสัญญาว่าจ้างบุคคลภายนอก
4) กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งาน ต้องมีการพิจารณาการควบคุมผู้ใช้งานที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอ เช่น กำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว และมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัดทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานจะต้องเปลี่ยนรหัสผ่านทุก 3 เดือน และต้องได้รับความเห็นชอบและอนุมัติจากผู้ดูแลระบบหรือผู้ได้รับมอบหมาย
5) ห้ามผู้ใช้งานซึ่งไม่ได้รับสิทธิให้เข้าใช้งานบุกรุกเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารไม่ว่าด้วยวิธีการใด

1.2 การใช้งานรหัสผ่านสำหรับผู้ใช้งาน

1) ผู้ใช้งานจะต้องใช้ชื่อผู้ใช้งานและรหัสผ่านของตนเองในการใช้งานระบบ เพื่อป้องกันการปฏิเสธความรับผิดชอบ
2) ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรกหรือได้รับรหัสผ่านใหม่ จะต้องเปลี่ยนรหัสผ่านที่ได้รับโดยทันที

3) ผู้ใช้งานต้องกำหนดรหัสผ่านและเปลี่ยนรหัสผ่านของตนเองในการใช้งานอย่างน้อยทุก ๆ 90 วัน หรือตามหลักเกณฑ์ซึ่งผู้ดูแลระบบกำหนด และต้องยินยอมให้ผู้ดูแลระบบดำเนินการใด ๆ เพื่อให้เกิดความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร
4) ผู้ใช้งานต้องเก็บรักษารหัสผ่านให้เป็นความลับ ระมัดระวังป้องกันรหัสผ่านของตนเองในการใช้งานไม่ให้รั่วไหลไปยังผู้อื่น และไม่มอบให้ผู้อื่นนำไปใช้ไม่ว่าด้วยเหตุใด ๆ ทั้งสิ้น เว้นแต่กรณีผู้ใช้งานที่มีอำนาจอนุมัติใด ๆ ในระบบเทคโนโลยีสารสนเทศและการสื่อสารไม่สามารถปฏิบัติงาน อันจะเป็นเหตุให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารไม่สามารถดำเนินการต่อไปได้ ให้แต่งตั้งผู้ปฏิบัติงานแทนในช่วงเวลาดังกล่าว เพื่อใช้เป็นหลักฐานในการตรวจสอบการใช้สิทธิ และหลังจากผู้ปฏิบัติงานแทนดำเนินการเรียบร้อยแล้ว ให้ผู้ใช้งานซึ่งเป็นเจ้าของรหัสผ่านทำการเปลี่ยนรหัสผ่านโดยทันที
5) กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ 8 ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน
6) ไม่กำหนดรหัสผ่านอย่างเป็นแบบแผน เช่น “abcdef” “aaaaaa” “123456”
7) ไม่กำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน เช่น ชื่อ-สกุล วัน เดือน ปีเกิด ที่อยู่
8) ไม่กำหนดรหัสผ่านเป็นคำศัพท์ที่อยู่ในพจนานุกรม
9) ผู้ใช้งานต้องออกจากระบบ (Log Off) ทันทีเมื่อไม่ใช้งาน เพื่อป้องกันผู้ใช้งานอื่นลักลอบใช้สิทธิในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร
10) การแจ้งปัญหาการใช้งานชื่อผู้ใช้งานและรหัสผ่าน ให้ผู้ใช้งานติดต่อผู้ดูแลระบบ เช่น ลืมชื่อผู้ใช้งานหรือรหัสผ่าน เป็นต้น

1.3 การบริหารจัดการการเข้าถึงของผู้ใช้งาน

1) กรณีผู้ใช้งานต้องการเข้าถึงระบบงานใดนอกเหนือจากระบบที่ฝ่ายงานของตนมีสิทธิเข้าถึง จะต้องทำคำขอและได้รับอนุมัติจากผู้บังคับบัญชาของเจ้าของระบบงานดังกล่าวก่อน
2) เจ้าของระบบงานจะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่เกี่ยวข้องกับหน้าที่และความรับผิดชอบเท่านั้น
3) ผู้ดูแลระบบมีหน้าที่ในการตรวจสอบการอนุมัติ และกำหนดสิทธิในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้งานในการขออนุญาตเข้าระบบงานนั้น พร้อมทั้งต้องเก็บบันทึกข้อมูลคำขอไว้เป็นหลักฐานประกอบการตรวจสอบ
4) การเพิ่ม เปลี่ยน หรือยกเลิกสิทธิการเข้าถึง ต้องดำเนินการผ่านขั้นตอนที่กำหนด (เช่น การร้องขอผ่านแบบฟอร์ม หรือ E-Mail เป็นต้น)
5) การจัดเก็บรักษาชื่อผู้ใช้และรหัสผ่านบัญชีผู้ใช้งานที่มีสิทธิสูงสุด (Highest Privilege Users)
    (1) ผู้ดูแลระบบจัดเก็บชื่อผู้ใช้และรหัสผ่านในซองปิดผนึกในที่ปลอดภัย
    (2) ผู้ดูแลระบบทำการบันทึกประวัติการเปิดซองทุกครั้ง
    (3) ซองชื่อผู้ใช้และรหัสผ่านจะถูกเปิดใช้งานได้ในกรณีฉุกเฉินเท่านั้น

(4) ผู้ดูแลระบบจะต้องมีการตรวจสอบบัญชีผู้ใช้งานที่มีสิทธิสูงสุดอย่างสม่ำเสมอ เพื่อตรวจสอบบัญชีผู้ใช้งานที่มีสิทธิสูงสุดให้สามารถเข้าใช้งานได้ตามปกติ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลง

1.4 การควบคุมการเข้าถึงระบบเครือข่ายสื่อสาร

เป็นการควบคุมบุคคลที่เข้าสู่ระบบเครือข่ายสื่อสาร รวมถึงการควบคุมป้องกันการบุกรุกได้อย่างเป็นระบบ และให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น โดยผู้ดูแลระบบจะต้องทำการออกแบบระบบเครือข่ายสื่อสารตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีการใช้งาน กลุ่มของผู้ใช้งาน และกลุ่มของระบบเทคโนโลยีสารสนเทศ ได้แก่ Internal Zone, External Zone และ DMZ Zone เป็นต้น จึงต้องมีการกำหนดมาตรการรักษาความปลอดภัย ดังนี้

1) ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบเทคโนโลยีสารสนเทศได้เท่าที่ได้รับอนุญาตให้เข้าถึงเท่านั้น
2) เจ้าหน้าที่ผู้รับผิดชอบต้องทำการลงทะเบียนอุปกรณ์ทุกเครื่องที่ใช้ติดต่อระบบเครือข่ายสื่อสารในระบบจัดการทรัพย์สินสารสนเทศของบริษัท
3) ผู้ดูแลระบบต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายสื่อสารในส่วนที่เกี่ยวข้องกับหน้าที่และความรับผิดชอบของผู้ใช้งานในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายสื่อสาร
4) ผู้ดูแลระบบจัดให้มีซอฟต์แวร์สำหรับบริหารจัดการและควบคุมระบบเครือข่าย (Network Management System) ซึ่งสามารถระบุอุปกรณ์บนเครือข่าย (Equipment Identification) ถึงระดับ IP Address, Computer name, MAC Address และสามารถสร้างผังการเชื่อมโยงเครือข่าย (Network Diagram)
5) ผู้ดูแลระบบมีการจัดทำผังการเชื่อมโยงเครือข่าย และมีการปรับปรุงให้เป็นปัจจุบันอยู่เสมอ
6) ผู้ดูแลระบบมีการบริหารจัดการเครือข่ายสื่อสาร ดังนี้
   (1) มีการแบ่งแยกเครือข่ายสื่อสารเป็น เครือข่ายสื่อสารภายใน เครือข่ายสื่อสารภายนอก และเครือข่ายสื่อสารแบบไร้สาย
   (2) มีการจัดแบ่งแยกส่วนเครือข่ายสื่อสาร/กลุ่ม เพื่อป้องกันและควบคุมการเข้าถึง ได้แก่ ส่วนที่เป็นสาธารณะ ส่วนที่เชื่อมต่อภายใน ส่วนที่เกี่ยวข้องกับสินทรัพย์สำคัญหรือที่เป็นอันตราย กลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบเทคโนโลยีสารสนเทศ
   (3) มีการติดตั้งอุปกรณ์ Gateway กั้นไว้ระหว่างเครือข่ายสื่อสาร เพื่อเป็นตัวควบคุมข้อมูลที่สื่อสารกันระหว่างเครือข่ายสื่อสาร
   (4) อุปกรณ์ในเครือข่ายสื่อสารมีการปรับแต่งให้สามารถควบคุมหรือกรองข้อมูลที่สื่อสารกันระหว่างเครือข่าย
7) ผู้ดูแลระบบมีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายอื่น ๆ ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ สามารถตรวจสอบได้อย่างน้อย 1 ปี
8) ผู้ดูแลระบบมีการสำรองข้อมูลการตั้งค่าของอุปกรณ์เครือข่ายสื่อสาร

