บริษัท เอสทีพี แอนด์ ไอ จำกัด (มหาชน)

นโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

(ได้ผ่านการพิจารณาอนุมัติจากคณะกรรมการบริษัท เมื่อการประชุมคณะกรรมการ ครั้งที่ 3/2566 วันที่ 10 มีนาคม 2566)

นโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

ด้วยบริษัท เอสทีพี แอนด์ ไอ จำกัด (มหาชน) ได้จัดให้มีการใช้งานระบบคอมพิวเตอร์เทคโนโลยีสารสนเทศในการอำนวยความสะดวกและเพิ่มศักยภาพในการปฏิบัติงานของพนักงานให้กับองค์กร เพื่อเป็นแนวทางให้พนักงานในการใช้งานระบบคอมพิวเตอร์เทคโนโลยีสารสนเทศของบริษัท ให้เกิดความสะดวกและปลอดภัย ทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานเครือข่ายระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง ลดความเสี่ยงที่อาจเกิดขึ้นจากการปฏิบัติงาน และภัยคุกคามต่าง ๆ ซึ่งอาจส่งผลกระทบต่อระบบธุรกิจของบริษัทให้ได้รับความเสียหายได้ ดังนั้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของบริษัท คงไว้ซึ่งการรักษาความลับ (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) ของสารสนเทศ จึงเห็นสมควรกำหนดนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศเพื่อให้ถือเป็นแนวทางในการปฏิบัติเดียวกัน อีกทั้งเป็นการบริหารทรัพยากรระบบคอมพิวเตอร์เทคโนโลยีสารสนเทศของบริษัท ให้เป็นไปอย่างมีประสิทธิภาพ โดยมีรายละเอียดดังต่อไปนี้

1. วัตถุประสงค์

1.1 เพื่อกำหนดทิศทาง หลักการ และกรอบของข้อกำหนดในการบริหารจัดการด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

1.2 เพื่อสร้างความรู้ความเข้าใจให้พนักงานปฏิบัติตามนโยบาย มาตรฐาน กรอบการดำเนินงาน ขั้นตอนการปฏิบัติงานคำแนะนำ รวมถึงกฎหมายที่เกี่ยวกับระบบคอมพิวเตอร์ได้อย่างถูกต้องและเหมาะสม

1.3 เพื่อให้พนักงาน และผู้ที่ต้องใช้ หรือเชื่อมต่อระบบคอมพิวเตอร์ของบริษัท ให้สามารถใช้งานระบบคอมพิวเตอร์ของบริษัทได้อย่างถูกต้องและเหมาะสม

1.4 เพื่อป้องกันไม่ให้ระบบคอมพิวเตอร์และข้อมูลสารสนเทศของบริษัท โดนบุกรุก ขโมยทำลายแทรกแซงการทำงาน หรือโจรกรรมในรูปแบบต่างๆ ที่อาจจะสร้างความเสียหายต่อการดำเนินธุรกิจของบริษัท

2. ขอบเขต

นโยบายฉบับนี้ใช้กับบริษัท เอสทีพี แอนด์ ไอ จำกัด (มหาชน) และบริษัทในเครือ ทั้งนี้ให้ครอบคลุมถึงบุคคลภายนอกที่ได้รับอนุญาตให้ใช้ระบบเครือข่าย คอมพิวเตอร์แม่ข่าย ระบบคอมพิวเตอร์ เครื่องคอมพิวเตอร์ คอมพิวเตอร์แบบพกพา อุปกรณ์สื่อสารแบบพกพา หรืออุปกรณ์สื่อสารโทรคมนาคม เพื่อเข้าถึงสารสนเทศของบริษัท

3. หลักการปฏิบัติในการรักษาความมั่นคงปลอดภัย (Security Principles)

หลักการปฏิบัติในกรรักษาความมั่นคงปลอดภัยนี้ มีหลักการเพื่อให้บรรลุตามวัตถุประสงค์ดังต่อไปนี้

- ความลับ (Confidentiality) การปกป้องความลับของข้อมูล โดยป้องกันการเข้าถึงและการเปิดเผยข้อมูลจากผู้ที่ไม่ได้รับอนุญาต รวมไปถึงข้อมูลส่วนบุคคลหรือข้อมูลที่เป็นกรรมสิทธิ์ของบริษัท
- ความสมบูรณ์ (Integrity) การทำให้มั่นใจว่าข้อมูลของบริษัท ต้องไม่มีการแก้ไข ดัดแปลง หรือโดนทำลายโดยผู้ที่ไม่ได้รับอนุญาต
- ความพร้อมใช้งาน (Availability) การทำให้มั่นใจว่าผู้ใช้งานที่ได้รับอนุญาตสามารถเข้าถึงข้อมูลได้อย่างรวดเร็วและเชื่อถือได้
- ภาระรับผิดชอบ (Accountability) การระบุหน้าที่ความรับผิดชอบของแต่ละบุคคล รวมถึงการรับผิดและรับชอบในผลของกระทำตามบทบาทหน้าที่นั้นๆ
- การพิสูจน์ตัวตน (Authentication) การทำให้มั่นใจว่าสิทธิการเข้าใช้งานระบบคอมพิวเตอร์และข้อมูลสารสนเทศต้องผ่านกระบวนการยืนยันตัวตนที่สมบูรณ์แล้วเท่านั้น
- การกำหนดสิทธิ (Authorization) การทำให้มั่นใจว่าการให้สิทธิเข้าใช้งานระบบคอมพิวเตอร์และข้อมูลสารสนเทศเป็นไปตามความจำเป็น (Least Privilege) และสอดคล้องกับความต้องการพื้นฐาน (Need to Know Basis) ตามที่ได้รับอนุญาต
- การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) การทำให้มั่นใจว่าผู้มีส่วนร่วม (Parties) ที่เกี่ยวข้องในการทำธุรกรรมไม่สามารถปฏิเสธได้ว่าไม่มีส่วนเกี่ยวข้องกับการทำธุรกรรมที่เกิดขึ้น

