แนวปฏิบัติการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

(Information Security Guildline Policy)

บริษัท สหพัฒนาอินเตอร์โฮลดิ้ง จำกัด (มหาชน)

19 กันยายน 2568

SPI

สารบัญ

แนวปฏิบัติการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ
บริษัท สหพัฒนาอินเตอร์โฮลดิ้ง จำกัด (มหาชน)
(ฉบับปรับปรุง ครั้งที่ 3)

1. คำนำ

ระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทฯ เป็นระบบที่มีความสำคัญต่อการให้บริการกับกรรมการบริษัท ผู้บริหาร พนักงาน และรวมถึงบุคคลภายนอกซึ่งได้รับอนุญาต ดังนั้น เพื่อให้การดำเนินธุรกรรมด้วยวิธีการทางอิเล็กทรอนิกส์ การปฏิบัติงานและบริหารงานได้อย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยเชื่อถือได้ และสามารถดำเนินงานได้อย่างต่อเนื่อง บริษัทฯ จึงได้จัดทำนโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เพื่อเป็นแนวทางในการใช้งานเทคโนโลยีสารสนเทศ

2. วัตถุประสงค์

2.1 เพื่อให้การดำเนินงานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทฯ มีความมั่นคง ปลอดภัยสามารถใช้งานได้อย่างต่อเนื่องและมีประสิทธิภาพอันจะทำให้การดำเนินธุรกรรมมีความถูกต้อง เชื่อถือได้ตามมาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

2.2 เพื่อกำหนดแนวทางปฏิบัติให้ผู้บริหาร ผู้ดูแลระบบ และเจ้าหน้าที่ผู้ใช้งานระบบ ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย ในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทฯ

2.3 เพื่อป้องกันเจ้าหน้าที่ผู้ใช้งานและผู้เกี่ยวข้องไม่ให้กระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายอื่นๆ ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

3. กำหนดคำนิยาม

คำนิยามที่ใช้ในแนวปฏิบัตินี้ ประกอบด้วย

"บริษัทฯ" หมายถึง บริษัท สหพัฒนาอินเตอร์โฮลดิ้ง จำกัด (มหาชน)

"ผู้ใช้งาน" หมายถึง บุคคลที่ได้รับอนุญาต ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทฯ โดยมีสิทธิ์และหน้าที่ตามที่บริษัทฯ กำหนด

"ผู้บริหาร" หมายถึง ผู้บริหารของบริษัทฯ

"ผู้ดูแลระบบ" หมายถึง ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ หรือผู้ได้รับมอบหมายให้ควบคุม ดูแล บริหารจัดการระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทฯ

"เจ้าหน้าที่" หมายถึง บุคลากรในสังกัดบริษัทฯ

"สินทรัพย์" หมายถึง ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทฯ เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่บริษัทฯ ซื้อมา เพื่อใช้งานที่ถูกต้องตามกฎหมาย เป็นต้น

"การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายถึง การควบคุมและจำกัดสิทธิ์การใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทฯ ที่เกี่ยวกับการให้บริการและข้อมูลตามความจำเป็นในการใช้งาน มีการป้องกันการลักลอบการเข้าถึงระบบโดยผู้ที่ไม่มีสิทธิ์ทั้งจากภายในและภายนอกบริษัทฯ

"ความมั่นคงปลอดภัยด้านสารสนเทศ" หมายถึง การคงไว้ซึ่งความลับ ความถูกต้องสมบูรณ์ และความพร้อมใช้งานของข้อมูลในระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทฯ

"เหตุการณ์ด้านความมั่นคงปลอดภัย" (Security Incidents) หมายถึง เหตุการณ์ที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทฯ หรือเหตุการณ์ที่สงสัยว่าจะเป็นจุดอ่อน หรือสร้างความเสียหายได้ในที่สุด ซึ่งส่งผลให้เป็นการละเมิดนโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทฯ เช่น การอนุญาตให้ผู้อื่นเข้าใช้งานระบบแทนตนเอง การไม่กำหนดรหัสผ่านหรือใช้รหัสผ่านที่ไม่ปลอดภัยในการเข้าใช้งานระบบ การเปิดเผยเอกสารสำคัญให้บุคคลภายนอกรับรู้ การติดตั้งหรือใช้งานโปรแกรมที่ไม่พึงประสงค์ การถูกบุกรุกหรือโจมตีทางเครือข่าย หรือ การเปิดเผยข้อมูลสำคัญโดยไม่ได้รับอนุญาต เป็นต้น

"สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด" ได้แก่ สถานการณ์ที่ผู้ดูแลระบบไม่ต้องการให้เกิดขึ้นหรือสร้างความเสียหายกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทฯ โดยผู้ดูแลระบบไม่ได้คาดการณ์ไว้ว่าจะเกิดขึ้น เช่น โปรแกรมไม่พึงประสงค์ โปรแกรมทำงานผิดพลาดหรือไม่ถูกต้อง ระบบถูกบุกรุกทางเครือข่าย ข้อมูลสำคัญถูกเปลี่ยนแปลงหรือสูญหาย หน้าเว็บไซต์ถูกเปลี่ยนแปลง การเปิดเผยข้อมูลสำคัญโดยไม่ได้รับอนุญาต ระบบถูกโจมตีจนไม่สามารถให้บริการได้ การหยุดชะงักของระบบคอมพิวเตอร์และเครือข่าย หรือเหตุการณ์อื่นๆ ที่เป็นการละเมิดนโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

"ฝ่ายเทคโนโลยีสารสนเทศ" หมายถึง หน่วยงาน และ/หรือ ผู้รับผิดชอบ ที่มีหน้าที่ดำเนินการเกี่ยวกับระบบเทคโนโลยีสารสนเทศและระบบงานคอมพิวเตอร์และเป็นศูนย์กลางเครือข่ายข้อมูลสารสนเทศของบริษัทฯ ในการศึกษา วิเคราะห์เพื่อพัฒนาระบบเทคโนโลยีสารสนเทศและระบบงานคอมพิวเตอร์ของบริษัทฯ และปฏิบัติงานร่วมกัน หรือ สนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้อง

"ข้อมูลคอมพิวเตอร์" หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึง ข้อมูลอิเล็กทรอนิกส์ ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

"ศูนย์สารสนเทศ" หมายถึง ห้องเครื่องแม่ข่าย (Server Room) ห้องสำรองข้อมูล (Backup Room) ห้องควบคุม (Control Room) ห้องเครือข่าย (Network Room) และส่วนระบบปรับอากาศ

"ระบบคอมพิวเตอร์" หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือ ชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

"ระบบเครือข่ายสื่อสาร" หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสาร หรือ การเชื่อมโยง หรือ การส่งข้อมูลสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของบริษัทฯ ซึ่งการเชื่อมโยงเป็นได้ ทั้งในรูปแบบใช้สายและแบบไร้สาย โดยระบบเครือข่ายสื่อสาร ได้แก่ ระบบเครือข่ายระยะใกล้ (Local Area Network: LAN) ระบบเครือข่ายระยะไกล (Wide Area Network: WAN) ระบบอินทราเน็ต (Intranet) และ ระบบอินเทอร์เน็ต (Internet)

"ระบบเครือข่ายสื่อสารระยะใกล้" หมายถึง เครือข่ายที่เชื่อมโยงกันในพื้นที่ใกล้เคียงกัน

"ระบบเครือข่ายสื่อสารระยะไกล" หมายถึง เครือข่ายเชื่อมโยงกันในระยะทางที่ห่างไกล

"ระบบอินทราเน็ต" หมายถึง ระบบเครือข่ายสื่อสารภายในที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูล และสารสนเทศภายในบริษัทฯ

"ระบบอินเทอร์เน็ต" หมายถึง ระบบเครือข่ายสื่อสารที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ของบริษัทฯ เข้ากับระบบเครือข่ายสื่อสารอินเทอร์เน็ตทั่วโลก

"สารสนเทศ" หมายถึง ข้อมูลที่ผ่านการประมวลผล การจัดระเบียบ ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ

"ระบบเทคโนโลยีสารสนเทศและการสื่อสาร" หมายถึง ระบบงานของบริษัทฯ ที่ประกอบด้วย ระบบคอมพิวเตอร์ ระบบฐานข้อมูล ระบบเครือข่ายสื่อสาร เจ้าหน้าที่ผู้ใช้ระบบ เจ้าหน้าที่ผู้พัฒนาระบบ เจ้าหน้าที่ผู้จัดการดูแลระบบ และผู้บริหารของบริษัทฯ นำมาทำงานร่วมกัน เพื่อกำหนดวัตถุประสงค์ รวบรวมจัดเก็บข้อมูล ประมวลผลข้อมูล และส่งผลลัพธ์หรือสารสนเทศที่ได้ให้ผู้ใช้ระบบและผู้บริหารของบริษัทฯ สามารถนำมาใช้ประโยชน์ในการวางแผน เพื่อช่วยสนับสนุนการปฏิบัติงาน การตัดสินใจ การบริหาร การวิเคราะห์ และติดตามผลการดำเนินงานของหน่วยงานระดับต่างๆ ของบริษัทฯ

"รหัสผ่าน (Password)" หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบ ยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูล และระบบเทคโนโลยีสารสนเทศและการสื่อสาร

"การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ" หมายถึง การดำเนินการรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทฯ ประกอบด้วย คุณสมบัติพื้นฐาน 3 ประการ ดังนี้

(1) การรักษาความลับ (Confidentiality) คือ การเก็บรักษาข้อมูลไว้เป็นความลับและจะมีเพียงผู้มีสิทธิ์เท่านั้นที่จะสามารถเข้าถึงข้อมูลเหล่านั้นได้

(2) บูรณภาพ (Integrity) คือ การรับรองว่าข้อมูลจะไม่ถูกกระทำการใดๆ อันมีผลให้เกิดการเปลี่ยนแปลงหรือแก้ไขจากผู้ซึ่งไม่มีสิทธิ์ไม่ว่าการกระทำนั้นจะมีเจตนาหรือไม่ก็ตาม