1.5 การควบคุมการเข้าถึงระบบปฏิบัติการ

เป็นการควบคุมบุคคลเข้าสู่ระบบปฏิบัติการที่อยู่ภายใต้ระบบเครือข่ายสื่อสารของบริษัท เพื่อรักษาความปลอดภัยของข้อมูลและทรัพยากร จึงต้องมีการกำหนดมาตรการรักษาความปลอดภัย

1) การติดตั้งโปรแกรมอรรถประโยชน์ (Utility Program/Software) เพื่อใช้งานร่วมกับระบบปฏิบัติการ
   (1) ต้องไม่ติดตั้งโปรแกรมซอฟต์แวร์ที่ละเมิดลิขสิทธิ์
   (2) ต้องติดตั้งโปรแกรมตามภารกิจและไม่ติดตั้งโปรแกรมที่ไม่เกี่ยวข้องกับการปฏิบัติงาน
   (3) ต้องติดโปรแกรมตามที่ฝ่ายเทคโนโลยีสารสนเทศกำหนดเท่านั้น
2) ฝ่ายเทคโนโลยีสารสนเทศกำหนดมาตรการจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Limitation of Connection Time) สำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรือแอปพลิเคชัน (Application) ที่มีความเสี่ยงหรือมีความสำคัญสูงเพื่อให้มีความมั่นคงปลอดภัย โดยผู้ใช้งานสามารถใช้งานได้นานที่สุด 30 นาทีต่อการเชื่อมต่อ 1 ครั้ง เฉพาะในช่วงเวลาทำการของฝ่ายเท่านั้น

1.6 การเข้ารหัสข้อมูล (Cryptography)

เพื่อให้มีการเข้ารหัสข้อมูลอย่างเหมาะสมและได้ผล และเพื่อป้องการความลับ การปลอมแปลง หรือความถูกต้องของสารสนเทศ

1) บริษัทต้องจัดให้มีการควบคุมการใช้งานระบบการเข้ารหัสข้อมูลที่คำนึงถึงชนิด และขั้นตอนวิธีการเข้ารหัสข้อมูล (Algorithm) สอดคล้องเหมาะสมกับระดับความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลที่เป็นความลับหรือมีความสำคัญ รวมทั้งกำหนดผู้รับผิดชอบในการดำเนินนโยบายและบริหารจัดการกุญแจเพื่อการเข้ารหัสข้อมูล (Key Management)
2) บริษัทต้องจัดให้มีการบริหารกุญแจเพื่อการเข้ารหัสข้อมูลตลอดช่วงเวลาการใช้งาน (Key Management Whole Life Cycle) โดยกำหนดแนวปฏิบัติเพื่อการคัดเลือกวิธีการเข้ารหัส การกำหนดความยาวของรหัส การใช้งานและการยกเลิกการใช้งานกุญแจเพื่อการเข้ารหัส กระบวนการบริหารจัดการกุญแจเพื่อการเข้ารหัส รวมทั้งติดตามให้มีการปฏิบัติให้เป็นไปตามนโยบายและแนวทางปฏิบัติดังกล่าวอย่างสม่ำเสมอ

1.7 การยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication)

1) ต้องกำหนดให้มีการยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication - MFA) สำหรับผู้ใช้งานที่มีบัญชีสิทธิสูงสุด (Highest Privilege/Administrator)
2) ต้องกำหนดให้มีการยืนยันตัวตนแบบหลายปัจจัยสำหรับระบบเทคโนโลยีสารสนเทศที่มีความเสี่ยงสูงหรือมีความสำคัญต่อธุรกิจ
3) รูปแบบของปัจจัยที่สองให้เป็นไปตามที่ฝ่ายเทคโนโลยีสารสนเทศกำหนด เช่น One-Time Password (OTP), Authenticator Application หรือ Hardware/Software Token

หมวดที่ 2 การควบคุมการเข้า-ออก ศูนย์สารสนเทศ

การบริหารจัดการศูนย์สารสนเทศ (Data Center Management) โดยเฉพาะในด้านการควบคุมการเข้า-ออก (Physical Entry Controls) มีความสำคัญอย่างมากต่อการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศของบริษัท โดยสามารถจัดทำในรูปแบบแนวปฏิบัติ (Best Practices) ดังนี้

1. การเข้าใช้งานศูนย์สารสนเทศและพื้นที่สำคัญภายในศูนย์สารสนเทศต้องดำเนินการโดยการขออนุญาตล่วงหน้าผ่านการแจ้งผู้บังคับบัญชา และ/หรือ ผู้ดูแลศูนย์สารสนเทศด้วยช่องทางที่บริษัทกำหนด (เช่น อีเมลล์หรือช่องทางการสื่อสารภายในองค์กร) โดยต้องระบุเหตุผล วัตถุประสงค์ วันและเวลาที่ต้องการเข้าใช้งานอย่างชัดเจน และต้องได้รับการอนุมัติก่อนทุกครั้งจึงจะสามารถเข้าพื้นที่ได้
2. มีการบันทึกวันและเวลาการเข้า-ออกพื้นที่ในศูนย์สารสนเทศเกี่ยวกับตัวบุคคลและเวลาที่ผ่านเข้า-ออก เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น
3. มีการควบคุมการเข้าออกศูนย์สารสนเทศ และพื้นที่สำคัญภายในศูนย์สารสนเทศด้วยการใช้การสแกนใบหน้า (Face Scan) เพื่อพิสูจน์ตัวตนของผู้มีสิทธิ
4. มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานในศูนย์สารสนเทศ จนกระทั่งเสร็จสิ้นภารกิจ เพื่อป้องกันการสูญหายของทรัพย์สิน หรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต
5. ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญในศูนย์สารสนเทศ

หมวดที่ 3 การใช้งานเครื่องคอมพิวเตอร์

การรักษาความมั่นคงปลอดภัยในการใช้งานเครื่องคอมพิวเตอร์เป็นส่วนสำคัญของการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในบริษัท โดยมีแนวปฏิบัติที่ควรดำเนินการ ดังนี้

3.1 การใช้งานของผู้ใช้งาน

1) ให้มีการกำหนดรหัสผ่าน เปลี่ยนรหัสผ่านและเก็บรักษารหัสผ่าน เป็นไปตามหมวดที่ 1.2 การใช้งานรหัสผ่านสำหรับผู้ใช้งาน
2) ให้ผู้ใช้งานล็อคหน้าจอ หรือออกจากระบบ (Log Off) ทันทีเมื่อไม่อยู่ที่โต๊ะ หรือในกรณีที่ไม่ใช้ระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันบุคคลอื่นมาใช้ระบบต่อเนื่อง และหากสงสัยว่ารหัสผ่านเกิดการรั่วไหล ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันที
3) ผู้ไม่ได้รับสิทธิให้เข้าใช้งานระบบเทคโนโลยีสารสนเทศใด ห้ามเข้าใช้งานระบบเทคโนโลยีสารสนเทศดังกล่าวไม่ว่าด้วยวิธีการใด ๆ
4) ห้ามติดตั้งซอฟต์แวร์ หรือโปรแกรมอื่นใดลงบนเครื่องคอมพิวเตอร์ที่ใช้ปฏิบัติงาน หรือติดตั้งอุปกรณ์เชื่อมโยงเครือข่ายเพิ่มเติม หรือเชื่อมโยงเครือข่ายคอมพิวเตอร์ที่ใช้ปฏิบัติงานกับเครือข่ายอื่นนอกจากเครือข่ายของบริษัท หรือนำเครื่องคอมพิวเตอร์ส่วนตัวมาใช้งานกับระบบเทคโนโลยีสารสนเทศ เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ
5) ไม่เปิดให้มีการแชร์ไฟล์ในเครื่องคอมพิวเตอร์ที่ใช้ปฏิบัติงาน เว้นแต่ในกรณีที่เป็นระบบงานที่บริษัทกำหนดไว้ หากมีความจำเป็นให้กำหนดระยะเวลาเท่าที่ใช้งานและยกเลิกการแชร์ไฟล์ทันทีที่ใช้งานเสร็จ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบคอมพิวเตอร์และข้อมูล

6) ไม่ดาวน์โหลด (Download) ข้อมูลหรือโปรแกรมที่ไม่เกี่ยวข้องกับการปฏิบัติงาน หรือจากเว็บไซต์ซึ่งไม่น่าเชื่อถือหรือไม่มั่นใจว่าจะปลอดภัย