การรักษาความมั่นคงปลอดภัยอย่างได้ผล จำเป็นต้องมีข้อตกลงร่วมกันและได้รับความเอาใจใส่อย่างจริงจังในทุกเรื่องที่เกี่ยวข้อง อันประกอบไปด้วย

- การรักษาความปลอดภัยถือว่าเป็นหน้าที่ของพนักงานและบุคคลภายนอกทุกคน
- การบริหาร และการปฏิบัติในด้านการรักษาความมั่นคงปลอดภัยเป็นกระบวนการที่ต้องกระทำอย่างต่อเนื่องอยู่ตลอดเวลา
- การมีจิตสำนึก รู้จักหน้าที่ มีความรับผิดชอบ และใส่ใจที่จะกระทำตามข้อปฏิบัติที่กำหนดไว้ในนโยบาย มาตรฐาน กรอบการดำเนินงาน ขั้นตอนการปฏิบัติงาน คำแนะนำ และกระบวนการต่างๆ ถือเป็นสิ่งสำคัญที่สุดในกระบวนการรักษาความมั่นคงปลอดภัย การอธิบายให้พนักงานและบุคคลภายนอกทราบอย่างชัดเจนเพื่อให้เข้าใจในหน้าที่ และความรับผิดชอบในการรักษาความปลอดภัยที่ตนเองรับผิดชอบเป็นสิ่งที่จะทำให้การรักษาความมั่นคงปลอดภัยดำเนินไปอย่างมีประสิทธิผล

4. คำจำกัดความ

4.1 "บริษัท (Company)" หมายถึง บริษัท เอสทีพี แอนด์ ไอ จำกัด (มหาชน) และบริษัทในเครือ

4.2 "หน่วยงานเทคโนโลยีสารสนเทศ" หมายถึง หน่วยงานที่รับผิดชอบในการดำเนินงานด้านบริหารจัดการเทคโนโลยีสารสนเทศของบริษัท

4.3 "พนักงาน (Employee)" หมายถึง พนักงานที่ได้รับการว่าจ้างให้ทำงานเป็นพนักงานทดลองงาน พนักงานประจำ พนักงานสัญญาจ้างพิเศษ และผู้บริหารทุกระดับที่อยู่ภายใต้การจ้างงานของบริษัท

4.4 "ผู้ใช้งาน (User)" หมายถึง พนักงานของบริษัท รวมไปถึงบุคคลภายนอกบริษัทที่ได้รับอนุญาตให้มีรหัสเข้าใช้งานในบัญชีรายชื่อผู้สามารถข้าใช้งาน หรือ/และ มีรหัสผ่านเพื่อเข้าใช้งานอุปกรณ์ประมวลผลสารสนเทศของบริษัท

4.5 "ผู้บังคับบัญชา" หมายถึง พนักงานซึ่งเป็นผู้บังคับบัญชาของหน่วยงานภายในตามโครงสร้างองค์กรของบริษัท

4.6 "ระบบคอมพิวเตอร์ (Computer System)" หมายถึง เครื่องมือ หรืออุปกรณ์คอมพิวเตอร์ทุกชนิดทั้ง Hardware และ Software ทุกขนาด อุปกรณ์เครือข่ายเชื่อมโยงข้อมูลทั้งชนิดมีสายและไร้สาย วัสดุอุปกรณ์การเก็บรักษา และการถ่ายโอนข้อมูลชนิดต่างๆ ระบบ Internet และระบบ Intranet รวมถึงอุปกรณ์ไฟฟ้า และสื่อสารโทรคมนาคมต่างๆ ที่สามารถทำงาน หรือใช้งานได้ในลักษณะเช่นเดียวกัน หรือคล้ายคลึงกับคอมพิวเตอร์ ทั้งที่เป็นทรัพย์สินของบริษัท ของพนักงาน ของบริษัทคู่ค้า และของผู้อื่นที่เกี่ยวข้องและจำเป็นในการใช้งานภายในสถานประกอบการของบริษัทตามที่ได้รับอนุญาต

4.7 "ข้อมูลและสารสนเทศ (Data & Information Technology)" หมายถึง ข้อมูล ข่าวสาร บันทึก ประวัติ ข้อความในเอกสาร โปรแกรมคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์รูปภาพ เสียง เครื่องหมายและสัญลักษณ์ต่างๆ ไม่ว่าจะเก็บไว้ในรูปแบบที่สามารถสื่อความหมายให้บุคคลสามารถเข้าใจได้โดยตรง หรือผ่านเครื่องมือหรืออุปกรณ์ใดๆ

4.8 "ข้อมูลสำคัญ" หรือ "ข้อมูลที่เป็นความลับ (Sensitive Data)" หมายถึง ข้อมูลสารสนเทศที่มีความสำคัญต่อการดำเนินธุรกิจของบริษัท หรือที่บริษัท มีพันธะผูกพันตามข้อกำหนดของกฎหมาย จรรยาบรรณในการประกอบธุรกิจ หรือสัญญาซึ่งบริษัท ไม่อาจนำไปเปิดเผยต่อบุคคลอื่น หรือนำไปใช้ประโยชน์อย่างอื่นนอกเหนือจากวัตถุประสงค์ในการดำเนินธุรกิจของบริษัท การรั่วไหลของข้อมูลสำคัญ หรือข้อมูลที่เป็นความลับดังกล่าวอาจเป็นเหตุให้การดำเนินธุรกิจของบริษัท ต้องหยุดชะงัก ขาดประสิทธิภาพ หรือบริษัทเสื่อมเสียชื่อเสียง

