นโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

(Information Security Management Policy)

Enterprise IT Governance Office

บริษัท กรุงเทพดุสิตเวชการ จำกัด (มหาชน) | 2 ซอยศูนย์วิจัย 7 ถนนเพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310

สารบัญ

นโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

(Information Security Management Policy)

บริษัท กรุงเทพดุสิตเวชการ จำกัด (มหาชน) มีความมุ่งมั่นในการพัฒนาและประยุกต์ใช้ระบบเทคโนโลยีสารสนเทศเพื่อขับเคลื่อนการดำเนินธุรกิจอย่างมีประสิทธิภาพ โดยมุ่งเน้นการยกระดับการบริหารจัดการ พัฒนานวัตกรรมด้านผลิตภัณฑ์และบริการ รวมถึงปรับปรุงกระบวนการทำงานให้ทันสมัย และสร้างประสบการณ์ที่ดีแก่ผู้รับบริการผ่านการใช้เทคโนโลยีดิจิทัลอย่างมีประสิทธิผล ทั้งนี้ การดำเนินการดังกล่าวตั้งอยู่บนพื้นฐานของความรับผิดชอบต่อสิ่งแวดล้อม สังคม และการกำกับดูแลกิจการที่ดี (Environmental, Social and Governance: ESG)

ท่ามกลางการเปลี่ยนแปลงอย่างรวดเร็วของเทคโนโลยี โดยเฉพาะการนำระบบดิจิทัลและเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) เข้ามาประยุกต์ใช้ในกระบวนการให้บริการ การวินิจฉัย ตัดสินใจ และบริหารจัดการ บริษัทเล็งเห็นถึงความจำเป็นในการพัฒนาและเสริมสร้างระบบควบคุมด้านความมั่นคงปลอดภัยสารสนเทศให้มีความครอบคลุม ทันสมัย และสอดคล้องกับแนวปฏิบัติที่ดี (Best Practices) และมาตรฐานสากล อาทิ ISO/IEC 27001, ISO 27799 และกรอบแนวทางของ NIST เพื่อให้สามารถรับมือกับภัยคุกคามทางไซเบอร์ที่ซับซ้อนและเปลี่ยนแปลงอยู่ตลอดเวลาได้อย่างมีประสิทธิภาพ พร้อมทั้งเสริมสร้างความมั่นใจให้แก่ผู้ป่วย ผู้ใช้บริการ คู่ค้า หน่วยงานกำกับดูแล และผู้มีส่วนได้ส่วนเสียทุกภาคส่วนอย่างมั่นคงและยั่งยืน

1. **วัตถุประสงค์** (Purpose)

นโยบายฉบับนี้จัดทำขึ้นเพื่อเป็นกรอบแนวทางในการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์กร โดยมุ่งเน้นให้การดำเนินงานในทุกระดับมีความปลอดภัย เชื่อถือได้ มีความต่อเนื่อง และสามารถตรวจสอบได้อย่างเป็นระบบ เพื่อรองรับการเติบโตขององค์กรภายใต้การใช้เทคโนโลยีดิจิทัลและปัญญาประดิษฐ์อย่างมั่นคงและยั่งยืน ทั้งนี้ บริษัทกำหนดวัตถุประสงค์หลักของนโยบายไว้ดังต่อไปนี้

1.1 กำหนดหลักการ แนวทาง และข้อกำหนดในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรอย่างครอบคลุม เป็นระบบ และสอดคล้องกับแนวปฏิบัติที่เป็นเลิศ

1.2 ปกป้องข้อมูลสารสนเทศที่ถือเป็นทรัพย์สินขององค์กร รวมถึงข้อมูลส่วนบุคคลด้านสุขภาพของผู้รับบริการ จากการเข้าถึง การเปิดเผย การเปลี่ยนแปลง หรือการทำลายโดยไม่ได้รับอนุญาต

1.3 ควบคุมและลดความเสี่ยงด้านความมั่นคงปลอดภัยที่อาจเกิดขึ้นจากการใช้ระบบเทคโนโลยีสารสนเทศและระบบปัญญาประดิษฐ์ (AI) ทั้งในส่วนที่พัฒนาและใช้งานโดยตรงภายในองค์กร และในส่วนที่ดำเนินการโดยบุคคลภายนอก (Third Parties) เพื่อให้สามารถบริหารจัดการความเสี่ยงได้ครอบคลุมในทุกมิติ และลดโอกาสของผลกระทบที่อาจเกิดขึ้นต่อข้อมูลสารสนเทศ ระบบงาน และความน่าเชื่อถือขององค์กร

1.4 กำหนดแนวทางในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย การกู้คืนระบบ และการฟื้นฟูการดำเนินงานให้สามารถกลับเข้าสู่ภาวะปกติได้อย่างมีประสิทธิภาพในกรณีที่เกิดเหตุไม่คาดคิด