หมวดที่ 4 การใช้งานอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์

การรักษาความมั่นคงปลอดภัยในการใช้งานอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์ (Internet & Email Security) เป็นเรื่องสำคัญมาก เนื่องจากเป็นช่องทางหลักที่ผู้ไม่ประสงค์ดีใช้โจมตีและหลอกลวงผู้ใช้งาน โดยสามารถแบ่งแนวปฏิบัติได้ ดังนี้

4.1 การใช้งานอินเทอร์เน็ต

1) ผู้ใช้งานต้องไม่ใช้ระบบอินเทอร์เน็ตในการใช้งานข้อมูลมัลติมีเดีย หรือดาวน์โหลดข้อมูลที่ไม่เกี่ยวกับการปฏิบัติงานและยึดครองช่องสัญญาณการสื่อสารข้อมูล
2) ให้ผู้ดูแลระบบ กำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์ เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัย เช่น Proxy, Firewall, IPS, IDS, IPS, Anti-Virus เป็นต้น
3) เครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์แบบพกพา และอุปกรณ์คอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่อระบบอินเทอร์เน็ตผ่านเว็บบราวเซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการปิดช่องโหว่ของระบบปฏิบัติการที่เว็บบราวเซอร์ติดตั้งอยู่
4) ผู้ใช้งานต้องไม่ใช้งานอินเทอร์เน็ตของบริษัทเพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว หรือการเข้าใช้เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม
5) ผู้ใช้งานจะถูกกำหนดสิทธิในการเข้าถึงระบบเทคโนโลยีสารสนเทศ และแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของบริษัท โดยผ่านความเห็นชอบจากผู้ดูแลระบบ
6) ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของบริษัท ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต
7) ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ตต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา
8) ผู้ใช้งานต้องปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ อย่างเคร่งครัด

4.2 การใช้งานจดหมายอิเล็กทรอนิกส์ (Email)

1) ผู้ใช้งานต้องลงทะเบียนเป็นผู้ได้รับสิทธิการใช้และรหัสผ่าน เพื่อเป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคลในการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ (Email) ของบริษัท ซึ่งผู้ใช้งานแต่ละคนจะต้องดูแลรักษาสิทธิการใช้งานและรหัสผ่านของตนเองไม่ให้ผู้อื่นนำไปใช้งานได้ หากมีการกระทำใดซึ่งเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เจ้าของสิทธิต้องรับผิดชอบผลจากความเสียหายที่เกิดขึ้นโดยไม่อาจปฏิเสธได้
2) ผู้ใช้งานต้องใช้ระบบจดหมายอิเล็กทรอนิกส์ (Email) ของบริษัท ในการรับ-ส่งจดหมายอิเล็กทรอนิกส์ซึ่งเกี่ยวกับการปฏิบัติงาน

3) ผู้ใช้งานต้องระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์ (Email) เพื่อไม่ให้เกิดความเสียหายต่อบริษัท สร้างความรำคาญต่อผู้อื่นหรือขัดต่อศีลธรรม และไม่แสวงหาประโยชน์จากการใช้จดหมายอิเล็กทรอนิกส์ (Email) ของบริษัท

4) ผู้ใช้งานต้องออกจากระบบจดหมายอิเล็กทรอนิกส์ (Email) ทันทีหลังจากการเลิกใช้งาน เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

5) ก่อนเปิดเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ (Email) ผู้ใช้งานต้องตรวจสอบผู้ส่งจดหมายอิเล็กทรอนิกส์ (Email) ก่อนเปิดเอกสารแนบเสมอ

6) ผู้ใช้งานไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์ (Email)หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

7) ผู้ใช้งานควรตรวจสอบกล่องจดหมายอิเล็กทรอนิกส์ (Email) ของตนเป็นประจำทุกวัน เพื่อไม่ให้พลาดข้อมูลสำคัญที่เกี่ยวข้องกับการปฏิบัติงาน และเพื่อความเป็นระเบียบเรียบร้อย ผู้ใช้งานควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ (Email) ให้เหลือเท่าที่จำเป็น โดยควรดำเนินการ Archive จดหมายหรือแฟ้มข้อมูลที่ไม่ใช้งานแล้วอย่างสม่ำเสมอ เพื่อลดปริมาณข้อมูลที่ไม่จำเป็น และช่วยให้สามารถค้นหาจดหมายอิเล็กทรอนิกส์ (Email) ที่ต้องการได้อย่างรวดเร็ว รวมถึงสนับสนุนการบริหารจัดการพื้นที่จัดเก็บของระบบจดหมายอิเล็กทรอนิกส์ (Email) อย่างมีประสิทธิภาพ

8) ผู้ใช้งานต้องสำรองข้อมูลที่มีความสำคัญในจดหมายอิเล็กทรอนิกส์ (Email) อย่างสม่ำเสมอ

หมวดที่ 5 การบริหารจัดการสินทรัพย์และเครือข่าย

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านการบริหารจัดการสินทรัพย์และเครือข่าย เป็นส่วนสำคัญของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management) โดยครอบคลุมทั้งการจัดการอุปกรณ์ (Asset) และโครงสร้างพื้นฐานด้านเครือข่าย (Network Infrastructure) ดังนี้

5.1 การบริหารจัดการระบบคอมพิวเตอร์

1) จัดทำทะเบียนคุมสินทรัพย์ในระบบจัดการทรัพย์สินสารสนเทศ

2) การรักษาความปลอดภัยระบบคอมพิวเตอร์ โดย

(1) กำหนดชื่อและ IP Address ในระบบคอมพิวเตอร์ ตามที่ฝ่ายเทคโนโลยีสารสนเทศกำหนด

(2) กำหนดบุคคลรับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่าง ๆ ของโปรแกรมระบบอย่างชัดเจน

(3) มีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบการรักษาความปลอดภัยระบบคอมพิวเตอร์

(4) ในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่า Parameter ในลักษณะที่ผิดปกติ จะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานผู้ดูแลรับผิดชอบโดยทันที

(5) เปิดใช้บริการ (Service) เท่าที่จำเป็น ทั้งนี้หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบการรักษาความปลอดภัยต้องมีมาตรการเพิ่มเติม

(6) มีการติดตั้ง Patch ที่จำเป็นของระบบงานสำคัญ เพื่อปิดช่องโหว่ต่าง ๆ ของโปรแกรมระบบ(System Software) เช่น ระบบปฏิบัติการ DBMS และ Web server อย่างสม่ำเสมอ

(7) ทดสอบ System Software เกี่ยวกับการรักษาความปลอดภัย และประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา

3) บำรุงรักษาอุปกรณ์ ในระบบคอมพิวเตอร์ให้สามารถทำงานได้อย่างมีประสิทธิภาพ โดยควบคุมดูแลให้มีการบำรุงรักษาอุปกรณ์ในระบบคอมพิวเตอร์ตามระยะเวลาที่กำหนด

5.2 การบริหารจัดการโปรแกรม

1) จัดทำทะเบียนคุมโปรแกรม

2) มีการติดตั้งโปรแกรมที่ถูกต้องตามลิขสิทธิหรือโปรแกรมสำหรับใช้งานฟรี (Freeware, Open Source) และติดตั้งเท่าที่จำเป็นต่อการใช้งาน

5.3 การบริหารจัดการระบบเครือข่ายสื่อสาร

1) มีการจัดแบ่งแยกส่วนเครือข่าย/กลุ่ม (VLAN / Zone)

2) จัดทำทะเบียนคุมการใช้งานระบบเครือข่ายสื่อสาร

3) จัดทำแผนผังและขอบเขตของระบบเครือข่ายสื่อสาร

4) ตรวจสอบการใช้งานระบบเครือข่ายสื่อสารให้สามารถใช้งานได้อย่างมีประสิทธิภาพ

5) ควบคุมการจัดเส้นทางบนระบบเครือข่ายสื่อสารและกำหนดวิธีการเข้าถึงระบบเครือข่ายสื่อสาร

6) จัดทำระบบป้องกันการบุกรุกและการใช้งานที่ผิดปกติผ่านระบบเครือข่ายสื่อสาร

7) ทดสอบการบุกรุกโจมตีระบบเครือข่ายสื่อสาร และจัดทำรายงานการโจมตี

8) กำหนดผู้รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ของระบบเครือข่ายสื่อสารและอุปกรณ์ที่เชื่อมต่อ

9) ทบทวนการกำหนดค่า Parameter อย่างน้อยปีละ 1 ครั้ง

10) ทำการบำรุงรักษาระบบเครือข่ายสื่อสารเพื่อให้สามารถใช้งานได้อย่างมีประสิทธิภาพ โดยควบคุมดูแลให้มีการบำรุงรักษาระบบเครือข่ายตามระยะเวลาที่กำหนด