4.9 "ระบบที่มีความสำคัญ (Important System)" หมายถึง ระบบคอมพิวเตอร์ที่บริษัทใช้ประโยชน์ เพื่อให้บริการทางธุรกิจทั้งระบบที่ก่อให้เกิดรายได้โดยตรง และระบบที่สนับสนุนให้เกิดรายได้ รวมถึงระบบอิเล็กทรอนิกส์อื่นใดที่ช่วยในการดำเนินธุรกิจของบริษัทให้เป็นปกติ และระบบที่ได้รับการกำหนด โดยหน่วยงานด้านความปลอดภัยข้อมูลและระบบสารสนเทศของบริษัท ทั้งนี้หากระบบที่มีความสำคัญดังกล่าวหยุดการทำงาน หรือมีความสามารถในการทำงานที่ลดถอยลงจะทำให้การดำเนินธุรกิจของบริษัทต้องหยุดชะงักหรือด้อยประสิทธิภาพ

4.10 "รีโมทแอคเซส (Remote Access)" หมายถึง การเข้าสู่ระบบสารสนเทศของบริษัทจากระยะไกล

4.11 "เจ้าของระบบ (System Owner)" หมายถึง หน่วยงานภายในซึ่งเป็นเจ้าของระบบคอมพิวเตอร์ และมีความรับผิดชอบในระบบคอมพิวเตอร์นั้นๆ

4.12 "ผู้ดูแลข้อมูล (Custodian)" หมายถึง ผู้ที่ได้รับมอบหมายจากเจ้าของระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศในการสนับสนุนงานการดูแล จัดการ และควบคุมการเข้าใช้ข้อมูลสารสนเทศให้เป็นไปตามข้อกำหนดหรือระดับสิทธิที่เจ้าของระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศกำหนด

4.13 "ผู้ดูแลระบบ (Administrator)" หมายถึง ผู้ที่ได้รับมอบหมายให้ดูแลใช้งาน และบำรุงรักษาระบบคอมพิวเตอร์ทั้งอุปกรณ์ Hardware Software และอุปกรณ์ต่อพ่วงที่ประกอบกันขึ้นเป็นระบบคอมพิวเตอร์ และระบบจะเป็นผู้ที่ให้รับอนุญาตให้มีอำนาจในการ ปรับเปลี่ยนเพิ่มเติม แก้ไข ปรับปรุงให้ระบบคอมพิวเตอร์ของบริษัท ทำงานได้อย่างถูกต้อง มีประสิทธิภาพสอดคล้องกับความต้องการทางธุรกิจและมีความปลอดภัย

4.14 "การรักษาความมั่นคงปลอดภัย" หรือ "ความมั่นคงปลอดภัย (Security)" หมายถึง กระบวนการ และการกระทำใดๆ เช่น การป้องกัน การเข้มงวดกวดขัน การระมัดระวัง การเอาใจใส่ในการใช้งาน และการดูแลรักษาระบบคอมพิวเตอร์ และข้อมูลสารสนเทศที่เป็นระบบและข้อมูลสำคัญ ให้พ้นจากความพยายามใดๆ ทั้งจากพนักงานภายใน และจากบุคคลภายนอก ในการเข้าถึง เพื่อโจรกรรมทำลาย หรือแทรกแซงการทำงานจนเป็นเหตุให้การดำเนินธุรกิงของบริษัท ได้รับความเสียหาย

4.15 "บุคคลภายนอก (External Party)" หมายถึง บุคลากรหรือหน่วยงานภายนอกที่ดำเนินธุรกิจหรือให้บริการที่อาจได้รับสิทธิเข้าถึงสารสนเทศ และอุปกรณ์ประมวลผลสารสนเทศของบริษัท เช่น

- บริษัทคู่ค้า (Business Partner)
- ผู้รับจ้างปฏิบัติงานให้กับบริษัท (Outsource)
- ผู้รับจ้างพัฒนาระบบหรือจัดหาวัสดุอุปกรณ์ต่างๆ (Supplier)
- ผู้ให้บริการต่างๆ (Service Provider)
- ที่ปรึกษา (Consultant)

5. หน้าที่ความรับผิดชอบ

5.1 หน้าที่ของกรรมการผู้จัดการ (MD)

5.1.1 กำหนดกลยุทธ์ในภาพรวม ควบคุมการปฏิบัติงานในบริษัท และอนุมัตินโยบายการรักษาความปลอดภัยระบบเทคในโลยีสารสนเทศของบริษัท

5.2 หน้าที่ของผู้จัดการฝ่ายบริหาร (Administrative Department Manager)

5.2.1 กำหนดเป้าหมาย และนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศของบริษัทโดยกำหนดให้ไปในทิศทางเดียวกันกับแผนยุทธศาสตร์ของบริษัท

5.2.2 ประเมินความต้องการใช้ทรัพยากรด้านสารสนเทศ ความคุ้มค่า รวมทั้งจัดหา และพัฒนาระบบสารสนเทศให้สอดคล้องกับกลยุทธ์ของบริษัท

5.2.3 ดูแลทรัพยากรด้านสารสนเทศของบริษัทให้สามารถสนับสนุนการปฏิบัติงานภายในอย่างมีประสิทธิภาพ