1.5 เสริมสร้างวัฒนธรรมด้านความมั่นคงปลอดภัยสารสนเทศภายในองค์กร และปลูกฝังความตระหนักรู้ให้แก่บุคลากรทุกระดับ พร้อมส่งเสริมให้มีการปฏิบัติตามนโยบาย กฎระเบียบ และมาตรฐานด้านความมั่นคงปลอดภัยที่องค์กรกำหนดไว้อย่างเคร่งครัด

1.6 เพื่อให้การดำเนินงานขององค์กรเป็นไปตามข้อกำหนดทางกฎหมาย ระเบียบข้อบังคับ และมาตรฐานสากลที่เกี่ยวข้อง

2. **ขอบเขต** (Scope)

นโยบายและแนวปฏิบัติฉบับนี้ครอบคลุมถึงการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในทุกกระบวนการที่เกี่ยวข้องกับระบบสารสนเทศขององค์กร ไม่ว่าจะอยู่ในระยะของการพัฒนา การจัดหา การนำมาใช้งาน การดูแลรักษา ตลอดจนการเลิกใช้งานระบบและทรัพยากรสารสนเทศ โดยมีวัตถุประสงค์เพื่อควบคุมและลดความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศในทุกระดับอย่างครอบคลุม เป็นระบบ และสามารถตรวจสอบได้ ขอบเขตของนโยบายฉบับนี้ครอบคลุมถึง

- ทรัพย์สินสารสนเทศ ทุกประเภทที่องค์กร เป็นเจ้าของ หรือมีหน้าที่รับผิดชอบในการบริหารจัดการ ไม่ว่าจะอยู่ภายใต้การควบคุมโดยตรงขององค์กร หรือดำเนินการผ่านบุคคลภายนอก เช่น ผู้ให้บริการระบบ ผู้รับจ้าง หรือคู่สัญญาทางธุรกิจ
- โครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ ระบบงาน ข้อมูลสารสนเทศ และผู้ใช้งานทุกประเภท ทั้งภายในและภายนอกองค์กร
- ระบบเทคโนโลยีสารสนเทศและระบบปัญญาประดิษฐ์ (Artificial Intelligence: AI) ทุกประเภท ไม่ว่าจะติดตั้งและดำเนินการภายในองค์กร (On-premises Systems) หรือให้บริการผ่านระบบคลาวด์ (Cloud-based Services)
- กิจกรรมที่เกี่ยวข้องกับการเข้าถึง การใช้ การประมวลผล การจัดเก็บ และการส่งผ่านข้อมูลสารสนเทศขององค์กร โดยเฉพาะข้อมูลส่วนบุคคลด้านสุขภาพ (Personal Health Information: PHI) ซึ่งถือเป็นข้อมูลอ่อนไหวตามที่กฎหมายและมาตรฐานที่เกี่ยวข้องกำหนด

นโยบายฉบับนี้ถือเป็นข้อกำหนดที่มีผลบังคับใช้กับคณะกรรมการ ผู้บริหารและพนักงานในกลุ่มธุรกิจของบริษัท กรุงเทพดุสิตเวชการ จำกัด (มหาชน) บริษัทย่อยและกิจการอื่น ๆ ที่บริษัทมีอำนาจควบคุมการดำเนินงาน (รายละเอียดดังเอกสารแนบท้าย 1) โดยไม่มีข้อยกเว้น และรวมถึงคู่สัญญาหรือบุคคลใดที่มีสิทธิเข้าถึงระบบสารสนเทศ/ข้อมูลองค์กร โดยทุกฝ่ายจะต้องยึดถือและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด เพื่อให้การใช้งานและบริหารจัดการระบบสารสนเทศเป็นไปอย่างมั่นคงปลอดภัย มีประสิทธิภาพ และสอดคล้องกับกฎหมายหรือข้อกำหนดที่เกี่ยวข้อง

1. คณะกรรมการบริษัท คณะกรรมการชุดย่อย และผู้บริหารระดับสูง ที่มีบทบาทในการกำหนดนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ กำกับดูแล และติดตามผลการดำเนินงานให้เป็นไปตามนโยบายและกรอบการกำกับดูแลขององค์กร
2. พนักงานและบุคลากรทุกระดับ รวมถึงผู้ปฏิบัติงานที่มีหน้าที่ใช้งานระบบสารสนเทศหรือบริหารจัดการระบบเทคโนโลยีสารสนเทศให้มีความปลอดภัย
3. หน่วยงานภายในทั้งหมดที่เกี่ยวข้องกับการพัฒนา การดูแลรักษา การใช้งาน หรือการบริหารจัดการระบบเทคโนโลยีสารสนเทศ ข้อมูลดิจิทัล และระบบสนับสนุนอื่น ๆ ขององค์กร
4. คู่ค้า ผู้ให้บริการภายนอก พันธมิตรทางธุรกิจ กิจการร่วมค้า และบุคคลที่เกี่ยวข้องที่มีหน้าที่เข้าถึงหรือดำเนินกิจกรรมใด ๆ ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศหรือข้อมูลขององค์กร โดยอยู่ภายใต้ข้อกำหนดด้านความมั่นคงปลอดภัยตามที่ระบุไว้ในสัญญา หรือข้อตกลงว่าด้วยการให้บริการ