5.4 การบริหารจัดการสินทรัพย์

การบริหารจัดการสินทรัพย์ คือกระบวนการวางแผน จัดหา ใช้งาน ดูแล และควบคุมสินทรัพย์ของบริษัทอย่างเป็นระบบ เพื่อให้เกิดประสิทธิภาพสูงสุด คุ้มค่า และลดความเสี่ยงที่เกี่ยวข้องกับสินทรัพย์ตลอดวงจรชีวิตการใช้งาน

1) จัดทำทะเบียนคุมสินทรัพย์

(1) กำหนดผู้รับผิดชอบต่อสินทรัพย์

(2) จัดหมวดหมู่สินทรัพย์

(3) กำหนดมาตรฐานคอมพิวเตอร์ในบริษัท

2) การเบิกใช้ทรัพย์สินคอมพิวเตอร์และเครือข่าย

(1) ผู้ใช้ที่ต้องการขอเบิกใช้ทรัพย์สินต้องกรอกข้อมูลคำร้องลง Form ที่กำหนด

(2) เจ้าหน้าที่ผู้รับผิดชอบพิจารณาตามขั้นตอนและความเหมาะสมในการขอเบิกใช้งานทรัพย์สินดังกล่าว โดยขอความเห็นชอบจากผู้บริหารหน่วยงานเจ้าของสินทรัพย์ หรือผู้ที่ได้รับมอบหมาย

(3) เมื่อมีการอนุมัติให้เบิกใช้ทรัพย์สิน เจ้าหน้าที่ผู้รับผิดชอบต้องบันทึกข้อมูลสถานที่จัดเก็บหรือติดตั้งใหม่ของทรัพย์สินดังกล่าว ลงในระบบทรัพย์สินสารสนเทศ ลงทะเบียนทรัพย์สินคอมพิวเตอร์และเครือข่ายสื่อสาร เพื่อจัดเก็บเป็นประวัติทรัพย์สิน

3) การแจ้งซ่อมบำรุงทรัพย์สินคอมพิวเตอร์และเครือข่าย

(1) เมื่อผู้ใช้งานพบการทำงานที่ผิดไปจากปกติของทรัพย์สิน หรือไม่สามารถใช้งานทรัพย์สินในการดำเนินงานได้ ผู้ใช้งานต้องแจ้งให้ดำเนินการซ่อมบำรุงให้เจ้าหน้าที่ผู้รับผิดชอบวิเคราะห์อาการเสียหายของทรัพย์สิน หากอยู่ในระยะเวลาประกัน เจ้าหน้าที่สามารถส่งทรัพย์สินเข้ารับการซ่อมบำรุงที่ศูนย์บริการของบริษัทผู้ผลิตทรัพย์สินได้โดยไม่เสียค่าใช้จ่ายในส่วนที่ระบุในประกัน หากทรัพย์สินดังกล่าวไม่อยู่ในระยะเวลาประกัน เจ้าหน้าที่ผู้รับผิดชอบต้องพิจารณาจากความเสียหายของทรัพย์สิน หากความเสียหายของทรัพย์สินสามารถแก้ไขได้ให้ดำเนินการแก้ไข หรือหากเสียหายมากอาจจำเป็นจะต้องจำหน่ายทรัพย์สินดังกล่าว

(2) ในระหว่างที่เจ้าหน้าที่ผู้รับผิดชอบส่งทรัพย์สินเข้ารับการซ่อมบำรุงนั้น หากมีทรัพย์สินอื่นที่สามารถใช้งานทดแทนทรัพย์สินดังกล่าวได้ ให้เจ้าหน้าที่ดำเนินการแจ้งแก่ผู้ใช้ทรัพย์สิน

(3) หลังจากที่เจ้าหน้าที่ผู้รับผิดชอบส่งทรัพย์สินที่พบความเสียหายเข้ารับการแก้ไขเรียบร้อยแล้ว ต้องดำเนินการทดสอบในส่วนที่พบความเสียหายอีกครั้งก่อนจัดส่งทรัพย์สินคืนผู้ใช้

(4) ผู้ใช้ทำการตรวจสอบทรัพย์สิน หากยังพบว่ามีความเสียหายในส่วนเดิมหรือส่วนอื่น ให้รีบแจ้งเจ้าหน้าที่ผู้รับผิดชอบเพื่อดำเนินการแก้ไขตามขั้นตอนต่อไป

4) การตรวจสอบและตรวจนับ (Audit & Inventory) ควรตรวจสอบทรัพย์สินสารสนเทศร่วมกับฝ่ายบัญชีหรือฝ่ายที่เกี่ยวข้อง อย่างน้อยปีละ 1 ครั้ง

5) การนำทรัพย์สินของบริษัท เช่น คอมพิวเตอร์พกพา โน้ตบุ๊ก หรืออุปกรณ์สารสนเทศอื่น ๆ ออกนอกสถานที่ทำงาน สามารถกระทำได้เมื่อได้รับอนุมัติจากผู้มีอำนาจตามระเบียบของบริษัท และผู้ใช้งานต้องรับผิดชอบในการดูแลรักษาทรัพย์สินให้อยู่ในสภาพปลอดภัย ไม่สูญหาย ไม่ถูกเข้าถึงโดยบุคคลที่ไม่ได้รับอนุญาต และต้องปฏิบัติตามมาตรการด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทอย่างเคร่งครัด

5.5 การจัดการสื่อบันทึกข้อมูล (Media Handling Policy)

เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับสื่อที่ใช้ในการบันทึกข้อมูลของบริษัท โดยการถูกเปิดเผยโดยไม่ได้รับอนุญาต การเปลี่ยนแปลง การขนย้าย การลบ หรือการทำลายข้อมูล

1) บริษัทไม่มีนโยบายอนุญาตให้ผู้ใช้งานระบบใช้งานสื่อบันทึกข้อมูลแบบเคลื่อนย้ายได้ (Removable Media) เช่น USB Flash Drive, External Hard Disk, CD/DVD หรือสื่อบันทึกข้อมูลประเภทอื่น เพื่อจัดเก็บ คัดลอก หรือถ่ายโอนข้อมูลของบริษัท โดยข้อมูลของบริษัทต้องจัดเก็บและแลกเปลี่ยนผ่านระบบที่บริษัทกำหนด เช่น

SharePoint, OneDrive หรือระบบ Cloud ภายในบริษัท และการเข้าถึงข้อมูลต้องเป็นไปตามสิทธิ์การใช้งานและการจัดชั้นความลับของสารสนเทศที่บริษัทกำหนด

2) หากจำเป็นต้องใช้งานสื่อบันทึกข้อมูลแบบให้แจ้งผู้เกี่ยวข้องโดยให้ผู้บังคับบัญชา และผู้จัดการฝ่ายเทคโนโลยีสารสนเทศพิจารณาอนุมัติ เพื่อเก็บประวัติการใช้งาน

5.6 การใช้สื่อบันทึกข้อมูลและแบ่งปันข้อมูลผ่านระบบ Share File

เพื่อกำหนดแนวทางในการใช้งานระบบจัดเก็บและแบ่งปันข้อมูล (Share File) เช่น Microsoft SharePoint Microsoft One Drive ภายในบริษัท และระบบ Share Drive ภายในบริษัท เพื่อให้เกิดความปลอดภัย ความเป็นส่วนตัว และประสิทธิภาพในการทำงานร่วมกัน

1) การเข้าถึงและการใช้งาน
   (1) ผู้ใช้งานต้องเข้าระบบด้วยบัญชีที่ได้รับอนุญาตจากผู้ดูแลระบบเท่านั้น
   (2) จำกัดสิทธิการเข้าถึงตามหลัก Least Privilege โดยให้เฉพาะผู้ที่จำเป็นต้องใช้ข้อมูล
   (3) ห้ามแชร์ลิงก์หรือไฟล์ที่ตั้งค่าให้ “Anyone with the link” เข้าถึงได้

2) การจัดเก็บไฟล์
   (1) ควรจัดเก็บไฟล์ในโฟลเดอร์ที่กำหนดตามแผนกหรือโครงการ
   (2) ห้ามอัปโหลดไฟล์ที่มีข้อมูลส่วนบุคคลที่สามารถระบุตัวตนได้ (PII) หรือข้อมูลอ่อนไหว (Sensitive Data) เช่น บัตรประชาชน หรือเลขบัญชี โดยไม่มีการเข้ารหัสหรือมาตรการป้องกัน
   (3) ห้ามจัดเก็บซอฟต์แวร์ผิดลิขสิทธิหรือไฟล์ที่ละเมิดกฎหมายใด ๆ
   (4) การบริหารพื้นที่การใช้งานให้ผู้ดูแลระบบเป็นผู้กำหนด