5.3 หน้าที่ของผู้จัดการแผนกเทคโนโลยีสารสนเทศ (Information Technology Section Manager)

5.3.1 กำหนดแนวทางการบริหารจัดการและแนวทางปฏิบัติด้านการรักษาปลอดภัยระบบเทคโนโลยีสารสนเทศของบริษัทโดยกำหนดให้ไปในทิศทางเดียวกันกับเป้าหมายและนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศของบริษัท

5.3.2 จัดการพัฒนานโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ Policy, Standard, Procedure และ Guideline เพื่อให้บริษัทได้มาซึ่งการรักษาความลับของข้อมูล (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity)และเสถียรภาพความมั่นคงของระบบ (Availability)

5.3.3 จัดการบริหารเฝ้าระวังการโจมตีระบบและภัยต่างๆ ที่อาจเกิดขึ้นกับระบบรวมทั้งวางแผนบริหารความต่อเนื่องทางธุรกิจเพื่อกู้ระบบยามฉุกเฉิน

5.3.4 มีการบริหารความเสี่ยงและการวิเคราะห์ความเสี่ยงที่อาจทำให้ระบบเกิดปัญหากระทบกับการดำเนินธุรกิจของบริษัท

5.3.5 นำเสนอผู้บริหารระดับสูงตามลำดับของโครงสร้างองค์กร ในเรื่องแผนการปฏิบัติงาน นโยบาย งบประมาณ และอัตรากำลัง

5.3.6 เตรียมพร้อมรับสถานการณ์ และเรียนรู้เทคนิคใหม่ ๆ ทางด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างสม่ำเสมอ

5.4 หน้าที่ของผู้บังคับบัญชา

5.4.1 ชี้แจง และส่งเสริมให้ผู้ใช้งานปฏิบัติตามนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ และตักเตือนลงโทษทางวินัยกรณีที่พบเห็นการปฏิบัติที่ไม่ถูกต้องเหมาะสม

5.5 หน้าที่ของผู้ใช้งาน

5.5.1 ต้องเรียนรู้ ทำความเข้าใจ และปฏิบัติตามน โบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศของบริษัทโดยเคร่งครัด

5.5.2 ให้ความร่วมมือกับบริษัทอย่างเต็มที่ในการป้องกันระบบคอมพิวเตอร์และข้อมูลสารสนเทศของบริษัท สอดส่องดูแลปกป้องข้อมูลและสารสนเทศของบริษัทให้มีความปลอดภัย

5.5.3 รายงานต่อบริษัททันที เมื่อพบว่าอุปกรณ์ หรือข้อมูลสารสนเทศสำคัญสูญหาย หรือพบเห็นการบุกรุก ขโมย ทำลาย หรือโจรกรรมสารสนเทศ รวมถึงระบบสารสนเทศที่อาจสร้างความเสียหายต่อบริษัท

5.6 หน้าที่ของเจ้าของข้อมูลและสารสนเทศ

5.6.1 จัดให้มีการจัดทำเอกสาร มาตรการ และขั้นตอนควบคุมการเข้าถึงข้อมูลให้เป็นไปตามนโยบายการรักษาความปลอดภัยระบบเทคโนโสยีสารสนเทศของบริษัท

5.6.2 ดูแลให้พนักงานปฏิบัติตามนโยบายการรักมาความปลอดภัยระบบเทคโนโลยีสารสนเทศของบริษัท

5.6.3 ควบคุมและอนุมัติการเข้าถึงข้อมูลและสารสนเทศ และระบบคอมพิวเตอร์ภายใต้หน้าที่และความรับผิดชอบ

5.6.4 รายงานเมื่อมีเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยของข้อมูลและสารสนเทศ

5.6.5 แจ้งหน่วยงานเทคโนโลยีสารสนเทศที่รับผิดชอบด้านการบริหารบัญชีผู้ใช้งาน และสิทธิ์ในการใช้ระบบสารสนเทศเพื่อลบ/เปลี่ยนแปลงสิทธิ์ เมื่อมีการเปลี่ยนแปลงพนักงาน / อำนาจหน้าที่ / โอนย้าย

6. บริษัทกำหนดนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศในประเด็นสำคัญประกอบด้วย

6.1 ความปลอดภัยเกี่ยวกับทรัพย์สินสารสนเทศ

6.1.1 ทรัพย์สินด้านสารสนเทศ ได้แก่ ฐานข้อมูล ไฟล์ข้อมูล ซอฟต์แวร์ เครื่องมือในการพัฒนา อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย อุปกรณ์สื่อสาร สื่อบันทึกข้อมูลภายนอก และอุปกรณ์ต่อพ่วงทุกชนิด ต้องมีการจัดทำบัญชีทรัพย์สินโดยผู้เป็นเจ้าของข้อมูล และผู้เกี่ยวข้องหน่วยงานสารสนเทศต้องร่วมจัดทำทะเบียนรายการทรัพย์สินด้านสารสนเทศ

6.1.2 บริษัทต้องกำหนดชั้นความลับ และกำหนดระดับความสำคัญของเอกสาร (Classification Guidelines) เพื่อป้องกันทรัพย์สินด้านสารสนเทศ ให้มีความปลอดภัยด้วยวิธีการที่เหมาะสม เอกสารหรือสิ่งดีพิมพ์ที่พิมพ์หรือทำซ้ำขึ้นมาจากต้นฉบับซึ่งมีการกำหนดชั้นความลับไว้ ทั้งในกรณีทั้งหมดหรือบางส่วน ให้ถือว่ามีชั้นความลับเดียวกันกับต้นฉบับข้อมูลนั้น