(3) ความพร้อมใช้งาน (Availability) คือ การรับรองได้ว่าข้อมูลหรือระบบเทคโนโลยีสารสนเทศและการสื่อสารทั้งหลาย พร้อมที่จะให้บริการในเวลาที่ต้องการใช้งาน

"ชุดคำสั่งไม่พึงประสงค์" (Malware) หมายถึง ชุดคำสั่งที่มีผลทำให้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร เกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

"จดหมายอิเล็กทรอนิกส์" (E-Mail) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายสื่อสารที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ เช่น SMTP, POP3 หรือ IMAP

"ผู้ใช้งานระบบ หรือ บัญชีผู้ใช้ที่มีสิทธิ์การเข้าถึงระดับสูงสุด Highest Privilege Users" หมายถึง ผู้ใช้งานระบบ หรือบัญชีผู้ใช้ที่มีสิทธิ์การเข้าถึงระดับสูงสุดภายในระบบเทคโนโลยีสารสนเทศ เครือข่าย หรือ แอปพลิเคชั่นหนึ่งๆ ซึ่งสามารถกระทำการสำคัญที่มีผลกระทบอย่างมากต่อความมั่นคง ความพร้อมใช้งาน และความลับของระบบได้

"ระบบ Help Desk" หมายถึง ระบบเทคโนโลยีสารสนเทศที่ใช้ในการรับเรื่อง แจ้งปัญหา ขอความช่วยเหลือ หรือ ร้องขอบริการด้านสารสนเทศจากผู้ใช้งานภายในบริษัทฯ โดยมีการจัดการติดตามสถานะ การมอบหมายงาน การตอบกลับ และการปิดงานอย่างเป็นระบบ เพื่อให้สามารถให้บริการผู้ใช้งานได้อย่างมีประสิทธิภาพ โปร่งใส และตรวจสอบได้

"ปัญญาประดิษฐ์" (Artificial Intelligence: AI) หมายถึง เทคโนโลยีที่สามารถจำลองกระบวนการคิดของมนุษย์ เช่น การเรียนรู้ การตัดสินใจ การสร้างเนื้อหา เป็นต้น

"เครื่องมือ AI สาธารณะ" หมายถึง ระบบ AI ที่เปิดให้บุคคลทั่วไปใช้งาน เช่น ChatGPT, Google Gemini, Copilot เป็นต้น

"ข้อมูลอ่อนไหว (Sensitive Data)" หมายถึง ข้อมูลที่เป็นความลับทางธุรกิจ ข้อมูลลูกค้า ข้อมูลส่วนบุคคล ฯลฯ

"ข้อมูลส่วนบุคคลที่สามารถระบุตัวตนได้" (Personally Identifiable Information: PII) หมายถึง ข้อมูลที่ใช้ระบุตัวบุคคลใดบุคคลหนึ่งได้ ซึ่งรวมถึงข้อมูลที่สามารถระบุตัวบุคคลได้ไม่ว่าจะใช้เพียงข้อมูลเดียวหรือเมื่อใช้ร่วมกับข้อมูลอื่น ตัวอย่างเช่น ชื่อ ที่อยู่ หมายเลขโทรศัพท์ ที่อยู่อีเมล หมายเลขประกันสังคม หมายเลขหนังสือเดินทาง หมายเลขใบขับขี่ บัตรประจำตัวที่ออกโดยรัฐบาล (หมายเลขประจำตัวผู้เสียภาษี) วันเกิด เชื้อชาติ สถานที่เกิด เป็นต้น

"การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร" (Information and Communication Technology Risk Assessment) หมายถึง กระบวนการวิเคราะห์ ตรวจสอบ และประเมินความเสี่ยง ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของบริษัทฯ เช่น ความเสี่ยงจากการโจมตีทางไซเบอร์ ความล้มเหลวของระบบเครือข่าย การรั่วไหลของข้อมูล หรือ การหยุดชะงักของบริการทางเทคโนโลยีสารสนเทศเพื่อหาแนวทางในการจัดการและลดผลกระทบที่อาจเกิดขึ้น

"ที่อยู่อินเทอร์เน็ตโปรโตคอล" (Internet Protocol Address: IP Address) หมายถึง หมายเลขประจำอุปกรณ์ในระบบเครือข่ายที่ใช้ระบุและสื่อสารระหว่างอุปกรณ์ต่างๆ ทั้งภายในและภายนอกองค์กร โดยอยู่ภายใต้การควบคุมของฝ่ายเทคโนโลยีสารสนเทศ

4. โครงสร้างด้านความปลอดภัยเทคโนโลยีสารสนเทศ

เพื่อให้มีการกำหนดกรอบการบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศของบริษัทฯ ตั้งแต่เริ่มต้น รวมถึงการควบคุมการปฏิบัติงานเพื่อให้มีความมั่นคงปลอดภัย บริษัทฯ จึงได้กำหนดผู้เกี่ยวข้องและหน้าที่ในการบริหารจัดการความปลอดภัยของสารสนเทศของบริษัทฯ ดังนี้

4.1 ฝ่ายเทคโนโลยีสารสนเทศ

(1) กำหนดแผน เป้าหมาย และระเบียบปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทฯ โดยครอบคลุมถึงงบประมาณ และจำนวนบุคลากร ให้สอดคล้องกับแผนกลยุทธ์ของบริษัทฯ

(2) จัดการพัฒนาระเบียบปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ซึ่งหมายรวมถึง นโยบาย มาตรฐาน แนวปฏิบัติ และคู่มือ เพื่อการดำเนินงานการรักษาความลับของข้อมูล (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และความมั่นคงของระบบ (Availability)

(3) การบริหารความเสี่ยง และการวิเคราะห์ความเสี่ยงที่อาจทำให้ระบบเกิดปัญหา กระทบกับการดำเนินธุรกิจของบริษัทฯ

(4) มีการกำกับดูแลระบบเทคโนโลยีสารสนเทศที่มั่นใจได้ว่า มีมาตรการที่วางไว้สามารถดำเนินการได้อย่างมีประสิทธิภาพ และมีการบริหารเฝ้าระวังการโจมตีระบบและภัยต่างๆ ที่อาจเกิดขึ้นกับระบบ รวมทั้งวางแผนบริหารความต่อเนื่องทางธุรกิจเพื่อกู้ระบบยามฉุกเฉิน

(5) เตรียมพร้อมรับสถานการณ์และเรียนรู้เทคนิคใหม่ๆ ทางด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ

(6) ประเมินความต้องการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศ ความคุ้มค่ารวมทั้งจัดหาและพัฒนาระบบเทคโนโลยีสารสนเทศให้สอดคล้องกับกลยุทธ์ของบริษัทฯ

(7) ดูแลทรัพยากรด้านเทคโนโลยีสารสนเทศของบริษัทฯ ให้สามารถสนับสนุนการปฏิบัติงานภายในอย่างมีประสิทธิภาพ

4.2 หน่วยงานภายใน หมายถึง พนักงานทุกคนของบริษัทฯ ที่มีส่วนเกี่ยวข้องกับสารสนเทศไม่ว่าทางใดทางหนึ่ง

(1) ปฏิบัติตามระเบียบปฏิบัติความปลอดภัยสารสนเทศอย่างเคร่งครัด

(2) รักษาความลับของข้อมูล สารสนเทศของบริษัทฯ และไม่เปิดเผยรหัสผ่านเข้าใช้ระบบของตนเอง

(3) รายงานเหตุการณ์ละเมิดความปลอดภัยสารสนเทศ และปัญหาทางด้านความปลอดภัยเมื่อเกิดเหตุการณ์ดังกล่าวให้กับหน่วยงานด้านเทคโนโลยีสารสนเทศ

(4) ใช้งานข้อมูล และทรัพย์สินทางข้อมูลของบริษัทฯ อย่างรับผิดชอบ และใช้ข้อมูลสำหรับงานที่ตนเองรับผิดชอบ หรือได้รับอนุญาตเท่านั้น

4.3 หน่วยงานภายนอก หมายถึง บุคคลภายนอกที่เข้ามาปฏิบัติงานในบริษัทฯ หรือทำงานให้กับบริษัทฯ ซึ่งมีส่วนเกี่ยวข้องในการใช้ข้อมูลหรือทรัพย์สินสารสนเทศอื่นของบริษัทฯ เช่น ผู้ให้บริการ/ผู้จำหน่าย ระบบคู่สัญญาหรือผู้ที่ได้รับอนุญาตโดย

(1) ปฏิบัติตามระเบียบปฏิบัติความปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างเคร่งครัด

(2) รักษาความลับของข้อมูล สารสนเทศของบริษัทฯ และไม่เปิดเผยรหัสผ่านเข้าใช้ระบบของตนเอง

(3) รายงานเหตุการณ์ละเมิดความปลอดภัยสารสนเทศ และปัญหาทางด้านความปลอดภัยเมื่อเกิดเหตุการณ์ดังกล่าวให้กับหน่วยงานด้านเทคโนโลยีสารสนเทศ

(4) ใช้งานข้อมูล และทรัพย์สินทางข้อมูลของบริษัทฯ อย่างรับผิดชอบ และใช้ข้อมูลสำหรับงานที่ตนเองรับผิดชอบ หรือได้รับอนุญาตเท่านั้น

5. **แนวปฏิบัติในการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ**

แนวปฏิบัติในการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ แบ่งออกเป็น 11 หมวด ดังนี้

หมวดที่ 1 การเข้าถึงและการควบคุมการใช้งานสารสนเทศและระบบเทคโนโลยีสารสนเทศและการสื่อสาร

เพื่อป้องกันไม่ให้บุคคลที่ไม่ได้รับอนุญาตเข้าถึงข้อมูล ระบบ หรือทรัพยากรทางเทคโนโลยี ซึ่งครอบคลุมทั้งด้านเทคนิคและการบริหารจัดการ

1.1 การควบคุมการเข้าถึงสิทธิ์ของผู้ใช้งาน

(1) มีการกำหนดสิทธิ์ของผู้ใช้งานในการเข้าถึงระบบ โดยพิจารณาจากหน้าที่ความรับผิดชอบในการเข้าถึงและการใช้งานข้อมูลของผู้ใช้งานแต่ละกลุ่มงาน