3) การแบ่งปันไฟล์
   (1) การแชร์ไฟล์ควรใช้การกำหนดสิทธิแบบ “View Only” หากไม่จำเป็นต้องแก้ไข
   (2) หากจำเป็นต้องแชร์ข้อมูลกับบุคคลภายนอก ต้องได้รับอนุมัติจากหัวหน้าหน่วยงาน
   (3) ควรใช้รหัสผ่านหรือวันหมดอายุในการแชร์ไฟล์เสมอหากระบบรองรับทั้งภายในและภายนอกบริษัท

4) การสำรองและกู้คืนข้อมูล
   (1) ระบบ SharePoint มีการสำรองข้อมูลอัตโนมัติ ผู้ดูแลระบบ จะรับผิดชอบในการกู้คืนข้อมูลในกรณีจำเป็น
   (2) ผู้ใช้งานควรหลีกเลี่ยงการลบไฟล์ถาวรโดยไม่จำเป็น

หมวดที่ 6 การควบคุมความมั่นคงปลอดภัยสำหรับการปฏิบัติงาน

ควรมีการกำหนดบทบาทและหน้าที่ของผู้รับผิดชอบในการปฏิบัติงาน และ/หรือ บุคคลที่เกี่ยวข้องกับการปฏิบัติงานในขั้นตอนต่าง ๆ และผู้มีอำนาจอนุมัติ

6.1 การบันทึกและเฝ้าระวังเหตุการณ์ (Logging & Monitoring)

1) ฝ่ายเทคโนโลยีสารสนเทศต้องจัดให้มีการบันทึก (Log) เหตุการณ์ด้านความมั่นคงปลอดภัยของระบบที่สำคัญ
2) ต้องกำหนดผู้รับผิดชอบในการทบทวน Log ดังกล่าวเป็นประจำ อย่างน้อยเดือนละ 1 ครั้ง หรือบ่อยกว่านั้น สำหรับระบบที่มีความเสี่ยงสูง และบันทึกผลการทบทวนไว้เป็นหลักฐาน

3) กรณีตรวจพบเหตุการณ์ผิดปกติจากการทบทวน Log ต้องดำเนินการตามขั้นตอนการบริหารจัดการเหตุการณ์ผิดปกติ

4) ระยะเวลาการจัดเก็บ Log ต้องไม่น้อยกว่าที่กฎหมายกำหนด (พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ อย่างน้อย 1 ปี)

6.2 การบริหารจัดการเหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัย (Incident Management)

1) ฝ่ายเทคโนโลยีสารสนเทศต้องจัดให้มีช่องทางกลางสำหรับผู้ใช้งานแจ้งเหตุการณ์ผิดปกติหรือเหตุการณ์ที่สงสัยว่าเป็นภัยคุกคามด้านความมั่นคงปลอดภัย

2) ต้องจัดระดับความรุนแรงของเหตุการณ์ผิดปกติอย่างน้อย 3 ระดับ (สูง/กลาง/ต่ำ) โดยพิจารณาจากผลกระทบต่อธุรกิจและขอบเขตความเสียหาย

3) ต้องกำหนดระยะเวลาเป้าหมายในการตอบสนองและแก้ไขเหตุการณ์ (Response/Resolution SLA) ตามระดับความรุนแรง

4) กรณีเหตุการณ์เกี่ยวข้องกับข้อมูลส่วนบุคคล ให้ปฏิบัติตามขั้นตอนการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ภายใน 72 ชั่วโมงตามที่กฎหมาย PDPA กำหนด

5) ต้องจัดทำสรุปผลและบทเรียนที่ได้รับ (Post-Incident Review) สำหรับเหตุการณ์ระดับสูง เพื่อป้องกันการเกิดซ้ำ

6) ต้องเก็บบันทึกประวัติเหตุการณ์ผิดปกติทั้งหมดไว้เป็นหลักฐานประกอบการตรวจสอบ

หมวดที่ 7 การสำรองข้อมูลและกู้คืนข้อมูล

เพื่อให้สารสนเทศและอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย และเพื่อป้องกันการสูญหายของข้อมูล

1) มีระบบจัดเก็บและสำรองข้อมูลตามประเภทของข้อมูล ได้แก่ โปรแกรมระบบปฏิบัติการโปรแกรมประยุกต์หรือแอปพลิเคชัน (Application Software) ชุดคำสั่ง และข้อมูล อย่างน้อย 1 ชุด แยกสถานที่จัดเก็บจากกันเพื่อความมั่นคงปลอดภัยและใช้งานได้อย่างต่อเนื่อง

2) กำหนดผู้รับผิดชอบในการสำรองข้อมูล ตรวจสอบความมีอยู่อย่างถูกต้อง ครบถ้วนของข้อมูล อย่างน้อยปีละ 1 ครั้ง และมีการบันทึกรายละเอียดการตรวจสอบ ในกรณีตรวจพบข้อมูลสูญหายไม่ถูกต้องครบถ้วน ให้ดำเนินการปรับปรุง แก้ไขข้อมูลให้มีความสมบูรณ์ครบถ้วนในทันที

3) กำหนดความถี่ในการสำรองข้อมูลของระบบงาน และทำการสำรองข้อมูลตามความถี่ที่กำหนดไว้ (ระบบงานที่มีการเปลี่ยนแปลงบ่อย ควรจะมีความถี่ในการสำรองข้อมูลมากขึ้น) และมีการนำข้อมูลที่สำรองไปเก็บไว้นอกสถานที่อย่างน้อย 1 ชุด

(1) กำหนดขั้นตอนการจัดทำสำรองข้อมูล และการกู้คืนข้อมูลอย่างถูกต้องรวมทั้งซอฟต์แวร์

(2) ทำการตรวจสอบว่าการสำรองข้อมูลที่เกิดขึ้นสำเร็จครบถ้วนหรือไม่

(3) ทำการทดสอบกู้คืนข้อมูลที่สำรองไว้ อย่างน้อยปีละ 1 ครั้ง รวมทั้งดำเนินการทดสอบว่าระบบงานทั้งหมดสามารถใช้งานได้หรือไม่

4) จัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้คืนระบบกลับคืนได้ภายในระยะเวลาที่กำหนด โดยมีแนวทางปฏิบัติสำหรับการกู้คืนข้อมูลจากภัยพิบัติ โดย

(1) มีการกำหนดระบบงานที่มีความสำคัญทั้งหมดของบริษัท และจัดทำเป็นบัญชีรายชื่อของระบบงานดังกล่าว รวมทั้งปรับปรุงบัญชีรายชื่อนี้ให้มีความทันสมัยอยู่เสมอตามระบบงานที่มีความสำคัญที่เกิดขึ้นใหม่

(2) ประเมินความเสี่ยงสำหรับระบบงานที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงที่พบ และให้ปรับปรุงรายงานการประเมินความเสี่ยงอย่างน้อยปีละ 1 ครั้ง

(3) กำหนดชนิดของข้อมูล เช่น ซอฟต์แวร์ต่าง ๆ ที่เกี่ยวข้องกับระบบงาน ขหรือข้อมูลในฐานข้อมูล

(4) กำหนดความถี่ในการสำรองข้อมูลและวิธีการสำรอง เช่น แบบ Full Backup หรือ Incremental Backup ของระบบงานที่มีความสำคัญเหล่านั้น

(5) จัดทำแผนกู้คืนเพื่อรับมือกับภัยพิบัติที่อาจเกิดขึ้นได้ แผนกู้คืนต้องมีรายละเอียดดังต่อไปนี้

- การกำหนดหน้าที่และความรับผิดชอบต่อผู้ที่เกี่ยวข้องทั้งหมด
- การประเมินความเสี่ยงสำหรับระบบงานที่มีความสำคัญ และกำหนดมาตรการเพื่อลดความเสี่ยง เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วง ทำให้ไม่สามารถเข้าใช้ระบบงานได้
- การกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบงาน
- การกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูลและทดสอบกู้คืนข้อมูลที่สำรองไว้
- การทดสอบตามแผนเตรียมความพร้อมและประสิทธิภาพของแผนที่จัดทำไว้ อย่างน้อย ปีละ 1 ครั้ง
- การกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการ เครือข่าย ฮาร์ดแวซอฟต์แวร์
- การสร้างความตระหนักหรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน

(6) ให้ทำการทบทวนแผนกู้คืนอย่างน้อยปีละ 1 ครั้ง

(7) ให้ทำการสำรองข้อมูลตามชนิด ความถี่ และวิธีการสำรองที่ได้กำหนดไว้ และให้ตรวจสอบอย่างสม่ำเสมอว่าข้อมูลที่สำรองไปนั้นมีความครบถ้วน