6.2 ความปลอดภัยเกี่ยวกับบุคลากร

6.2.1 ต้องมีการกำหนดหน้าที่ และความรับผิดชอบทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศอย่างเป็นลายลักษณ์อักษร สำหรับผู้ใช้งาน หรือที่ว่าจ้างหน่วยงานภายนอกมาปฏิบัติงาน รวมทั้งกำหนดมาตรการป้องกันและดูแลรักษาความปลอดภัยสำหรับสารสนเทศของบริษัท

6.2.2 จัดอบรมให้ความรู้แก่ผู้ใช้งานทุกคนเกี่ยวกับความตระหนักและวิธีปฏิบัติเพื่อสร้างความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ต้องมีการลงนามและเก็บรวบรวมไว้ในแฟ้มประวัติของบุคลากร ถ้ามีการเปลี่ยนแปลงทางด้านความมั่นคงปลอดภัยต้องแจ้งให้พนักงานทราบ

6.2.3 ต้องมีการกำหนดบทลงโทษทางวินัยสำหรับผู้ที่ฝ่าฝืนนโยบาย กฎและแนวปฏิบัติของบริษัท หากเป็นการละเมิดข้อกฎหมาย บทลงโทษจะเป็นไปตามฐานความผิดที่ได้กระทำ และเป็นไปตามระเบียบบริษัท

6.2.4 หากมีการแต่งตั้งโยกย้าย ปลดหรือเปลี่ยนแปลงตำแหน่งใดๆ สายงานทรัพยากรบุคคล ต้องแจ้งให้ผู้รับการว่าจ้างทราบ และผู้รับการว่าจ้างต้องปฏิบัติตามเงื่อนไขในสัญญาว่าจ้างจนกว่าจะสิ้นสุดการว่าจ้าง และพนักงานซึ่งพ้นตำแหน่งจากการจ้างงานไม่ว่ากรณีใด ต้องคืนทรัพย์สินที่เกี่ยวข้องกับระบบสารสนเทศ เช่น กุญแจ บัตรประจำตัวพนักงาน บัตรผ่านเข้า-ออกศูนย์คอมพิวเตอร์ อุปกรณ์ต่อพ่วง คู่มือ และเอกสารต่าง ๆ ให้แก่ผู้บังคับบัญชาก่อนวันสุดท้ายของการว่าจ้างงาน ซึ่งหน่วยงานเทคโนโลยีสารสนเทศต้องถอดถอนสิทธิการเข้าใช้งานดังกล่าวด้วย

6.2.5 ต้องสร้างความตระหนักเรื่องความมั่นคงปลอดภัยเบื้องต้นให้พนักงานเข้าใหม่พร้อมทั้งจัดให้พนักงานมีการลงนามหนังสือยินยอมการใช้ระบบเทคโนโลยีสารสนเทศของบริษัทอย่างปลอดภัย

6.3 ความปลอดภัยเกี่ยวกับพื้นที่จัดเก็บข้อมูลและปฏิบัติงาน

6.3.1 ต้องมีการสร้างความมั่นคงปลอดภัยทางกายภาพต่อสำนักงาน ห้องทำงาน และ ทรัพย์สินอื่นๆ และต้องจัดให้มีการป้องกันภัยคุกคามต่างๆ เช่น ไฟไหม้ น้ำท่วมแผ่นดินไหว การก่อความไม่สงบ เป็นต้น รวมถึงการปฏิบัติงานในพื้นที่ ที่ต้องรักษาความมั่นคงปลอดภัยต้องมีการจัดการป้องกันที่เพียงพอ

6.3.2 การส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก ต้องมีบริเวณเฉพาะที่จัดไว้ต่างหากเพื่อป้องกันการเข้าถึงทรัพย์สินสารสนเทศของบริษัทโดยไม่ได้รับอนุญาต

6.3.3 พนักงานต้องป้องกันอุปกรณ์ของสำนักงานเพื่อลดความเสี่ยงจากภัยคุกคามทางด้านสิ่งแวดล้อม และอันตรายต่างๆ รวมทั้งความเสี่ยงในการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต

6.3.4 ทรัพย์สินด้านสารสนเทศจะต้องอยู่ในพื้นที่ที่เหมาะสมมีความปลอดภัย มีการจำแนกพื้นที่ในการใช้งานระบบสารสนเทศอย่างเหมาะสม มีการแยกศูนย์คอมพิวเตอร์ออกจากสถานที่ทำงานทั่วไป และกั้นเป็นห้องต่างหาก มีการควบคุมการเข้า-ออกพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัยให้เข้า-ออกได้เฉพาะผู้ที่มีหน้าที่รับผิดชอบ

6.3.5 การเดินสายเคเบิ้ลต่างๆ ต้องมีการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต และการเดินสายนั้นต้องติดป้ายกำกับให้รู้ต้นทางปลายทางของสาย

6.3.6 ต้องบำรุงรักษาระบบคอมพิวเตอร์ ระบบเครือข่าย และคอมพิวเตอร์แม่ข่ายอย่างสม่ำเสมอหรือตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

6.3.7 ต้องมีมาตรการป้องกันอุปกรณ์ต่างๆ ที่ใช้งานอยู่นอกสำนักงานเพื่อไม่ให้เกิดความเสียหายต่ออุปกรณ์เหล่านั้น

6.3.8 พนักงานต้องมีการตรวจสอบอุปกรณ์ที่มีสื่อบันทึกข้อมูลเพื่อดูว่าข้อมูลสำคัญที่อยู่ในอุปกรณ์ดังกล่าวได้ถูกลบทิ้งหรือถูกบันทึกทับก่อนที่จะนำอุปกรณ์ดังกล่าวทิ้งไป โดยต้องเป็นไปตามที่หน่วยงานเทคโนโลยีสารสนเทศกำหนด