(2) ผู้ใช้งานต้องบันทึกคำร้องในระบบ Help Desk ทำหนังสือขอมีสิทธิ์เป็นลายลักษณ์อักษรให้กับฝ่ายเทคโนโลยีสารสนเทศ หรือหน่วยงานที่ได้รับมอบหมาย

(3) ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมาย เป็นผู้พิจารณาอนุญาต โดยให้ปฏิบัติตามระเบียบปฏิบัติงาน เรื่อง การขอรับบริการจากฝ่ายเทคโนโลยีสารสนเทศ (SOP-IT-01)

1.2 การบริหารจัดการสิทธิ์ผู้ใช้งาน

(1) ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ได้กำหนดสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารนั้นๆ ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้งาน และหน้าที่ความรับผิดชอบของผู้ใช้งานเป็นไปตามระเบียบที่บริษัทฯ กำหนด และทบทวนสิทธิ์อย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง หรือในกรณีฝ่ายทรัพยากรบุคคลมีการแจ้งย้าย/เปลี่ยนตำแหน่งงานใหม่/ออกจากงาน/เกษียณ หรือในกรณีที่หน่วยงานต้นสังกัด ยื่นทำขอต่อฝ่ายเทคโนโลยีสารสนเทศเพื่อให้มีสิทธิ์หรือยกเลิกสิทธิ์ต่างๆ ในการใช้งานอนุญาต โดยให้ปฏิบัติตามระเบียบปฏิบัติงาน เรื่อง การขอรับบริการจากฝ่ายเทคโนโลยีสารสนเทศ (SOP-IT-01)

(2) ผู้ดูแลระบบต้องกำหนดสิทธิ์บัญชีรายชื่อผู้ใช้งานรายใหม่และรหัสผ่าน สำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

(3) เมื่อเจ้าหน้าที่ออกจากงาน หรือเปลี่ยนแปลงหน้าที่ความรับผิดชอบในระบบที่ขอสิทธิ์การใช้งาน ให้ฝ่ายพัฒนาองค์กรและบุคลากร แจ้งฝ่ายเทคโนโลยีสารสนเทศ และฝ่ายบริหารสำนักงาน โดยทันที ผ่านระบบบริหารงานบุคคล เพื่อถอดถอนสิทธิ์ของผู้ที่ออกจากงานหรือเปลี่ยนสิทธิ์ในระบบทันทีที่ได้รับแจ้ง

(4) กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งาน ต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิ์พิเศษนั้นอย่างรัดกุมเพียงพอ โดยควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว และมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัดทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานต้องเปลี่ยนรหัสผ่านทุก 3 เดือน และต้องได้รับความเห็นชอบและอนุมัติจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศหรือผู้ได้รับมอบหมาย

(5) ห้ามผู้ใช้งานซึ่งไม่ได้รับสิทธิ์ให้เข้าใช้งาน บุกรุกเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารไม่ว่าด้วยวิธีการใด

1.3 การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานระบบที่สำคัญของบริษัทฯ

(1) ผู้ดูแลระบบมีการกำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งาน หรือใช้ระบบการกำหนดรหัสผ่านอัตโนมัติ และระบบต้องไม่แสดงรหัสผ่านให้เห็นบนหน้าจอ

(2) ระบบต้องกำหนดให้ผู้ใช้งานต้องเปลี่ยนรหัสผ่านเมื่อเข้าระบบครั้งแรก

(3) ผู้ดูแลระบบมีการกำหนดระยะเวลาการเปลี่ยนรหัสผ่าน โดยกำหนดให้ระบบมีการบันทึกประวัติการเปลี่ยนรหัสผ่าน เพื่อป้องกันการใช้รหัสซ้ำ เช่น ระบบงาน SAP ในบริษัทฯ ต้องเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ 90 วัน

(4) การแจ้งปัญหาการใช้งานชื่อผู้ใช้งานและรหัสผ่าน ให้ผู้ใช้งานติดต่อผู้ดูแลระบบ เช่น ลืมชื่อผู้ใช้งาน หรือรหัสผ่าน เป็นต้น

1.4 การใช้งานรหัสผ่านสำหรับผู้ใช้งาน

(1) ผู้ใช้ต้องใช้ชื่อผู้ใช้งาน และรหัสผ่านของตนเองในการใช้งานระบบ เพื่อป้องกันการปฏิเสธความรับผิดชอบ

(2) ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรกหรือได้รับรหัสผ่านใหม่ ต้องเปลี่ยนรหัสผ่านที่ได้รับโดยทันที

(3) ผู้ใช้งานต้องกำหนดรหัสผ่าน และเปลี่ยนรหัสผ่านของตนเองในการใช้งาน อย่างน้อยทุกๆ 90 วัน หรือตามหลักเกณฑ์ซึ่งผู้ดูแลระบบกำหนด และต้องยินยอมให้ผู้ดูแลระบบดำเนินการใดๆ เพื่อให้เกิดความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร

(4) ผู้ใช้งานต้องเก็บรักษารหัสผ่านให้เป็นความลับ และระมัดระวังป้องกันรหัสผ่านของตนเองในการใช้งานไม่ให้รั่วไหลไปยังผู้อื่น และไม่มอบให้ผู้อื่นนำไปใช้ไม่ว่าด้วยเหตุใดๆ ทั้งสิ้น เว้นแต่กรณีผู้ใช้งานที่มีอำนาจอนุมัติใดๆ ในระบบเทคโนโลยีสารสนเทศและการสื่อสารไม่สามารถปฏิบัติงานอันจะเป็นเหตุให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารไม่สามารถดำเนินการต่อไปได้ ให้แต่งตั้งผู้ปฏิบัติงานแทนในช่วงเวลาดังกล่าว เพื่อใช้เป็นหลักฐานในการตรวจสอบการใช้สิทธิ์ และหลังจากผู้ปฏิบัติงานแทนดำเนินการเรียบร้อยแล้ว ให้ผู้ใช้งานซึ่งเป็นเจ้าของรหัสผ่านทำการเปลี่ยนรหัสผ่านโดยทันที

(5) กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ 8 ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

(6) ไม่กำหนดรหัสผ่านอย่างเป็นแบบแผน เช่น “abcdef” “aaaaaa” “123456”

(7) ไม่กำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน เช่น ชื่อสกุล วัน เดือน ปีเกิด ที่อยู่

(8) ไม่กำหนดรหัสผ่านเป็นคำศัพท์ที่อยู่ในพจนานุกรม

(9) ผู้ใช้งานต้องออกจากระบบ (Log off) ทันที เมื่อไม่ใช้งาน เพื่อป้องกันผู้ใช้งานอื่นลักลอบใช้สิทธิ์ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร

1.5 การบริหารจัดการการเข้าถึงของผู้ใช้งาน

(1) ผู้ใช้งานต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงาน

(2) เจ้าของข้อมูล และ/หรือ เจ้าของระบบงาน จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่เกี่ยวข้องกับหน้าที่และความรับผิดชอบ

(3) ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติ และกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้งานในการขออนุญาตเข้าระบบงานนั้น ต้องบันทึกข้อมูลตามที่ฝ่ายเทคโนโลยีสารสนเทศกำหนด และให้มีการลงนามอนุมัติเอกสารดังกล่าวโดยผู้มีอำนาจที่เป็นเจ้าของข้อมูล และ/หรือ เจ้าของระบบงาน เพื่อเก็บไว้เป็นหลักฐาน

(4) การลงทะเบียน เจ้าหน้าที่กำหนดให้มีขั้นตอนปฏิบัติสำหรับการลงทะเบียนเจ้าหน้าที่ใหม่ หรือเมื่อย้าย/เปลี่ยนตำแหน่งงานใหม่/ออกจากงาน/เกษียณ ภายในบริษัทฯ หน่วยงาน/ผู้ใช้งานต้องทำบันทึก และบันทึกคำร้องในระบบตามที่ฝ่ายเทคโนโลยีสารสนเทศกำหนด เพื่อให้มีสิทธิ์หรือยกเลิกสิทธิ์ต่างๆ ในการใช้งาน โดยให้ปฏิบัติตามระเบียบปฏิบัติงาน เรื่อง การขอรับบริการจากฝ่ายเทคโนโลยีสารสนเทศ (SOP-IT-01)

1) ผู้ใช้งานรายใหม่ ต้องทำการบันทึกข้อมูลเพื่อลงทะเบียน ในระบบบริหารบุคคล และในระบบ (Help Desk)

2) ระบบ Help Desk การขอคำร้องในระบบ **“ขอปรับปรุงระบบเทคโนโลยีสารสนเทศ และขออนุญาตเข้าใช้ ระบบ SAP”** ที่ผู้ใช้งานรายใหม่ได้ทำการแจ้ง ต้องได้รับการอนุมัติ จากผู้บังคับบัญชาของผู้ขอคำร้องและผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

3) ผู้ดูแลระบบจะกำหนดสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารในส่วนที่เกี่ยวข้องกับหน้าที่และความรับผิดชอบของผู้ใช้งาน โดยได้รับความเห็นชอบจากผู้มีอำนาจ และทบทวนสิทธิ์อย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง หรือในกรณีฝ่ายทรัพยากรบุคคลมีการแจ้งย้าย/เปลี่ยนตำแหน่งงานใหม่/ออกจากงาน/เกษียณ หรือในกรณีที่หน่วยงานต้นสังกัด ยื่นทำขอต่อฝ่ายเทคโนโลยีสารสนเทศเพื่อให้มีสิทธิ์หรือยกเลิกสิทธิ์ต่างๆ ในการใช้งาน

(5) การจัดเก็บรักษาชื่อผู้ใช้และรหัสผ่านบัญชีผู้ใช้งานที่มีสิทธิ์สูงสุด (Highest Privilege Users)

1) ผู้ดูแลระบบจัดเก็บชื่อผู้ใช้และรหัสผ่านในซองปิดผนึกในที่ปลอดภัย

2) ผู้ดูแลระบบทำการบันทึกประวัติการเปิดซองทุกครั้ง

3) ซองชื่อผู้ใช้และรหัสผ่านจะถูกเปิดใช้งานได้ในกรณีฉุกเฉินเท่านั้น

4) ผู้ดูแลระบบจะต้องมีการตรวจสอบบัญชีผู้ใช้งานที่มีสิทธิ์สูงสุดอย่างสม่ำเสมอ เพื่อตรวจสอบบัญชีผู้ใช้งานที่มีสิทธิ์สูงสุดให้สามารถเข้าใช้งานได้ตามปกติ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลง

1.6 การควบคุมการเข้าถึงระบบเครือข่ายสื่อสาร

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

(1) ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบเทคโนโลยีสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(2) เจ้าหน้าที่ผู้รับผิดชอบต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายสื่อสารในระบบจัดการทรัพย์สินสารสนเทศบริษัทฯ

(3) ผู้ดูแลระบบต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายสื่อสารในส่วนที่เกี่ยวข้องกับหน้าที่และความรับผิดชอบของผู้ใช้งาน ในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายสื่อสาร

(4) ผู้ดูแลระบบจัดให้มีซอฟท์แวร์สำหรับบริหารจัดการและควบคุมระบบเครือข่าย (Network Management System) ซึ่งสามารถระบุอุปกรณ์บนเครือข่าย (Equipment Identification) ถึงระดับ IP Address, Computer Name, MAC Address และสามารถสร้างผังการเชื่อมโยงเครือข่าย (Network Diagram)

(5) ผู้ดูแลระบบมีการจัดทำผังการเชื่อมโยงเครือข่าย และมีการปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(6) ผู้ดูแลระบบมีการบริหารจัดการเครือข่ายสื่อสาร ดังนี้

1) มีการแบ่งแยกเครือข่ายสื่อสารเป็นเครือข่ายสื่อสารภายใน เครือข่ายสื่อสารภายนอกและเครือข่ายสื่อสารแบบไร้สาย

2) มีการจัดแบ่งแยกส่วนเครือข่ายสื่อสาร/กลุ่ม เพื่อป้องกันและควบคุมการเข้าถึง ได้แก่ ส่วนที่เป็นสาธารณะ ส่วนที่เชื่อมต่อภายใน ส่วนที่เกี่ยวข้องกับสินทรัพย์สำคัญหรือที่เป็นอันตรายกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบเทคโนโลยีสารสนเทศ

3) มีการติดตั้งอุปกรณ์ Gateway กั้นไว้ระหว่างเครือข่ายสื่อสาร เพื่อเป็นตัวควบคุมข้อมูลที่สื่อสารกันระหว่างเครือข่ายสื่อสาร

4) อุปกรณ์ในเครือข่ายสื่อสารมีการปรับแต่งให้สามารถควบคุมหรือกรองข้อมูลที่สื่อสารกันระหว่างเครือข่าย

(7) ผู้ดูแลระบบมีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายอื่นๆ ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ โดยสามารถตรวจสอบข้อมูลย้อนหลังได้ภายใน 1 ปี

(8) ผู้ดูแลระบบมีการสำรองข้อมูลการตั้งค่าของอุปกรณ์เครือข่ายสื่อสาร

1.7 การควบคุมการเข้าถึงระบบปฏิบัติการ

เป็นการควบคุมบุคคลเข้าสู่ระบบปฏิบัติการที่อยู่ภายใต้ระบบเครือข่ายสื่อสารของบริษัทฯ เพื่อรักษาความปลอดภัยของข้อมูล และทรัพยากร จึงต้องมีการกำหนดมาตรการรักษาความปลอดภัย

(1) การติดตั้งโปรแกรมอรรถประโยชน์ (Utility Program/Software) เพื่อใช้งานร่วมกับระบบปฏิบัติการ

1) ต้องไม่ติดตั้งโปรแกรมซอฟต์แวร์ที่ละเมิดลิขสิทธิ์

2) ต้องติดตั้งโปรแกรมตามภารกิจและไม่ติดตั้งโปรแกรมที่ไม่เกี่ยวข้องกับการปฏิบัติงาน

3) ต้องติดโปรแกรมต้องติดตั้งโปรแกรมตามที่ฝ่ายเทคโนโลยีสารสนเทศกำหนดเท่านั้น ตามระเบียบปฏิบัติงาน เรื่อง การติดตั้งโปรแกรมและจัดซื้อคอมพิวเตอร์พื้นฐาน (SOP-IT-03) ของฝ่ายเทคโนโลยีสารสนเทศ หากนอกจากมาตรฐานที่ฝ่ายเทคโนโลยีสารสนเทศกำหนด ให้บันทึกคำร้องในระบบ Help Desk และต้องได้รับอนุมัติจากผู้บังคับบัญชา ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศหรือผู้มีอำนาจอนุมัติ

(2) ฝ่ายเทคโนโลยีสารสนเทศ กำหนดมาตรการจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Limitation of Connection Time) สำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรือแอปพลิเคชัน (Application) ที่มีความเสี่ยง หรือมีความสำคัญสูง เพื่อให้มีความมั่นคงปลอดภัย โดยผู้ใช้งานสามารถใช้งานได้นานที่สุด 30 นาทีต่อการเชื่อมต่อ 1 ครั้ง เฉพาะในช่วงเวลาทำการของหน่วยงานเท่านั้น

1.8 การเข้ารหัสข้อมูล (Cryptography)

เพื่อให้มีการเข้ารหัสข้อมูลอย่างเหมาะสมและได้ผล และเพื่อป้องการความลับ การปลอมแปลง หรือความถูกต้องของสารสนเทศ

(1) บริษัทฯ ต้องจัดให้มีนโยบายควบคุมการใช้งานระบบการเข้ารหัสข้อมูล ที่คำนึงถึงชนิด และ ขั้นตอนวิธีการเข้ารหัสข้อมูล (Algorithm) ที่สอดคล้องเหมาะสมกับระดับความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลที่เป็นความลับหรือมีความสำคัญ รวมทั้งกำหนดผู้รับผิดชอบในการดำเนินนโยบายและบริหารจัดการกุญแจเพื่อการเข้ารหัสข้อมูล (Key Management)

(2) บริษัทฯ ต้องจัดให้มีนโยบายการบริหารกุญแจเพื่อการเข้ารหัสข้อมูล ตลอดช่วงเวลาการใช้งาน (Key Management Whole Life Cycle) โดยกำหนดแนวปฏิบัติเพื่อการคัดเลือกวิธีการเข้ารหัส การกำหนด ความยาวของรหัส การใช้งานและการยกเลิกการใช้งานกุญแจเพื่อการเข้ารหัส กระบวนการบริหารจัดการ กุญแจเพื่อการเข้ารหัส รวมทั้งติดตามให้มีการปฏิบัติให้เป็นไปตามนโยบายและแนวทางปฏิบัติดังกล่าว อย่างสม่ำเสมอ

หมวดที่ 2 การควบคุมการเข้า-ออก ศูนย์สารสนเทศ

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

(1) มีขั้นตอนการขออนุญาต การกำหนดสิทธิ์ และควบคุมการเข้าศูนย์สารสนเทศ และพื้นที่สำคัญภายในศูนย์สารสนเทศ

(2) มีระบบการบันทึกวันและเวลาการเข้า-ออกพื้นที่ในศูนย์สารสนเทศโดยอัตโนมัติเกี่ยวกับตัวบุคคลและเวลาที่ผ่านเข้า-ออก เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

(3) มีการควบคุมการเข้าออกศูนย์สารสนเทศ และพื้นที่สำคัญภายในศูนย์สารสนเทศ ด้วยการใช้บัตรประจำตัวและลายนิ้วมือ หรือใช้บัตรประจำตัวและรหัสผ่าน เพื่อพิสูจน์ตัวตนของผู้มีสิทธิ์

(4) มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานในศูนย์สารสนเทศ จนกระทั่งเสร็จสิ้นภารกิจ เพื่อป้องกันการสูญหายของทรัพย์สิน หรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

(5) ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญในศูนย์สารสนเทศ

หมวดที่ 3 การใช้งานเครื่องคอมพิวเตอร์

การรักษาความมั่นคงปลอดภัยในการใช้งานเครื่องคอมพิวเตอร์ เป็นส่วนสำคัญของการรักษาความมั่นคงปลอดภัยสารสนเทศในบริษัทฯ โดยมีแนวปฏิบัติที่ควรดำเนินการ ดังนี้

3.1 การใช้งานของผู้ใช้งาน

(1) ให้มีการกำหนดรหัสผ่าน เปลี่ยนรหัสผ่านและเก็บรักษารหัสผ่าน เป็นไปตาม ข้อ 4.1 การใช้งานรหัสผ่านสำหรับผู้ใช้งาน

(2) ให้ผู้ใช้งานออกจากระบบ (Log off) ทันทีในกรณีที่ไม่ใช้ระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันบุคคลอื่นมาใช้ระบบต่อเนื่อง และหากสงสัยว่ารหัสผ่านเกิดการรั่วไหล ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันที

(3) ผู้ไม่ได้รับสิทธิ์ให้เข้าใช้งาน ห้ามบุกรุกเข้าใช้งานระบบเทคโนโลยีสารสนเทศไม่ว่าด้วยวิธีการใดๆ

(4) ห้ามติดตั้งซอฟต์แวร์ หรือโปรแกรมอื่นใดลงบนเครื่องคอมพิวเตอร์ที่ใช้ปฏิบัติงาน หรือติดตั้งอุปกรณ์เชื่อมโยงเครือข่ายเพิ่มเติม หรือเชื่อมโยงเครือข่ายคอมพิวเตอร์ที่ใช้ปฏิบัติงานกับเครือข่ายอื่นนอกจากเครือข่ายของบริษัทฯ หรือนำเครื่องคอมพิวเตอร์ส่วนตัวมาใช้งานกับระบบเทคโนโลยีสารสนเทศ เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

(5) ไม่เปิดให้มีการแชร์ไฟล์ในเครื่องคอมพิวเตอร์ที่ใช้ปฏิบัติงาน เว้นแต่ในกรณีที่เป็นระบบงานที่บริษัทฯ กำหนดไว้ หากมีความจำเป็นให้กำหนดระยะเวลาเท่าที่ใช้งานและยกเลิกการแชร์ไฟล์ทันทีที่ใช้งานเสร็จ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบคอมพิวเตอร์และข้อมูล