(8) ให้ทำการทดสอบกู้คืนข้อมูลที่สำรองไว้นั้นว่าสามารถกู้คืนได้อย่างครบถ้วนหรือไม่ อย่างน้อยปีละ 1 ครั้ง ถ้าพบว่ามีปัญหาเกิดขึ้นในระหว่างการทดสอบกู้คืน ให้ดำเนินการแก้ไขและบันทึกข้อมูลปัญหานั้นไว้ พร้อมทั้งวิธีการแก้ไขอย่างเป็นลายลักษณ์อักษร

5) จัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินที่ไม่สามารถดำเนินการด้วยวิธีทางอิเล็กทรอนิกส์ เพื่อให้การปฏิบัติงานเป็นไปอย่างต่อเนื่อง

หมวดที่ 8 การประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศและการสื่อสาร

การประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Information and Communication Technology Risk Assessment) มีวัตถุประสงค์เพื่อระบุ วิเคราะห์ และประเมินระดับความเสี่ยงที่อาจเกิดขึ้นกับทรัพยากรสารสนเทศ เพื่อกำหนดแนวทางในการจัดการและลดความเสี่ยงอย่างเหมาะสม โดยสามารถสรุปแนวทางการประเมินความเสี่ยงได้ ดังนี้

1) มีคณะทำงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศเพื่อดำเนินการ ดังต่อไปนี้
   (1) จัดลำดับความสำคัญของความเสี่ยง
   (2) จัดทำแผนบริหารความเสี่ยง
   (3) ดำเนินการตามแผนบริหารความเสี่ยง
2) มีการตรวจสอบและประเมินความเสี่ยงในเรื่องความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและระบบคอมพิวเตอร์อย่างน้อยปีละ 1 ครั้ง
3) มีการรายงานการตรวจสอบและประเมินความเสี่ยงเสนอผู้รับผิดชอบและหน่วยงานที่รับผิดชอบ และจะดำเนินการปรับปรุงตามคำแนะนำหน่วยงานที่รับผิดชอบนั้นโดยทันที
4) มีการกำหนดความรับผิดชอบของผู้ใช้งานหรือผู้บริหาร ให้ผู้ใช้งานและผู้บริหารรับผิดชอบในกรณีเกิดความเสียหายหรืออันตรายอันเนื่องมาจากผู้ใช้งานหรือผู้บริหารบกพร่อง หรือไม่ปฏิบัติตามนโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศและแนวปฏิบัติในการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศแล้วแต่กรณี

หมวดที่ 9 การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เพื่อเสริมสร้างวัฒนธรรมองค์กรที่ให้ความสำคัญกับความปลอดภัยของข้อมูล และลดความเสี่ยงที่อาจเกิดจากความประมาทหรือความไม่รู้ของผู้ใช้งาน โดยมีเป้าหมายหลักเพื่อให้บุคลากรทุกระดับในองค์กรสามารถปฏิบัติตามแนวทางต่อไปนี้

1) มีการเผยแพร่ประชาสัมพันธ์และฝึกอบรมให้เจ้าหน้าที่บริษัทรับทราบ เข้าใจ และไม่กระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายอื่น ๆ ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ รวมถึงมีความรับผิดชอบในการใช้ทรัพยากรทางด้านเทคโนโลยีสารสนเทศของบริษัทอย่างเหมาะสม และจัดอบรมหรือจัดทดสอบประจำปีอย่างน้อยปีละ 1 ครั้ง
2) การทบทวนปรับปรุงนโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศและแนวปฏิบัติในการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศให้มีความทันสมัย และเป็นมาตรฐานที่ยอมรับ อย่างน้อยปีละ 1 ครั้ง

หมวดที่ 10 การจัดหา พัฒนา และดูแลระบบเทคโนโลยีสารสนเทศ (Systems Acquisition, Development and Maintenance)

1) การวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Requirements Analysis and Specification เพื่อให้มั่นใจว่ามีการสร้างความปลอดภัยสารสนเทศให้กับระบบ

เทคโนโลยีสารสนเทศ ตลอดวงจรการพัฒนาระบบ ซึ่งรวมถึงความต้องการด้านความปลอดภัยสารสนเทศที่ให้บริการผ่านเครือข่ายสาธารณะ

(1) ต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยไว้อย่างชัดเจน ในระบบที่จะพัฒนาขึ้นมาใช้งาน ซื้อมาใช้งาน หรือการปรับปรุงระบบที่มีอยู่แล้ว หน่วยงานดูแลระบบเทคโนโลยีสารสนเทศ จะต้องทำการวิเคราะห์ระบบเทคโนโลยีสารสนเทศ ว่ามีความเสี่ยงใดบ้างที่จะทำให้ข้อมูลเกิดความเสียหาย โดยมุ่งเน้นในส่วนต่าง ๆ ดังนี้

- มาตรการปฏิบัติก่อนที่จะเกิดความเสียหาย เช่น การสำรองข้อมูล ระบบเครือข่ายสำรอง เป็นต้น
- มาตรการปฏิบัติหลังจากเกิดความเสียหาย เช่น แผนการกู้คืนข้อมูล ระยะเวลาในการกู้คืนข้อมูล เป็นต้น

(2) ความมั่นคงปลอดภัยของบริการสารสนเทศบนเครือข่ายสาธารณะ (Securing application services on public networks) สารสนเทศที่เกี่ยวข้องกับการบริการสารสนเทศที่มีการส่งผ่านเครือข่ายสาธารณะต้องได้รับการป้องกัน และการเปิดเผย หรือเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต

(3) การป้องกันธุรกรรมของบริการสารสนเทศ (Protecting application services transactions) สารสนเทศที่เกี่ยวข้องกับธุรกรรมของบริการสารสนเทศ ต้องได้รับการป้องกันจากการรับส่งข้อมูลที่ไม่สมบูรณ์ การส่งข้อมูลผิดเส้นทางการเปลี่ยนแปลงข้อความโดยไม่ได้รับอนุญาต การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต การส่งข้อมูลซ้ำโดยไม่ได้รับอนุญาต

2) ระเบียบปฏิบัติสำหรับกระบวนการในการพัฒนาระบบและสนับสนุน (Security in Development and Support Processes) เพื่อให้มั่นใจได้ว่ามีระบบเทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัย ครอบคลุมทั้งวงจรการพัฒนาระบบสารสนเทศ ระเบียบปฏิบัติการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure Development Policy)

(1) ต้องมีการกำหนดหลักเกณฑ์สำหรับการพัฒนาซอฟต์แวร์ และมีการปฏิบัติตามระเบียบปฏิบัติหรือข้อกำหนดที่บริษัท กำหนดขึ้นมา เช่น การพัฒนาซอฟต์แวร์ ควรคำนึงความปลอดภัยในทุกขั้นตอนของการพัฒนา และนักพัฒนา (Developer) ควรมีความสามารถในการหลีกเลี่ยงไม่ให้โปรแกรมที่พัฒนาตรวจพบช่วงโหว่ และต้องสามารถแก้ไขช่องโหว่ที่ตรวจพบได้

(2) กระบวนการในการควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์ (System Change Control Procedures) ผู้พัฒนาระบบเทคโนโลยีสารสนเทศต้องมีกระบวนการ เพื่อควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำหรับระบบเทคโนโลยีสารสนเทศที่ใช้งานจริง หรือให้บริการอยู่แล้ว เช่น

คำขอให้แก้ไขต้องมาจากผู้ที่มีสิทธิ

- ต้องมีการอนุมัติคำขอโดยผู้มีอำนาจอนุมัติ
- ต้องมีการควบคุมผลข้างเคียงที่อาจเกิดขึ้นหลังจากมีการแก้ไข
- เมื่อแก้ไขเสร็จแล้วต้องมีการตรวจรับจากผู้มีอำนาจอนุมัติ หรือ ผู้ใช้งาน

(3) การตรวจสอบซอฟต์แวร์หลังจากการเปลี่ยนแปลงระบบปฏิบัติการ (Technical Review of Applications After Operating Platform Changes) เมื่อระบบปฏิบัติการมีการแก้ไขหรือเปลี่ยนแปลง ผู้พัฒนาระบบเทคโนโลยีสารสนเทศจะต้องตรวจสอบ และทดสอบซอฟต์แวร์ต่าง ๆ ที่ใช้งานว่าไม่มีผลกระทบต่อการทำงานและความมั่นคงปลอดภัย

(4) การควบคุมการเปลี่ยนแปลงของซอฟต์แวร์สำเร็จรูป (Restrictions on Changes to Software Packages) เมื่อมีการใช้งานซอฟต์แวร์สำเร็จรูปต้องมีการควบคุมการเปลี่ยนแปลงเท่าที่จำเป็น และการเปลี่ยนแปลงทั้งหมดจะต้องถูกทดสอบ และจัดทำเป็นเอกสารเพื่อให้สามารถนำมาใช้งานได้เมื่อมีการปรับปรุงซอฟต์แวร์ในอนาคต