6.3.9 ต้องมีขั้นตอนปฏิบัติสำหรับการจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายให้

6.3.10 ต้องมีการกำหนดมาตรการการป้องกันเอกสารระบบจากการเข้าถึงโดยไม่ได้รับอนุญาต

6.3.11 ต้องกำหนดขั้นตอนปฏิบัติสำหรับการจัดการ และจัดเก็บสารสนเทศ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

6.3.12 ต้องมีมาตรการการกำจัดสื่อที่ใช้ในการบันทึกข้อมูลอย่างเป็นลายลักษณ์อักษร เช่น การเผา ตัดหั่น หรือทำลายสื่อบันทึกข้อมูลที่มีข้อมูลสำคัญในนั้น เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต โดยกำหนดให้มีบุคลากรผู้ทำหน้าที่ในการสอดส่องและดูแลการกำจัดหรือการทำลายสื่อบันทึกข้อมูล (ทั้งทำลายเองหรือจ้างบริษัทรับทำลายเป็นผู้ทำลายสื่อบันทึกข้อมูลเหล่านั้น) การทำลายเอกสารและสื่อที่ใช้ในการบันทึกข้อมูล จะต้องได้รับการอนุมัติจากเจ้าของข้อมูล รวมทั้งบันทึกรายละเอียดอย่างเหมาะสม

6.4 ความปลอดภัยเกี่ยวกับการดูแลระบบสารสนเทศ

6.4.1 ต้องจัดทำคู่มือขั้นตอนการปฏิบัติงาน เช่น ขั้นตอนการกู้คืนระบบ ขั้นตอนการบำรุงรักษาและดูแลระบบเป็นต้น และปรับปรุงคู่มือขั้นตอนการปฏิบัติงานเมื่อมีการเปลี่ยนแปลงขั้นตอนหรือ

ผู้รับผิดชอบ และต้องกำหนดให้มีการควบคุมการเปลี่ยนแปลง ปรับปรุงหรือแก้ไขระบบคอมพิวเตอร์ ระบบเครือข่าย คอมพิวเตอร์แม่ข่าย ฮาร์ดแวร์และซอฟต์แวร์

6.4.2 ต้องมีการแบ่งหน้าที่ความรับผิดชอบของผู้ดูแลระบบเพื่อลดโอกาสในการเปลี่ยนแปลงหรือแก้ไขโดยไม่ได้รับอนุญาต

6.5 ความปลอดภัยเกี่ยวกับการบริการของหน่วยงานภายนอก

6.5.1 ต้องมีการจัดทำข้อตกลงเพื่อควบคุมการให้บริการโดยหน่วยงานภายนอก เช่น มีการยอมรับนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศของบริษัท และขอบเขต รายละเอียดระดับการให้บริการ ต้องได้รับการตรวจสอบจากฝ่ายกฎหมายของบริษัท รวมถึงสัญญาในการไม่เปิดเผยข้อมูลของบริษัท เป็นต้น

6.5.2 หน่วยงานภายนอกหรือบุคคลภายนอกอื่นๆ ที่ให้รับอนุญาตในการเข้าถึงระบบสารสนเทศของบริษัทต้องยอมรับและปฏิบัติตามนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศของบริษัท

6.5.3 บริษัทจะประเมินความเสี่ยงในการเข้าถึงระบบสารสนเทศ หรือที่มีผลกระทบต่อบริษัท ของหน่วยงานภายนอกหรือบุคคลภายนอกอื่นๆ ถ้าจำเป็นต้องมีการเปิดเผยข้อมูลนั้นออกไป หน่วยงานภายนอกหรือบุคคลภายนอกนั้นต้องเซ็นสัญญาว่าจะไม่เปิดเผยความลับของบริษัท

6.5.4 ต้องตรวจสอบการให้บริการหรือสัญญาที่ทำกับหน่วยงานภายนอกและบุคคลภายนอกที่เข้ามาให้บริการกับบริษัท โดยมีการทบทวนอย่างสม่ำเสมอตามความจำเป็น รวมถึงต้องกำหนดให้ทำการปรับปรุงเงื่อนไขการให้บริการของหน่วยงานภายนอก เช่น เมื่อมีการปรับปรุงระบบสารสนเทศใหม่ การพัฒนาระบบสารสนเทศใหม่ การเปลี่ยนเทคโนโลยีใหม่ เป็นต้น

6.6 ความปลอดภัยเกี่ยวกับเครือข่ายคอมพิวเตอร์

6.6.1 ต้องกำหนดมาตรการเพื่อป้องกันภัยคุกคามต่างๆ ทางเครือข่าย และกำหนดสิทธิ์ผู้ที่ใช้งานผ่านเครือข่ายโดยอนุญาตเฉพาะผู้ที่มีสิทธิ์เท่านั้น

6.6.2 ต้องจำกัดการเชื่อมต่อจากภายนอกเข้าสู่ระบบเครือข่ายภายใน เช่น การเข้าถึงเครือข่ายจากระยะไกลผ่านทางอินเตอร์เน็ต รวมถึงไม่ติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใดๆ ที่เกี่ยวข้องกับการให้บริการเครือข่าย โดยไม่ได้รับอนุญาต