(6) ไม่ดาวน์โหลด (Download) ข้อมูลหรือโปรแกรมที่ไม่เกี่ยวข้องกับการปฏิบัติงาน หรือ จากเว็บไซต์ซึ่งไม่น่าเชื่อถือ หรือไม่มั่นใจว่าจะปลอดภัย

หมวดที่ 4 การใช้งานอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์

การรักษาความมั่นคงปลอดภัยในการใช้งานอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์ (Internet & Email Security) เป็นเรื่องสำคัญมาก เนื่องจากเป็นช่องทางหลักที่ผู้ไม่ประสงค์ดีใช้โจมตีและหลอกลวงผู้ใช้งาน โดยสามารถแบ่งแนวปฏิบัติได้ ดังนี้

4.1 การใช้งานอินเทอร์เน็ต

(1) ผู้ใช้งานต้องไม่ใช้ระบบอินเทอร์เน็ตเพื่อวัตถุประสงค์ที่ไม่เกี่ยวข้องกับการปฏิบัติงาน เช่น การใช้งานข้อมูลมัลติมีเดีย การดาวน์โหลดไฟล์ที่ไม่เกี่ยวข้องกับงาน หรือ การกระทำใด ๆ ที่ส่งผลให้สิ้นเปลืองหรือยึดครองช่องสัญญาณการสื่อสารข้อมูลเกินความจำเป็น

(2) ให้ผู้ดูแลระบบ กำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์ เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัย เช่น Proxy, Firewall, IPS, IDS, IPS, Anti-Virus เป็นต้น

(3) เครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์แบบพกพา และอุปกรณ์คอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่อระบบอินเทอร์เน็ตผ่านเว็บบราวเซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการปิดช่องโหว่ของระบบปฏิบัติการที่เว็บบราวเซอร์ติดตั้งอยู่

(4) ผู้ใช้งานต้องไม่ใช้งานอินเทอร์เน็ตของบริษัทฯ เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว หรือการเข้าใช้เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม

(5) ผู้ใช้งานจะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของบริษัทฯ โดยผ่านความเห็นชอบจากผู้ดูแลระบบ

(6) ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของบริษัทฯ ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

(7) ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

(8) ผู้ใช้งานต้องปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ อย่างเคร่งครัด

4.2 การใช้งานจดหมายอิเล็กทรอนิกส์

(1) ผู้ใช้งานต้องลงทะเบียนเป็นผู้ได้รับสิทธิ์การใช้และรหัสผ่าน เพื่อเป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคลในการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของบริษัทฯ ซึ่งผู้ใช้งานแต่ละคนจะต้องดูแลรักษาสิทธิ์การใช้งานและรหัสผ่านของตนเองไม่ให้ผู้อื่นนำไปใช้งานได้ หากมีการกระทำใดซึ่งเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เจ้าของสิทธิ์ต้องรับผิดชอบผลจากความเสียหายที่เกิดขึ้นโดยไม่อาจปฏิเสธได้

(2) ผู้ใช้งานต้องใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทฯ ในการรับ-ส่งจดหมายอิเล็กทรอนิกส์ซึ่งเกี่ยวกับการปฏิบัติงาน

(3) ผู้ใช้งานต้องระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อบริษัทฯ สร้างความน่ารำคาญต่อผู้อื่น หรือขัดต่อศีลธรรม และไม่แสวงหาประโยชน์จากการใช้จดหมายอิเล็กทรอนิกส์ของบริษัทฯ

(4) ผู้ใช้งานต้องออกจากระบบจดหมายอิเล็กทรอนิกส์ทันทีหลังจากการเลิกใช้งาน เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

(5) ผู้ใช้งานต้องตรวจสอบความน่าเชื่อถือของผู้ส่งทุกครั้ง ก่อนเปิดไฟล์แนบจากจดหมายอิเล็กทรอนิกส์

(6) ผู้ใช้งานไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

(7) ผู้ใช้งานควรตรวจสอบกล่องจดหมายอิเล็กทรอนิกส์ของตนเป็นประจำทุกวัน เพื่อไม่ให้พลาดข้อมูลสำคัญที่เกี่ยวข้องกับการปฏิบัติงาน และเพื่อความเป็นระเบียบเรียบร้อย ผู้ใช้งานควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ให้เหลือเท่าที่จำเป็น โดยควรดำเนินการ Archive จดหมายหรือแฟ้มข้อมูลที่ไม่ใช้งานแล้วอย่างสม่ำเสมอ เพื่อลดปริมาณข้อมูลที่ไม่จำเป็น และช่วยให้สามารถค้นหาอีเมลที่ต้องการได้อย่างรวดเร็ว รวมถึงสนับสนุนการบริหารจัดการพื้นที่จัดเก็บของระบบอีเมลอย่างมีประสิทธิภาพ

(8) ผู้ใช้งานต้องสำรองข้อมูลที่มีความสำคัญในจดหมายอิเล็กทรอนิกส์อย่างสม่ำเสมอ

หมวดที่ 5 การบริหารจัดการสินทรัพย์และเครือข่าย

แนวปฏิบัติในการ รักษาความมั่นคงปลอดภัยด้านการบริหารจัดการสินทรัพย์และเครือข่าย 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 ต่างๆ ของโปรแกรมระบบอย่างชัดเจน

3) มีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบการรักษาความปลอดภัยระบบคอมพิวเตอร์

4) ในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่า Parameter ในลักษณะที่ผิดปกติ จะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานผู้ดูแลรับผิดชอบโดยทันที

5) เปิดใช้บริการ (Service) เท่าที่จำเป็น ทั้งนี้ หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบการรักษาความปลอดภัย ต้องมีมาตรการเพิ่มเติม

6) มีการติดตั้ง Patch ที่จำเป็นของระบบงานสำคัญ เพื่อปิดช่องโหว่ต่างๆ ของโปรแกรมระบบ (System Software) เช่น ระบบปฏิบัติการ DBMS และ Web Server อย่างสม่ำเสมอ

7) ทดสอบ System Software เกี่ยวกับการรักษาความปลอดภัย และประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้ง และหลังจากการแก้ไขหรือบำรุงรักษา

(3) บำรุงรักษาอุปกรณ์ ในระบบคอมพิวเตอร์ให้สามารถทำงานได้อย่างมีประสิทธิภาพ โดยควบคุมดูแลให้มีการบำรุงรักษาอุปกรณ์ในระบบคอมพิวเตอร์ตามระยะเวลาที่กำหนด

5.2 การบริหารจัดการโปรแกรม

(1) จัดทำทะเบียนคุมโปรแกรม

(2) มีการติดตั้งโปรแกรมที่ถูกต้องตามลิขสิทธิ์หรือโปรแกรมสำหรับใช้งานฟรี (Freeware, Open Source) และติดตั้งเท่าที่จำเป็นต่อการใช้งาน โดยให้ปฏิบัติตามระเบียบปฏิบัติงาน เรื่อง การติดตั้งโปรแกรมและจัดซื้อคอมพิวเตอร์พื้นฐาน (SOP-IT-03)

5.3 การบริหารจัดการระบบเครือข่ายสื่อสาร

(1) มีการจัดแบ่งแยกส่วนเครือข่าย/กลุ่ม (VLAN / Zone)

(2) จัดทำทะเบียนคุมการใช้งานระบบเครือข่ายสื่อสาร

(3) จัดทำแผนผังและขอบเขตของระบบเครือข่ายสื่อสาร

(4) ตรวจสอบการใช้งานระบบเครือข่ายสื่อสารให้สามารถใช้งานได้อย่างมีประสิทธิภาพ

(5) ควบคุมการจัดเส้นทางบนระบบเครือข่ายสื่อสารและกำหนดวิธีการเข้าถึงระบบเครือข่ายสื่อสารบริษัทฯ

(6) จัดทำระบบป้องกันการบุกรุกและการใช้งานที่ผิดปกติผ่านระบบเครือข่ายสื่อสาร

(7) ทดสอบการบุกรุกโจมตีระบบเครือข่ายสื่อสาร และจัดทำรายงานการโจมตี

(8) กำหนดผู้รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ของระบบเครือข่ายสื่อสารและอุปกรณ์ที่เชื่อมต่อ

(9) ทบทวนการกำหนดค่า Parameter อย่างน้อยปีละ 1 ครั้ง

(10) ทำการบำรุงรักษาระบบเครือข่ายสื่อสารเพื่อให้สามารถใช้งานได้อย่างมีประสิทธิภาพ โดยควบคุมดูแลให้มีการบำรุงรักษาระบบเครือข่ายตามระยะเวลาที่กำหนด

5.4 การบริหารจัดการสินทรัพย์

การบริหารจัดการสินทรัพย์คือ กระบวนการวางแผน จัดหา ใช้งาน ดูแล และควบคุมสินทรัพย์ของบริษัทฯ อย่างเป็นระบบ เพื่อให้เกิดประสิทธิภาพสูงสุด คุ้มค่า และลดความเสี่ยงที่เกี่ยวข้องกับสินทรัพย์ตลอดวงจรชีวิตการใช้งาน

(1) จัดทำทะเบียนคุมสินทรัพย์

1) กำหนดผู้รับผิดชอบต่อสินทรัพย์

2) จัดหมวดหมู่สินทรัพย์

3) กำหนดมาตรฐานคอมพิวเตอร์ในบริษัทฯ

(2) การเบิกใช้ทรัพย์สินคอมพิวเตอร์และเครือข่าย

1) ผู้ใช้ที่ต้องการขอเบิกใช้ทรัพย์สินต้องกรอกข้อมูลคำร้องขอลงในระบบ Help Desk "ขอใช้งานระบบเทคโนโลยีสารสนเทศ" ขอใช้ทรัพย์สินคอมพิวเตอร์ รวมถึงสถานที่จัดเก็บหรือติดตั้ง และพร้อมกับระบุรายละเอียด และต้องให้ผู้บังคับบัญชาพิจารณาอนุมัติ ในระบบ และให้ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศตรวจสอบงาน โดยให้ปฏิบัติตามระเบียบปฏิบัติงาน เรื่อง การขอรับบริการจากฝ่ายเทคโนโลยีสารสนเทศ (SOP-IT-01)