(5) หลักการวิศวกรรมระบบด้านความมั่นคงปลอดภัย (Secure system engineering principles)เพื่อให้เกิดความมั่นคงปลอดภัยทางด้านวิศวกรรม ระบบต้องมีการกำหนดขึ้นมาเป็นลายลักษณ์อักษร โดยมีการปรับปรุงอย่างต่อเนื่อง และมีการประยุกต์ใช้กับงานพัฒนาระบบ โดยให้คณะกรรมการความปลอดภัยฯ มีหน้าที่ดูแลระบบด้านความมั่นคงปลอดภัยด้านโครงสร้างสำนักงาน

(6) การจ้างหน่วยงานภายนอกเพื่อพัฒนาระบบงาน (Outsourced Development) ในการทำสัญญาว่าจ้างการพัฒนาระบบของบริษัท ต้องมีความชัดเจนและครอบคลุมถึงสัญญาทางด้านลิขสิทธิซอฟต์แวร์ การใช้ระบบการตรวจสอบระบบ โดยละเอียดก่อนติดตั้งใช้งานจริง รวมถึงการรับรองคุณภาพของระบบ และการกำหนดขอบเขตในการจ้างพัฒนาระบบ

(7) การทดสอบด้านความมั่นคงปลอดภัยของระบบ (System security testing) โปรแกรมหรือระบบที่พัฒนาขึ้นมาควรมีการทดสอบคุณสมบัติด้านความมั่นคงปลอดภัย โดยต้องมีการทดสอบอยู่ในช่วงระหว่างการพัฒนา การทดสอบเพื่อรับรองระบบ (System/User acceptance testing) มีการจัดทำแผนการทดสอบหรือเกณฑ์ที่เกี่ยวข้องเพื่อรับรองระบบ โดยต้องมีการจัดทำทั้งสำหรับระบบใหม่และระบบที่ปรับปรุง

(8) การประเมินความเสี่ยงผู้ให้บริการภายนอก (Third-Party/Supplier Risk Management)

- ก่อนเริ่มใช้บริการผู้ให้บริการภายนอกที่เข้าถึงระบบเทคโนโลยีสารสนเทศหรือข้อมูลของบริษัท (เช่น ผู้พัฒนาระบบ ผู้ให้บริการ Cloud ผู้ดูแลบำรุงรักษาระบบ) ต้องมีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของผู้ให้บริการนั้นตามความเหมาะสมของระดับความเสี่ยง
- สัญญาว่าจ้างกับผู้ให้บริการภายนอกต้องระบุข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศและการรักษาความลับของข้อมูล (Confidentiality/NDA)
- ต้องมีการทบทวนความเสี่ยงของผู้ให้บริการภายนอกที่มีความสำคัญสูงเป็นระยะ อย่างน้อยปีละ 1 ครั้ง

- กรณีสิ้นสุดสัญญาหรือยุติการให้บริการ ต้องมีขั้นตอนเพิกถอนสิทธิการเข้าถึงระบบและข้อมูลของผู้ให้บริการภายนอกโดยทันที และตรวจสอบการส่งคืนหรือทำลายข้อมูลของบริษัทตามที่ตกลงในสัญญา

3) ระเบียบปฏิบัติข้อมูลสำหรับการทดสอบ (Test Data) เพื่อให้มีการป้องกันข้อมูลที่นำมาใช้ในการทดสอบ

(1) การแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation of Development, Testing and Operational Environments)

- สภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการ ต้องมีการจัดทำแยกกันเพื่อลดความเสี่ยงของการเข้าถึง หรือการเปลี่ยนแปลงสภาพแวดล้อมสำหรับการให้บริการโดยไม่ได้รับอนุญาต
- ในการพัฒนาระบบ ต้องจัดให้มีการแยกสภาพแวดล้อมสำหรับระบบที่ใช้ในการพัฒนา (Development System) และระบบที่ใช้งานจริง (Production System)
- ต้องจัดให้มีระเบียบปฏิบัติที่ชัดเจนในการโอนย้ายโปรแกรมที่พัฒนาเสร็จแล้ว ไปยังระบบที่ใช้งานจริง
- ต้องไม่มีการติดตั้งคอมไพเลอร์ (Compiler) หรือโปรแกรมสำหรับการพัฒนาโปรแกรมอื่น ๆ ในระบบคอมพิวเตอร์ที่ใช้งานจริง

(2) การป้องกันข้อมูลสำหรับการทดสอบ (Protection of Test Data) ข้อมูลจริงที่จะนำไปใช้ในการทดสอบระบบ จะต้องได้รับอนุญาตจากผู้รับผิดชอบในการรักษาข้อมูลนั้น ๆ ก่อน เมื่อใช้งานเสร็จจะต้องทำการลบข้อมูลจริงออกจากระบบทดสอบทันที และทำการบันทึกไว้เป็นหลักฐานว่าได้นำข้อมูลจริงไปใช้ในการทดสอบอะไรบ้าง รวมถึงวัน เวลา และหน่วยงานที่ทดสอบ แจ้งไปยังผู้รับผิดชอบในการรักษาข้อมูลนั้นอีกครั้ง

หมวดที่ 11 การใช้งานปัญญาประดิษฐ์ (AI)

เพื่อกำหนดแนวปฏิบัติที่ปลอดภัยในการใช้งานเทคโนโลยีปัญญาประดิษฐ์ (AI) ภายในบริษัท เพื่อป้องกันความเสี่ยงด้านความมั่นคงปลอดภัยของข้อมูลที่ขัดกับกฎหมายและจริยธรรม โดยมุ่งเน้นการป้องกันข้อมูลรั่วไหล ความเสียหายต่อบริษัทและภาพลักษณ์

1) ขั้นตอนการปฏิบัติงาน (Procedures) เพื่อให้การใช้เทคโนโลยีปัญญาประดิษฐ์ (AI) ภายในบริษัท เป็นไปอย่างเหมาะสม ปลอดภัย และสอดคล้องกับกฎหมาย รวมถึงจริยธรรมในการดำเนินธุรกิจ บริษัทกำหนดขั้นตอนการปฏิบัติงาน ดังนี้

(1) การขออนุมัติใช้งานเครื่องมือ AI ใหม่

- พนักงานที่มีความประสงค์จะใช้งานเครื่องมือ AI ใหม่ ต้องเสนอคำขอผ่านหัวหน้างานโดยชี้แจงวัตถุประสงค์และลักษณะการใช้งาน
- หัวหน้างานจะส่งคำขอดังกล่าวให้ฝ่ายเทคโนโลยีสารสนเทศ (IT) หรือฝ่ายบริหารความเสี่ยงพิจารณาเรื่องความเหมาะสมและประเมินความเสี่ยง
- เมื่อได้รับการอนุมัติแล้ว จึงสามารถดำเนินการใช้งานเครื่องมือ AI ได้ตามวัตถุประสงค์ที่ระบุไว้ แนวทางการใช้งานที่อนุญาต บริษัทอนุญาตให้ใช้งาน AI ได้ในกรณีที่มีลักษณะดังต่อไปนี้

(2) แนวทางการใช้งานที่ไม่อนุญาต เพื่อป้องกันความเสี่ยงทางกฎหมายและจริยธรรม ห้ามใช้งาน AI ในกรณีต่อไปนี้

- เพื่อเพิ่มประสิทธิภาพในการทำงาน การวิเคราะห์ข้อมูล และการตัดสินใจในบริษัท
- ใช้เฉพาะกับข้อมูลที่ไม่ใช่ข้อมูลความลับหรือข้อมูลที่เผยแพร่โดยทั่วไป (Public/Non-sensitive Data) ซึ่งไม่เกี่ยวข้องกับข้อมูลภายในของบริษัท หรือข้อมูลที่อ่อนไหว
- ใช้ผ่านระบบหรือเครื่องมือ AI ที่ได้รับการตรวจสอบและอนุมัติจากฝ่ายเทคโนโลยีสารสนเทศ
- ต้องตั้งค่าไม่ให้ AI นำข้อมูลไปจัดเก็บ ประมวลผล หรือนำไปใช้ในการฝึกโมเดลของผู้ให้บริการเพื่อลดความเสี่ยงข้อมูลรั่วไหลหรือถูกใช้โดยไม่ได้รับอนุญาต
- กรณีผลลัพท์ที่ถูกสร้างโดย AI ให้ระบุให้ชัดเจนถึงที่มาของผลลัพท์ดังกล่าว เช่น “เนื้อหานี้ถูกสร้างด้วย AI” หรือ “This Content is generated by AI” เป็นต้น

(3) แนวทางการใช้งานที่ไม่อนุญาต เพื่อป้องกันความเสี่ยงทางกฎหมายและจริยธรรม ห้ามใช้งาน AI ในกรณีต่อไปนี้