6.7 ความปลอดภัยเกี่ยวกับการแลกเปลี่ยนข้อมูลและสารสนเทศ

6.7.1 ต้องกำหนดนโยบาย แนวปฏิบัติ และมาตรการเพื่อป้องกันปัญหาของการแลกเปลี่ยนสารสนเทศภายในบริษัท ภายในกลุ่มบริษัท และหน่วยงานภายนอกที่ผ่านช่องทางการสื่อสารทุกชนิดอย่างเป็นลายลักษณ์อักษร เช่น การส่งข้อความทางอิเล็กทรอนิกส์ เป็นต้น

6.7.2 ต้องมีมาตรการตรวจทานก่อนส่งข้อมูลสารสนเทศออกสู่สาธารณะ โดยมีการประเมินความเสี่ยงและกำหนดมาตรการลดความเสี่ยงก่อนนำข้อมูลไปเผยแพร่

6.8 ความปลอดภัยเกี่ยวกับการตรวจสอบการเข้าใช้งานระบบสารสนเทศ

6.8.1 ต้องกำหนดให้มีการบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศและกิจกรรมการใช้งานของผู้ใช้งานอย่างสม่ำเสมอ และต้องมีมาตรการป้องกันข้อมูลที่บันทึกที่เกี่ยวข้องกับการใช้งานสารสนเทศ ไม่ให้มีการเปลี่ยนแปลงหรือแก้ไขโดยไม่ได้รับอนุญาต รวมถึงต้องบันทึกกิจกรรมการดำเนินงานของเจ้าหน้าที่ที่เกี่ยวข้องกับระบบนั้นๆ ด้วย

6.8.2 ต้องกำหนดให้มีการบันทึกเหตุการณ์ข้อผิดพลาดที่เกี่ยวข้อง วิเคราะห์ข้อผิดพลาดเหล่านั้น และดำเนินการแก้ไขตามสมควร และต้องตั้งเวลาของเครื่องคอมพิวเตอร์ให้ตรงกัน โดยอ้างอิงจากแหล่งเวลาที่ถูกต้องเพื่อช่วยในการตรวจสอบช่วงเวลาหากเครื่องของบริษัทถูกบุกรุก

6.8.3 การเข้าถึงและการใช้งานระบบสารสนเทศของพนักงานจะต้องถูกสอบทานและทบทวนตามรอบระยะเวลาที่กำหนดไว้จากส่วนงานตรวจสอบภายใน โดยส่วนงานตรวจสอบภายในมีสิทธิ์ที่จะสอดส่องดูแลการกระทำใดๆ ที่ผู้ตรวจสอบสงสัยว่ามีการฝ่าฝืนนโยบายดังกล่าว

6.9 ความปลอดภัยเกี่ยวกับการควบคุมการเข้าถึงระบบสารสนเทศ

6.9.1 ต้องกำหนดให้มีขั้นตอนสำหรับการลงทะเบียนต่างๆ เพื่อให้มีสิทธิ์และควบคุมสิทธิ์ในการเข้าถึงสารสนเทศและระบบสารสนเทศของบริษัทตามความจำเป็นรวมถึงขั้นตอนการยกเลิกสิทธิ์การใช้งาน เช่น เมื่อลาออกหรือเปลี่ยนแปลงตำแหน่ง เป็นต้น รวมถึงต้องมีกระบวนการจัดการรหัสผ่านสำหรับผู้ใช้งาน เพื่อควบคุมการจัดสรร รหัสผ่านให้แก่ผู้ใช้งานตามความเหมาะสมหรือที่เกี่ยวข้องกับงานที่ได้รับมอบหมาย

6.9.2 ผู้ใช้งานต้องเป็นผู้รับผิดชอบในการดูแล รักษาบัญชีผู้ใช้งาน และรหัสผ่านของตนให้มีความมั่นคงปลอดภัยเพียงพอ

6.9.3 พนักงานต้องมีวิธีป้องกันไม่ให้ผู้ไม่มีสิทธิ์สามารถเข้าถึงอุปกรณ์สำนักงานที่ไม่มีพนักงานดูแล เช่น แจ้งหัวหน้าหน่วยงาน หรือเจ้าหน้าที่รักษาความปลอดภัยทุกครั้งที่พบเห็น รวมถึงมีนโยบายเพื่อควบคุมไม่ให้มีการปล่อยให้ทรัพย์สินสารสนเทศที่สำคัญ เช่น เอกสาร สื่อบันทึกข้อมูล อยู่ในสถานที่ที่ไม่ปลอดภัยหรือพบเห็นได้ง่าย

6.9.4 ต้องจัดทำนโยบายการใช้งานเครือข่ายซึ่งจะต้องครอบคลุมว่าบริการใดอนุญาตให้ผู้ใช้งานสามารถใช้ได้ บริการใดไม่สามารถใช้งานได้

6.9.5 การเข้าถึงระบบสารสนเทศและสารสนเทศของบริษัทจะกระทำได้เมื่อได้รับอนุมัติโดยหัวหน้าหน่วยงานและหัวหน้าหน่วยงานเทคโนโลยีสารสนเทศสามารถใช้ได้เฉพาะที่เกี่ยวข้องกับงานในหน้าที่ของบุคคลนั้น และต้องถูกจำกัดการเข้าถึง ให้เฉพาะผู้ที่ ได้รับอนุญาต หรือผู้ที่มีความจำเป็นต้องใช้ข้อมูลนั้น และต้องได้รับความยินยอมจากเจ้าของข้อมูล