2) เจ้าหน้าที่ผู้รับผิดชอบพิจารณาตามขั้นตอนและความเหมาะสมในการขอเบิกใช้งานทรัพย์สินดังกล่าว โดยขอความเห็นชอบจากผู้บริหารหน่วยงานเจ้าของสินทรัพย์ หรือผู้ที่ได้รับมอบหมาย

3) เมื่อคำร้องได้รับอนุมัติ เจ้าหน้าที่ผู้รับผิดชอบต้องบันทึกข้อมูลสถานที่จัดเก็บหรือติดตั้งใหม่ของทรัพย์สิน ลงในระบบทรัพย์สินสารสนเทศ และลงทะเบียนในทะเบียนทรัพย์สินคอมพิวเตอร์และเครือข่ายสื่อสาร เพื่อจัดเก็บไว้เป็นประวัติทรัพย์สินของบริษัทฯ

(3) การแจ้งซ่อมบำรุงทรัพย์สินคอมพิวเตอร์และเครือข่าย

1) เมื่อผู้ใช้งานพบการทำงานที่ผิดไปจากปกติของทรัพย์สิน หรือไม่สามารถใช้งานทรัพย์สินในการดำเนินงานได้ ผู้ใช้งานต้องแจ้งให้ดำเนินการซ่อมบำรุง โดยกรอกข้อมูลทรัพย์สินที่ต้องการแจ้งคำร้องลงในระบบ Help Desk "แจ้งคำร้อง แจ้งซ่อม / รับบริการ" โดยให้ปฏิบัติตามระเบียบปฏิบัติงาน เรื่อง การขอรับบริการจากฝ่ายเทคโนโลยีสารสนเทศ (SOP-IT-01) เจ้าหน้าที่ผู้รับผิดชอบวิเคราะห์อาการเสียหายของทรัพย์สิน จากข้อมูลระบบ Help Desk และจากการทดสอบการทำงานด้วยตนเอง รวมถึงพิจารณาข้อมูลประกอบโดยเฉพาะในส่วนของระยะเวลาประกันของทรัพย์สินดังกล่าว ซึ่งหากอยู่ในระยะเวลาประกัน เจ้าหน้าที่สามารถส่งทรัพย์สินเข้ารับการซ่อมบำรุงที่ศูนย์บริการของบริษัทผู้ผลิตทรัพย์สินได้ โดยไม่เสียค่าใช้จ่ายในส่วนที่ระบุในประกัน หากทรัพย์สินดังกล่าวไม่อยู่ในระยะเวลาประกัน เจ้าหน้าที่ผู้รับผิดชอบต้องพิจารณาจากความเสียหายของทรัพย์สิน หากความเสียหายของทรัพย์สินสามารถแก้ไขได้ให้ดำเนินการแก้ไข หรือหากเสียหายมากอาจจำเป็นจะต้องจำหน่ายทรัพย์สินดังกล่าว

2) ในระหว่างที่เจ้าหน้าที่ผู้รับผิดชอบส่งทรัพย์สินเข้ารับการซ่อมบำรุงนั้น หากมีทรัพย์สินอื่นที่สามารถใช้งานทดแทนทรัพย์สินดังกล่าวได้ ให้เจ้าหน้าที่ดำเนินการแจ้งแก่ผู้ใช้ทรัพย์สิน

3) หลังจากที่เจ้าหน้าที่ผู้รับผิดชอบส่งทรัพย์สินที่พบความเสียหายเข้ารับการแก้ไขเรียบร้อยแล้ว ต้องดำเนินการทดสอบในส่วนที่พบความเสียหายอีกครั้ง ก่อนจัดส่งทรัพย์สินคืนผู้ใช้ โดยเจ้าหน้าที่ผู้รับผิดชอบกรอกข้อมูลรายละเอียดการซ่อมบำรุง และการทดสอบทรัพย์สินลงในระบบ Help Desk และส่งคืนทรัพย์สินดังกล่าวให้กับผู้ใช้งาน

4) ผู้ใช้ทำการตรวจสอบทรัพย์สิน หากยังพบว่ามีความเสียหายในส่วนเดิมหรือส่วนอื่น ให้รีบแจ้งเจ้าหน้าที่ผู้รับผิดชอบ เพื่อดำเนินการแก้ไขตามขั้นตอนต่อไป

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

5.5 การจัดการสื่อบันทึกข้อมูล (Media Handling Policy)

เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับสื่อที่ใช้ในการบันทึกข้อมูลของบริษัทฯ โดยการถูกเปิดเผยโดยไม่ได้รับอนุญาต การเปลี่ยนแปลง การขนย้าย การลบ หรือการทำลายข้อมูล

(1) การบริหารจัดการสำหรับสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ ต้องมีการจัดทำขั้นตอนสำหรับบริหารจัดการสื่อบันทึกข้อมูล โดยต้องมีความสอดคล้องกับวิธีหรือขั้นตอนการจัดชั้นความลับของสารสนเทศที่บริษัทฯ กำหนดไว้ สื่อบันทึกข้อมูลที่มีข้อมูล ต้องมีการป้องกันข้อมูลจากการถูกเข้าถึงโดยไม่ได้รับอนุญาต การนำไปใช้ผิดวัตถุประสงค์ หรือความเสียหายในระหว่างที่นำส่ง หรือขนย้ายสื่อบันทึกข้อมูลนั้นต้องกำหนดวิธีปฏิบัติ และสิทธิ์สำหรับการใช้งานสื่อบันทึกข้อมูล อนึ่ง บริษัทฯ ไม่มีนโยบายให้ผู้ใช้งานระบบ ใช้งานสื่อบันทึกข้อมูลสื่อบันทึกข้อมูล

(2) หากจำเป็นต้องใช้งานสื่อบันทึกข้อมูลแบบให้แจ้งผู้เกี่ยวข้องโดยให้ผู้บังคับบัญชา และผู้จัดการฝ่ายเทคโนโลยีสารสนเทศพิจารณาอนุมัติ เพื่อเก็บประวัติการใช้งาน

5.6 การใช้สื่อบันทึกข้อมูลและแบ่งปันข้อมูลผ่านระบบ Share File

เพื่อกำหนดแนวทางในการใช้งานระบบจัดเก็บและแบ่งปันข้อมูล (Share File) เช่น Microsoft SharePoint Microsoft One Drive ภายในบริษัทฯ และ ระบบ Share Drive ภายในบริษัทฯ เพื่อให้เกิดความปลอดภัย ความเป็นส่วนตัว และประสิทธิภาพในการทำงานร่วมกัน

(1) การเข้าถึงและการใช้งาน
   1) ผู้ใช้งานต้องเข้าระบบด้วยบัญชีที่ได้รับอนุญาตจากฝ่ายเทคโนโลยีสารสนเทศ เท่านั้น
   2) จำกัดสิทธิ์การเข้าถึงตามหลัก **Least Privilege** โดยให้เฉพาะผู้ที่จำเป็นต้องใช้ข้อมูล
   3) ห้ามแชร์ลิงก์หรือไฟล์ที่ตั้งค่าให้ “Anyone with the link” เข้าถึงได้

(2) การจัดเก็บไฟล์
   1) ควรจัดเก็บไฟล์ในโฟลเดอร์ที่กำหนดตามแผนกหรือโครงการ
   2) ห้ามอัปโหลดไฟล์ที่มีข้อมูลส่วนบุคคลที่สามารถระบุตัวตนได้ (PII) หรือข้อมูลอ่อนไหว (Sensitive Data) เช่น บัตรประชาชน เลขบัญชี โดยไม่มีการเข้ารหัสหรือมาตรการป้องกัน เป็นต้น
   3) ห้ามจัดเก็บซอฟต์แวร์ผิดลิขสิทธิ์หรือไฟล์ที่ละเมิดกฎหมายใดๆ
   4) การบริหารพื้นที่การใช้งานให้ฝ่ายเทคโนโลยีสารสนเทศเป็นผู้กำหนด

(3) การแบ่งปันไฟล์
   1) การแชร์ไฟล์ควรใช้การกำหนดสิทธิ์แบบ “View Only” หากไม่จำเป็นต้องแก้ไข
   2) หากจำเป็นต้องแชร์ข้อมูลกับบุคคลภายนอก ต้องได้รับอนุมัติจากหัวหน้าหน่วยงาน
   3) ควรใช้รหัสผ่านหรือวันหมดอายุในการแชร์ไฟล์เสมอหากระบบรองรับทั้งภายในและภายนอกบริษัทฯ

(4) การสำรองและกู้คืนข้อมูล
   1) ระบบ SharePoint มีการสำรองข้อมูลอัตโนมัติ ฝ่ายเทคโนโลยีสารสนเทศจะรับผิดชอบในการกู้คืนข้อมูลในกรณีจำเป็น โดยผู้ใช้งานสามารถแจ้งคำร้องในระบบ Help Desk โดยปฏิบัติตามระเบียบปฏิบัติงาน เรื่อง การขอรับบริการจากฝ่ายเทคโนโลยีสารสนเทศ (SOP-IT-01)
   2) ผู้ใช้งานควรหลีกเลี่ยงการลบไฟล์ถาวรโดยไม่จำเป็น

หมวดที่ 6 การควบคุมความมั่นคงปลอดภัยสำหรับการปฏิบัติงาน

6.1 ควรมีการจัดทำตารางงาน ลำดับของงานก่อนหลัง สำหรับการส่งงานเข้าไปประมวลผลในเครื่องคอมพิวเตอร์ และการจัดการข้อผิดพลาดที่เกิดขึ้น (Job Schedule) ทั้งนี้ การจัดตารางงานนั้น ควรมีการทดสอบการทำงานว่าเป็นไปตามลำดับของงานตามที่กำหนดไว้

6.2 ควรมีการกำหนดบทบาทและหน้าที่ของผู้รับผิดชอบในการปฏิบัติงาน และ/หรือบุคคลที่เกี่ยวข้องกับการปฏิบัติงานในขั้นตอนต่างๆ และผู้มีอำนาจอนุมัติ