- ห้ามป้อน ส่ง หรือเปิดเผยข้อมูลภายในของบริษัท เช่น ข้อมูลทางการเงิน ข้อมูลลูกค้า ข้อมูลพนักงาน หรือข้อมูลโครงการที่ยังไม่เผยแพร่ผ่านระบบ AI ที่ไม่อยู่ภายใต้การควบคุมของบริษัท
- ห้ามใช้งาน AI เพื่อสื่อสารในนามบริษัทหรือดำเนินการใด ๆ ที่เป็นการสื่อสารกับบุคคลภายนอกโดยไม่ได้รับอนุญาตอย่างเป็นทางการ
- ห้ามคัดลอก สร้าง หรือเผยแพร่เนื้อหาที่ละเมิดลิขสิทธิ์ โดยใช้เครื่องมือ AI โดยไม่มีการอ้างอิงหรือได้รับสิทธิ์จากเจ้าของลิขสิทธิ์
- ห้ามใช้งาน AI เพื่อวิเคราะห์ หรือตัดสินใจแทนมนุษย์ในประเด็นที่มีความละเอียดอ่อนหรือส่งผลกระทบต่อบุคคล เช่น การสรรหาบุคลากร การประเมินผลการปฏิบัติงาน หรือการลงโทษทางวินัย เว้นแต่จะมีการกลั่นกรองโดยผู้มีอำนาจและเป็นไปตามขั้นตอนของบริษัท อย่างเคร่งครัด
- ห้ามใช้ AI ในการกระทำที่ขัดต่อกฎหมาย ผิดศีลธรรม หรือผิดจรรยาบรรณวิชาชีพ หรือหลีกเลี่ยงหรือฝ่าในการควบคุมภายในบริษัท ทำให้เกิดความเสียหาย หรือทำให้บริษัทเสื่อมเสียชื่อเสียง
- ห้ามใช้ AI สร้างเนื้อหาเท็จ ปลอมแปลง หรือทำให้บุคคลอื่นเข้าใจผิด รวมถึงการสร้างภาพ เสียง วิดีโอปลอม (Deepfake) ที่อาจสร้างความเสียหายแก่บริษัท หรือบุคคลอื่น
- ห้ามใช้ AI เพื่อแอบอ้างเป็นบุคคลอื่น หรือเลียนแบบลายเซ็น เสียง หรืออัตลักษณ์ของบุคคลอื่นโดยไม่ได้รับอนุญาต

2) ข้อควรระวังในการใช้งาน AI (AI Risk Awareness) การใช้งานเทคโนโลยีปัญญาประดิษฐ์ (AI) อาจก่อให้เกิดความเสี่ยงด้านข้อมูล ความถูกต้อง ความปลอดภัย และจริยธรรมในการใช้งาน ดังนั้นผู้ใช้งานต้องตระหนักถึงข้อควรระวังดังต่อไปนี้

(1) ข้อมูลที่ป้อนเข้าสู่ระบบ AI อาจถูกจัดเก็บ ประมวลผล หรือใช้ในการพัฒนาโมเดลของผู้ให้บริการ จึงต้องหลีกเลี่ยงการป้อนข้อมูลที่เป็นความลับหรือข้อมูลส่วนบุคคลของบริษัทและลูกค้า

(2) ผลลัพธ์จาก AI อาจไม่ถูกต้องหรือคลาดเคลื่อน (AI Hallucination) ผู้ใช้งานต้องตรวจสอบความถูกต้องก่อนนำไปใช้งานทุกครั้ง โดยเฉพาะข้อมูลด้านกฎหมาย การเงิน ต้องมีการสอบทายโดยผู้เชียวชาญในเรื่องนั้น ๆ ก่อนนำไปใช้เสมอ

(3) ระบบ AI อาจมีอคติ (Bias) จากข้อมูลที่ใช้ในการฝึกสอน จึงไม่ควรใช้ AI เพียงลำพังในการตัดสินใจที่มีผลกระทบต่อบุคคลหรือองค์กร เช่น การคัดเลือกพนักงาน การประเมินผลงาน การอนุมัติสินเชื่อ เป็นต้น หากใช้งานระบบ AI ต้องมีมนุษย์เป็นผู้พิจารณาและตัดสินใจขั้นสุดท้ายเสมอ

(4) ผลลัพธ์จาก AI อาจเกี่ยวข้องกับทรัพย์สินทางปัญญาหรือลิขสิทธิ์ ผู้ใช้งานต้องตรวจสอบก่อนนำไปเผยแพร่หรือใช้งานเชิงพาณิชย์

(5) ห้ามใช้ผลลัพธ์จาก AI โดยไม่ผ่านการตรวจสอบเพื่อสื่อสารในนามบริษัท หรือทำให้เกิดความเข้าใจผิดต่อบุคคลภายนอก

(6) ผู้ใช้งานต้องตระหนักว่า AI เป็นเพียงเครื่องมือสนับสนุนการทำงาน และไม่สามารถแทนการใช้ดุลยพินิจของมนุษย์ในเรื่องสำคัญได้

3) การจัดอบรมและส่งเสริมความรู้เกี่ยวกับการใช้งาน AI

(1) จัดอบรมและส่งเสริมความรู้เกี่ยวกับการใช้งาน AI อย่างมีจริยธรรมให้แก่พนักงาน

(2) ประสานงานร่วมกับฝ่ายเทคโนโลยีสารสนเทศ และผู้บริหารเพื่อบูรณาการการใช้งาน AI กับนโยบายด้านบุคลากร

4) การรายงานเหตุการณ์ละเมิด กรณีพบเหตุการณ์ผิดปกติหรือการละเมิดนโยบาย ผู้ใช้งานต้องดำเนินการดังนี้

(1) รายงานเหตุการณ์รั่วไหลของข้อมูลผ่านระบบ AI ทันทีต่อฝ่ายความมั่นคงปลอดภัยสารสนเทศ และฝ่ายคุ้มครองข้อมูลส่วนบุคคล

(2) รายงานการพบผลลัพธ์ที่อาจก่อให้เกิดความเสียหาย เช่น ข้อมูลที่ผิดพลาดร้ายแรง ผลลัพธ์ที่มีอคติ หรือเนื้อหาที่ไม่เหมาะสม ต่อหัวหน้างานและฝ่าย Compliance

(3) รายงานการพบการใช้งาน AI ที่ฝ่าฝืนนโยบาย ผ่านช่องทางการรับเรื่องร้องเรียน (Whistleblower) ของบริษัท

(4) รายงานต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ภายใน 72 ชั่วโมง หากมีเหตุละเมิดหรือข้อมูลส่วนบุคคลรั่วไหล (Data Breach)

ส่วนที่ 6 บทลงโทษ

พนักงานทุกคนมีหน้าที่ต้องปฏิบัติตามระเบียบฉบับนี้อย่างเคร่งครัด หากฝ่าฝืน ละเลย หรือจงใจไม่ปฏิบัติตามจนเป็นเหตุให้เกิดความเสียหาย หรือมีความเสี่ยงที่จะเกิดความเสียหายต่อบริษัท พนักงานจะต้องได้รับการพิจารณาโทษทางวินัยตามความร้ายแรงของพฤติกรรมและการกระทำผิดดังกล่าว

ทั้งนี้ หากพนักงานกระทำการใด ๆ ให้ข้อมูลของลูกค้า คู่ค้า หรือบุคคลอื่นรั่วไหล หรือมีการนำไปเปิดเผยเพื่อหาประโยชน์โดยมิชอบ พนักงานจะต้องรับผิดชอบเป็นการส่วนตัว และบริษัทมีสิทธิดำเนินคดีตามกฎหมายและความรับผิดทางแพ่งนอกเหนือจากการลงโทษทางวินัยได้ด้วย หากการฝ่าฝืนของพนักงานทำให้บริษัทต้องระวางโทษปรับจากหน่วยงานราชการ เนื่องจากมีการฝ่าฝืนต่อกฎหมาย เช่น ประมวลกฎหมายอาญา, พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์, พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPA) หรือถูกฟ้องร้องเรียกค่าเสียหายจากบุคคลหรือหน่วยงานภายนอก บริษัทขอสงวนสิทธิ์ในการฟ้องร้องดำเนินคดีทางอาญาและ/หรือ ทางแพ่งเพื่อเรียกค่าเสียหายเต็มจำนวนจากพนักงานที่กระทำความผิดดังกล่าว

ส่วนที่ 7 ทะเบียนควบคุมเอกสาร

ลำดับ	วันที่จัดทำ	รายละเอียดการดำเนินการ	วันที่บังคับใช้
01	15 มิถุนายน 2569	จัดทำเอกสารและอนุมัติประกาศใช้ครั้งแรก	10 สิงหาคม 2569