6.9.6 การเข้าถึงระบบสารสนเทศทุกระบบแต่ละครั้งต้องได้รับการพิสูจน์ และยืนยันตัวตนทุกครั้งอย่างน้อยด้วย Username และ Password ที่ได้รับจากผู้ดูแลระบบ ก่อนที่จะเข้าใช้งานได้ตามสิทธิที่ได้รับ และหากเป็นระบบสำคัญ หรือเป็นการใช้งานจากระยะไกล (Remote Access) จะต้องกำหนดให้มีการยืนยันตัวตนแบบ 2 ขั้นตอน (Two -Factor Authentication) ทั้งนี้ สิทธิ์ในการใช้งานต้องถูกทบทวนสิทธิ์อย่างน้อยปีละ 1 ครั้ง

6.9.7 การเปลี่ยนแปลงระบบสารสนเทศ /ระบบเน็ตเวิร์ค หรือแอพพลิเคชั่นใดๆ จะต้องได้รับการตรวจสอบและอนุญาตจากเจ้าของข้อมูล รวมถึงได้รับอนุมัติจากผู้จัดการแผนกเทคโนโลยีสารสนเทศ

6.9.8 ต้องมีมาตรการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบโดยมาตรการต้องครอบคลุมทั้งการป้องกันทางกายภาพและการป้องกันการเข้าถึงโดยผ่านทางเครือข่าย

6.9.9 ต้องจัดให้มีระบบ หรือวิธีการในการตรวจสอบคุณภาพของรหัสผ่าน และมีวิธีการควบคุมดูแลให้ผู้ใช้งานเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด

6.9.10 ต้องจำกัดและควบคุมการใช้โปรแกรมยูทิลิตี้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้ เช่น จำกัดการใช้งานโปรแกรมดังกล่าวให้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น เป็นต้น และต้องกำหนดวิธีการตัดเวลาการใช้งานเครื่องคอมพิวเตอร์ เพื่อเครื่องคอมพิวเตอร์นั้นไม่ได้ใช้งานเป็นระยะเวลาหนึ่ง รวมถึงต้องจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ ที่มีความสำคัญสูง

7. การแจกจ่ายเอกสารนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

7.1 แผนการเผยแพร่นโยบาย

7.1.1 เอกสารนโยบายฉบับนี้จะจัดทำให้ผู้ใช้งานทุกคนได้อ่าน ทำความเข้าใจ และประกาศบนเว็บไซต์ของบริษัท

7.2 แผนการฝึกอบรม

7.2.1 ทำแผนการฝึกอบรมเรื่องนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศตามความจำเป็น

8. วิธีการปฏิบัติให้เป็นไปตามนโยบาย

หน่วยงานเทคโนโลยีสารสนเทศ ฝ่ายบริหาร ได้จัดทำนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศโดยอ้างอิงมาตรฐาน ISO/IEC 27001:2013 Information Security Management Systems เพื่อให้เกิดความมั่นคงปลอดภัยแก่สารสนเทศของบริษัท

9. การพิจารณาโทษทางวินัย

9.1 ผู้ใช้งานที่มีเจตนาฝ่าฝืนนโยบาย เงื่อนไข ข้อตกลงตามเอกสารฉบับนี้ แม้ว่าการฝ่าฝืนจะกระทำไม่สำเร็จโดยสมบูรณ์ก็ให้ถือว่ามีความผิดโดยสมบูรณ์

9.2 พนักงานและลูกจ้างที่ฝ่าฝืนข้อกำหนดนโยบายด้านความมั่นคงปลอดภัย เทคโนโลยีสารสนเทศ โดยจงใจหรือประมาทเลินเล่อ และก่อหรืออาจก่อให้เกิดความเสียหายแก่บริษัท หรือบุคคลหนึ่งบุคคลใด บริษัทจะพิจารณาดำเนินการทางวินัย ความผิดทางแพ่งและอาญาแก่พนักงานและลูกจ้างนั้น ตามกฎหมาย ข้อบังคับ ระเบียบ หรือประกาศที่เกี่ยวข้อง

9.3 ผู้บังคับบัญชาผู้ใด งดเว้น หรือละเว้นการปฏิบัติตามหน้าที่ และเป็นเหตุให้พนักงานหรือลูกจ้างที่อยู่ภายใต้การบังคับบัญชาของตน ฝ่าฝืนข้อกำหนดของนโยบายด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศนี้ ให้นำบทพิจารณาโทษทางวินัยใน ข้อ 9.2 มาใช้บังคับโดยไม่อนุโลม

9.4 การฝ่าฝืนข้อกำหนดใด ๆ ตามนโยบายด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศนี้แม้จะไม่ก่อให้เกิดความเสียหายแก่บริษัท หรือบุคคลหนึ่งบุคคลใดก็ตาม ถ้าผู้บังคับบัญชาเห็นว่ามีเหตุอันสมควร อาจจะบันทึกในประวัติการปฏิบัติงานและจะใช้เป็นข้อมูลประกอบการพิจารณาต่ออายุสัญญาจ้าง การขึ้นเงินเดือน หรือ เลื่อนตำแหน่งด้วยก็ได้

9.5 ผู้กระทำความผิดเกี่ยวกับ กฎ ระเบียบ เงื่อนไข หรือนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของบริษัทจะต้องถูกลงโทษตามระเบียบบริษัท โดยแผนกทรัพยากรบุคคลจะเป็นผู้ดำเนินการสอบสวนและลงโทษทางวินัยตามขั้นตอนในระเบียบบริษัทที่กำหนดไว้

10. การทบทวนนโยบาย

ผู้จัดการด้านเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมาย ต้องดำเนินการทบทวนนโยบายฉบับนี้เป็นประจำอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ และต้องเสนอให้ประธานกรรมการบริหารอนุมัติหากมีการเปลี่ยนแปลง