หมวดที่ 7 การสำรองข้อมูลและกู้คืนข้อมูล

เพื่อให้สารสนเทศและอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย และเพื่อป้องกันการสูญหายของข้อมูล

7.1 มีระบบจัดเก็บและสำรองข้อมูล ตามประเภทของข้อมูล ได้แก่ โปรแกรมระบบปฏิบัติการโปรแกรมประยุกต์หรือแอปพลิเคชั่น (Application Software) ชุดคำสั่ง และข้อมูล อย่างน้อย 1 ชุด แยกสถานที่จัดเก็บแยกจากกัน เพื่อความมั่นคงปลอดภัยและใช้งานได้อย่างต่อเนื่อง โดยให้ปฏิบัติตามระเบียบปฏิบัติงาน เรื่อง การสำรองข้อมูลและการกู้คืนข้อมูล (SOP-IT-02) ของฝ่ายเทคโนโลยีสารสนเทศ

7.2 กำหนดผู้รับผิดชอบในการสำรองข้อมูล ตรวจสอบความมีอยู่อย่างถูกต้อง ครบถ้วนของข้อมูล อย่างน้อยปีละ 1 ครั้ง และมีการบันทึกรายละเอียดการตรวจสอบ ในกรณีตรวจพบข้อมูลสูญหายไม่ถูกต้องครบถ้วน ให้ดำเนินการปรับปรุง แก้ไขข้อมูลให้มีความสมบูรณ์ครบถ้วนในทันที

7.3 กำหนดความถี่ในการสำรองข้อมูลของระบบงาน และทำการสำรองข้อมูลตามความถี่ที่กำหนดไว้ (ระบบงานที่มีการเปลี่ยนแปลงบ่อย ควรจะมีความถี่ในการสำรองข้อมูลมากขึ้น) และมีการนำข้อมูลที่สำรองไปเก็บไว้นอกสถานที่อย่างน้อย 1 ชุด

(1) กำหนดขั้นตอนการจัดทำสำรองข้อมูล และการกู้คืนข้อมูลอย่างถูกต้อง รวมทั้งซอฟต์แวร์

(2) ทำการตรวจสอบว่าการสำรองข้อมูลที่เกิดขึ้นนั้น สำเร็จครบถ้วน หรือไม่

(3) ทำการทดสอบกู้คืนข้อมูลที่สำรองไว้ อย่างน้อยปีละ 1 ครั้ง รวมทั้งดำเนินการทดสอบว่าระบบงานทั้งหมดสามารถใช้งานได้ หรือไม่

7.4 จัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้คืนระบบกลับคืนได้ภายในระยะเวลาที่กำหนด โดยมีแนวทางปฏิบัติสำหรับการกู้คืนข้อมูลจากภัยพิบัติ โดย

(1) จัดทำบัญชีรายชื่อระบบงานที่มีความสำคัญทั้งหมดของบริษัทฯ พร้อมทั้งปรับปรุงบัญชีรายชื่อให้ทันสมัยอยู่เสมอ เพื่อรองรับการเปลี่ยนแปลงหรือระบบงานสำคัญใหม่ที่เกิดขึ้น

(2) ประเมินความเสี่ยงสำหรับระบบงานที่มีความสำคัญเหล่านั้น และกำหนดมาตรการ เพื่อลดความเสี่ยงที่พบ และให้ปรับปรุงรายงานการประเมินความเสี่ยงอย่างน้อยปีละ 1 ครั้ง

(3) กำหนดชนิดของข้อมูล เช่น ซอฟต์แวร์ต่างๆ ที่เกี่ยวข้องกับระบบงาน หรือข้อมูลในฐานข้อมูล

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

(5) จัดทำแผนกู้คืนเพื่อรับมือกับภัยพิบัติที่อาจเกิดขึ้นได้ แผนกู้คืนต้องมีรายละเอียดดังต่อไปนี้

1) การกำหนดหน้าที่ และความรับผิดชอบต่อผู้ที่เกี่ยวข้องทั้งหมด
2) การประเมินความเสี่ยงสำหรับระบบงานที่มีความสำคัญเหล่านั้น และกำหนดมาตรการ เพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วง ทำให้ไม่สามารถเข้ามาใช้ระบบงานได้
3) การกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบงาน
4) การกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูลและทดสอบกู้คืนข้อมูลที่สำรองไว้
5) การทดสอบตามแผนเตรียมความพร้อมและประสิทธิภาพของแผนที่จัดทำไว้ อย่างน้อยปีละ 1 ครั้ง
6) การกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการ เครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์
7) การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน

(6) กำหนดให้มีการทบทวนแผนกู้คืนอย่างน้อยปีละ 1 ครั้ง

(7) กำหนดให้มีการสำรองข้อมูลตามชนิด ความถี่ และวิธีการสำรองที่ได้กำหนดไว้ และให้ตรวจสอบอย่างสม่ำเสมอว่าข้อมูลที่สำรองไปนั้นมีความครบถ้วน

(8) กำหนดให้มีให้ทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างน้อยปีละ 1 ครั้ง หากพบปัญหาในการกู้คืน ต้องดำเนินการแก้ไขและบันทึกรายละเอียดของปัญหา รวมถึงวิธีการแก้ไขไว้เป็นลายลักษณ์อักษร

7.5 จัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินที่ไม่สามารถดำเนินการด้วยวิธีทางอิเล็กทรอนิกส์ เพื่อให้การปฏิบัติงานเป็นไปอย่างต่อเนื่อง โดยให้ปฏิบัติตามระเบียบปฏิบัติงาน เรื่อง การสำรองข้อมูลและการกู้คืนข้อมูล (SOP-IT-02) ของฝ่ายเทคโนโลยีสารสนเทศ

หมวดที่ 8 การประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศและการสื่อสาร

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

8.1 มีคณะทำงานบริหารความเสี่ยงของฝ่ายเทคโนโลยีสารสนเทศ เพื่อดำเนินการ

(1) จัดลำดับความสำคัญของความเสี่ยง

(2) จัดทำแผนบริหารความเสี่ยง

(3) ดำเนินการตามแผนบริหารความเสี่ยง

8.2 มีการตรวจสอบและประเมินความเสี่ยงในเรื่องความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและระบบคอมพิวเตอร์อย่างน้อยปีละ 1 ครั้ง

8.3 มีการรายงานการตรวจสอบและประเมินความเสี่ยงเสนอผู้รับผิดชอบ และหน่วยงานที่รับผิดชอบ และจะดำเนินการปรับปรุงตามคำแนะนำหน่วยงานที่รับผิดชอบนั้นโดยทันที

8.4 มีการกำหนดความรับผิดชอบของผู้ใช้งานหรือผู้บริหาร ให้ผู้ใช้งานและผู้บริหารรับผิดชอบในกรณีเกิดความเสียหายหรืออันตรายอันเนื่องมาจากผู้ใช้งานหรือผู้บริหารบกพร่องหรือไม่ปฏิบัติตามนโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศและแนวปฏิบัติในการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ แล้วแต่กรณี

หมวดที่ 9 การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เพื่อเสริมสร้างวัฒนธรรมองค์กรที่ให้ความสำคัญกับความปลอดภัยของข้อมูล และลดความเสี่ยงที่อาจเกิดจากความประมาทหรือความไม่รู้ของผู้ใช้งาน โดยมีเป้าหมายหลักเพื่อให้บุคลากรทุกระดับในองค์กร โดยสามารถปฏิบัติตามแนวทางต่อไปนี้

9.1 มีการเผยแพร่ประชาสัมพันธ์และฝึกอบรม ให้เจ้าหน้าที่บริษัทฯ รับทราบ เข้าใจและไม่กระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายอื่นๆ ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ รวมถึงมีความรับผิดชอบในการใช้ทรัพยากรทางด้านเทคโนโลยีสารสนเทศของบริษัทฯ อย่างเหมาะสม และจัดอบรมอย่างน้อยปีละ 1 ครั้ง

9.2 มีการทบทวนปรับปรุงนโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศและแนวปฏิบัติในการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศให้มีความทันสมัย และเป็นมาตรฐานที่ยอมรับอย่างน้อยปีละ 1 ครั้ง

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

10.1 การวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Requirements Analysis and Specification) เพื่อให้มั่นใจว่ามีการสร้างความปลอดภัยสารสนเทศให้กับระบบเทคโนโลยีสารสนเทศตลอดวงจรการพัฒนาระบบ ซึ่งรวมถึงความต้องการด้านความปลอดภัยสารสนเทศที่ให้บริการผ่านเครือข่ายสาธารณะ

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

1) มาตรการปฏิบัติก่อนที่จะเกิดความเสียหาย เช่น การสำรองข้อมูล ระบบเครือข่ายสำรอง เป็นต้น
2) มาตรการปฏิบัติหลังจากเกิดความเสียหาย เช่น แผนการกู้คืนข้อมูล ระยะเวลาในการกู้คืนข้อมูล เป็นต้น

(2) ความมั่นคงปลอดภัยของบริการสารสนเทศบนเครือข่ายสาธารณะ (Securing Application Services on Public Networks) สารสนเทศที่เกี่ยวข้องกับการบริการสารสนเทศที่มีการส่งผ่านเครือข่ายสาธารณะ ต้องได้รับการป้องกันการเข้าถึง การเปิดเผย หรือเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต

(3) การป้องกันธุรกรรมของบริการสารสนเทศ (Protecting Application Services Transactions) สารสนเทศที่เกี่ยวข้องกับธุรกรรมของบริการสารสนเทศ ต้องได้รับการป้องกันจากการรับส่งข้อมูลที่ไม่สมบูรณ์ การส่งข้อมูลผิดเส้นทาง การเปลี่ยนแปลงข้อความโดยไม่ได้รับอนุญาต การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต การส่งข้อมูลซ้ำโดยไม่ได้รับอนุญาต

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

(1) การกำหนดหลักเกณฑ์สำหรับการพัฒนาซอฟต์แวร์ และมีการปฏิบัติตามระเบียบปฏิบัติหรือข้อกำหนดที่บริษัทฯ กำหนดขึ้นมา เช่น การพัฒนาซอฟต์แวร์ ควรคำนึงความปลอดภัยในทุกขั้นตอนของการพัฒนา และนักพัฒนา (Developer) ควรมีความสามารถในการหลีกเลี่ยงไม่ให้โปรแกรมที่พัฒนาตรวจพบช่วงโหว่ และต้องสามารถแก้ไขช่องโหว่ที่ตรวจพบได้

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

1) คำขอแก้ไขต้องมาจากผู้ที่มีสิทธิ์เท่านั้น
2) ต้องได้รับการอนุมัติจากผู้มีอำนาจก่อนดำเนินการ
3) ต้องมีการควบคุมและติดตามผลกระทบ (Side Effects) ที่อาจเกิดขึ้นหลังการแก้ไข
4) เมื่อแก้ไขเสร็จสิ้น ต้องผ่านการตรวจรับจากผู้มีอำนาจอนุมัติ หรือ ผู้ใช้งาน

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

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

(5) หลักการวิศวกรรมระบบด้านความมั่นคงปลอดภัย (Secure System Engineering Principles) เพื่อให้เกิดความมั่นคงปลอดภัยทางด้านวิศวกรรม ระบบต้องมีการกำหนดขึ้นมาเป็นลายลักษณ์อักษร โดยมีการปรับปรุงอย่างต่อเนื่อง และมีการประยุกต์ใช้กับงานพัฒนาระบบ โดยให้คณะกรรมการความปลอดภัยฯ มีหน้าที่ดูแลระบบด้านความมั่นคงปลอดภัยด้านโครงสร้างสำนักงาน

(6) การจ้างหน่วยงานภายนอกเพื่อพัฒนาระบบงาน (Outsourced Development) ในการทำสัญญาว่าจ้างการพัฒนาระบบของบริษัทฯ ต้องมีความชัดเจนและครอบคลุมถึงสัญญาทางด้านลิขสิทธิ์ซอฟต์แวร์ การใช้ระบบ การตรวจสอบระบบ โดยละเอียดก่อนติดตั้งใช้งานจริง รวมถึงการรับรองคุณภาพของระบบ และการกำหนดขอบเขตในการจ้างพัฒนาระบบ

(7) การทดสอบด้านความมั่นคงปลอดภัยของระบบ (System Security Testing) โปรแกรมหรือระบบที่พัฒนาขึ้นมา ควรมีการทดสอบคุณสมบัติด้านความมั่นคงปลอดภัย โดยต้องมีการทดสอบอยู่ในช่วงระหว่างการพัฒนา การทดสอบเพื่อรับรองระบบ (System/User Acceptance Testing) มีการจัดทำแผนการทดสอบหรือเกณฑ์ที่เกี่ยวข้องเพื่อรับรองระบบ โดยต้องมีการจัดทำทั้งสำหรับระบบใหม่และระบบที่ปรับปรุง

10.3 ระเบียบปฏิบัติข้อมูลสำหรับการทดสอบ (Test Data) เพื่อให้มีการป้องกันข้อมูลที่นำมาใช้ในการทดสอบ

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

1) ต้องมีการแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน เพื่อลดความเสี่ยงจากการเข้าถึงหรือการเปลี่ยนแปลงระบบงานจริงโดยไม่ได้รับอนุญาต
2) ในการพัฒนาระบบ ต้องจัดให้มีการแยก ระบบพัฒนา (Development System) ออกจากระบบงานจริง (Production System) อย่างชัดเจน
3) ต้องกำหนดระเบียบปฏิบัติที่ชัดเจนสำหรับการโอนย้ายโปรแกรมที่พัฒนาเสร็จสิ้นไปยังระบบงานจริง
4) ต้องห้ามติดตั้งคอมไพเลอร์ (Compiler) หรือโปรแกรมสำหรับการพัฒนาอื่นๆ ในระบบคอมพิวเตอร์ที่ใช้งานจริง (Production System)

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

หมวดที่ 11 การใช้งานปัญญาประดิษฐ์ (AI)

เพื่อกำหนดแนวปฏิบัติที่ปลอดภัยในการใช้งานเทคโนโลยีปัญญาประดิษฐ์ (AI) ภายในบริษัทฯ เพื่อป้องกันความเสี่ยงด้านความมั่นคงปลอดภัยของข้อมูล ที่ขัดกับกฎหมาย และจริยธรรม โดยเน้นการป้องกันข้อมูลรั่วไหล ความเสียหายต่อบริษัทฯ และภาพลักษณ์

11.1 ขั้นตอนการปฏิบัติงาน (Procedures) เพื่อให้การใช้เทคโนโลยีปัญญาประดิษฐ์ (AI) ภายในบริษัทฯ เป็นไปอย่างเหมาะสม ปลอดภัย และสอดคล้องกับกฎหมาย รวมถึงจริยธรรมในการดำเนินธุรกิจ บริษัทกำหนดขั้นตอนการปฏิบัติงาน ดังนี้

(1) การขออนุมัติใช้งานเครื่องมือ AI ใหม่

1) พนักงานที่มีความประสงค์จะใช้งานเครื่องมือ AI ใหม่ ต้องเสนอคำขอผ่านหัวหน้างานโดยชี้แจงวัตถุประสงค์และลักษณะการใช้งาน ผ่านระบบ Helpdesk โดยปฏิบัติตามระเบียบปฏิบัติงาน เรื่อง การขอรับบริการจากฝ่ายเทคโนโลยีสารสนเทศ (SOP-IT-01)
2) หัวหน้างานจะส่งคำขอดังกล่าวให้ฝ่ายเทคโนโลยีสารสนเทศ (IT) หรือฝ่ายบริหารความเสี่ยงพิจารณาเรื่องความเหมาะสมและประเมินความเสี่ยง
3) เมื่อได้รับการอนุมัติแล้ว จึงสามารถดำเนินการใช้งานเครื่องมือ AI ได้ตามวัตถุประสงค์ที่ระบุไว้

(2) แนวทางการใช้งานที่อนุญาต บริษัทอนุญาตให้ใช้งาน AI ได้ในกรณีที่มีลักษณะดังต่อไปนี้

1) เพื่อเพิ่มประสิทธิภาพในการทำงาน เช่น การร่างเอกสาร การสรุปรายงานเบื้องต้น การแปลภาษา หรือการวิเคราะห์ข้อมูลทั่วไป
2) ใช้เฉพาะกับข้อมูลที่ไม่เป็นความลับหรือข้อมูลทั่วไป (Public/Non-Sensitive Data) ซึ่งไม่เกี่ยวข้องกับข้อมูลภายในของบริษัทฯ หรือข้อมูลที่อ่อนไหว

3) ใช้ผ่านระบบหรือเครื่องมือ AI ที่ได้รับการตรวจสอบและอนุมัติจากฝ่ายเทคโนโลยีสารสนเทศหรือฝ่ายที่มีอำนาจโดยชอบ

(3) แนวทางการใช้งานที่ไม่อนุญาต เพื่อป้องกันความเสี่ยงทางกฎหมายและจริยธรรม ห้ามใช้งาน AI ในกรณีต่อไปนี้

1) ห้ามป้อน ส่ง หรือเปิดเผยข้อมูลภายในของบริษัทฯ เช่น ข้อมูลทางการเงิน ข้อมูลลูกค้า ข้อมูลพนักงาน หรือข้อมูลโครงการที่ยังไม่เผยแพร่ ผ่านระบบ AI ที่ไม่อยู่ภายใต้การควบคุมของบริษัทฯ

2) ห้ามใช้งาน AI เพื่อสื่อสารในนามบริษัทฯ หรือดำเนินการใด ๆ ที่เป็นการสื่อสารกับบุคคลภายนอกโดยไม่ได้รับอนุญาตอย่างเป็นทางการ

3) ห้ามคัดลอก สร้าง หรือเผยแพร่เนื้อหาที่ละเมิดลิขสิทธิ์ โดยใช้เครื่องมือ AI โดยไม่มีการอ้างอิงหรือได้รับสิทธิ์จากเจ้าของลิขสิทธิ์

4) ห้ามใช้งาน AI เพื่อวิเคราะห์ หรือตัดสินใจแทนมนุษย์ในประเด็นที่มีความละเอียดอ่อนหรือส่งผลกระทบต่อบุคคล เช่น การสรรหาบุคลากร การประเมินผลการปฏิบัติงาน หรือการลงโทษทางวินัย เว้นแต่จะมีการกลั่นกรองโดยผู้มีอำนาจและเป็นไปตามขั้นตอนของบริษัทฯ อย่างเคร่งครัด

11.2 การจัดอบรมและส่งเสริมความรู้เกี่ยวกับการใช้งาน AI

(1) จัดอบรมและส่งเสริมความรู้เกี่ยวกับการใช้งาน AI อย่างมีจริยธรรมให้แก่พนักงาน

(2) ประสานงานร่วมกับฝ่ายเทคโนโลยีสารสนเทศ และผู้บริหารเพื่อบูรณาการการใช้งาน AI กับนโยบายด้านบุคลากร

6. บทลงโทษ

บริษัทฯ จะดำเนินการลงโทษทางวินัยแก่ผู้ฝ่าฝืนหรือเพิกเฉยต่อการกระทำผิด ตามนโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ และ/หรือ แนวปฏิบัติในการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ จะต้องได้รับโทษตามที่กฎหมายกำหนด (ถ้ามี)

แนวปฏิบัติในการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศฉบับนี้ **ได้รับอนุมัติโดยมติที่ประชุมคณะกรรมการธรรมาภิบาลและบริหารความเสี่ยง ครั้งที่ 1 (ชุดที่ 11) เมื่อวันที่ 27 สิงหาคม 2568 และให้มีผลบังคับใช้ตั้งแต่วันที่ 19 กันยายน 2568 เป็นต้นไป** โดยยกเลิกแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่มีผลใช้บังคับเมื่อวันที่ 28 สิงหาคม 2567 ที่ได้รับอนุมัติจากที่ประชุมคณะกรรมการธรรมาภิบาลและบริหารความเสี่ยง ครั้งที่ 1 (ชุดที่ 10) เมื่อวันที่ 4 กรกฎาคม 2567

(นางอรรชกา สีบุญเรือง)
ประธานกรรมการธรรมาภิบาลและบริหารความเสี่ยง