นโยบายนี้ให้ใช้บังคับควบคู่กับระเบียบ ประกาศ หรือแนวทางปฏิบัติภายในอื่น ๆ ที่องค์กรกำหนดไว้ โดยมีผลครอบคลุมถึงระบบและบริการทางดิจิทัลทุกประเภทที่องค์กรนำมาใช้ในการดำเนินธุรกิจ

3. คำจำกัดความ (Definitions)

เพื่อให้การปฏิบัติตามนโยบายการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศเป็นไปอย่างมีประสิทธิภาพ ชัดเจน และอยู่บนพื้นฐานของความเข้าใจที่เป็นมาตรฐานเดียวกันในทุกระดับขององค์กร บริษัทจึงกำหนดคำจำกัดความของคำศัพท์ที่เกี่ยวข้องกับนโยบายฉบับนี้ไว้ดังต่อไปนี้

คำศัพท์	ความหมาย
1. บริษัท (Company)	บริษัท กรุงเทพดุสิตเวชการ จำกัด (มหาชน)
2. บริษัทย่อย	บริษัทที่บริษัท กรุงเทพดุสิตเวชการ จำกัด (มหาชน) มีอำนาจควบคุมการดำเนินงาน
3. องค์กร	บริษัท กรุงเทพดุสิตเวชการ จำกัด (มหาชน) และบริษัทย่อย
4. ความมั่นคงปลอดภัยสารสนเทศ (Information Security)	การรักษาและปกป้องความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูลและระบบสารสนเทศ จากการเข้าถึง การใช้ การเปิดเผย การเปลี่ยนแปลง หรือการทำลายโดยไม่ได้รับอนุญาต
5. ข้อมูลส่วนบุคคลด้านสุขภาพ (Personal Health Information: PHI)	ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับสุขภาพกายหรือจิตใจ การให้บริการทางการแพทย์ การวินิจฉัยโรค หรือประวัติการรักษาของบุคคลซึ่งสามารถระบุตัวตนได้โดยตรงหรือโดยอ้อม
6. ระบบเทคโนโลยีสารสนเทศ (Information Technology Systems)	ระบบ โครงสร้างพื้นฐาน โปรแกรมประยุกต์ และอุปกรณ์ที่ใช้ในการจัดเก็บ ประมวลผล ส่งผ่าน หรือรักษาข้อมูลสารสนเทศภายในองค์กร
7. ปัญญาประดิษฐ์ (Artificial Intelligence: AI)	ระบบหรือเทคโนโลยีที่สามารถเลียนแบบการตัดสินใจ การเรียนรู้ หรือการวิเคราะห์ของมนุษย์ โดยอาศัยข้อมูล อัลกอริทึม หรือแบบจำลองเชิงสถิติ
8. ทรัพย์สินสารสนเทศ (Information Assets)	ข้อมูล ระบบ เครือข่าย แอปพลิเคชัน ซอฟต์แวร์ ฮาร์ดแวร์ และองค์ความรู้ที่มีมูลค่าและความสำคัญต่อการดำเนินธุรกิจขององค์กร
9. เทคโนโลยีสารสนเทศและการสื่อสาร (Information and Communication Technology – ICT)	เทคโนโลยีที่ใช้ในการจัดเก็บ ประมวลผล ถ่ายทอด และแลกเปลี่ยนข้อมูลสารสนเทศ ทั้งในรูปแบบของข้อความ เสียง ภาพ และข้อมูลดิจิทัล โดยรวมถึงอุปกรณ์ฮาร์ดแวร์ ซอฟต์แวร์ เครือข่ายคอมพิวเตอร์ ระบบโทรคมนาคม และเครื่องมือดิจิทัลอื่น ๆ ที่สนับสนุนการสื่อสารภายในองค์กรและกับบุคคลภายนอก ทั้งนี้เทคโนโลยีสารสนเทศและการสื่อสารถือเป็นองค์ประกอบสำคัญที่รองรับการดำเนินงาน การให้บริการ และการบริหารจัดการขององค์กรในยุคดิจิทัล
10. บุคคลภายนอก (Third Party)	บุคคลหรือหน่วยงานที่มิใช่พนักงานขององค์กร แต่มีหน้าที่เข้าถึงหรือให้บริการที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ เช่น ผู้รับจ้าง ผู้ให้บริการคลาวด์ ผู้พัฒนาแอปพลิเคชัน หรือคู่ค้า
11. ภัยคุกคามไซเบอร์ (Cyber Threat)	เหตุการณ์หรือการกระทำใด ๆ ที่อาจเป็นอันตรายหรือส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูล ระบบ หรือโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ
12. ช่องโหว่ (Vulnerability)	จุดอ่อนหรือข้อบกพร่องในระบบ เทคโนโลยี กระบวนการ หรือพฤติกรรมของผู้ใช้งาน ที่อาจถูกใช้เป็นช่องทางในการโจมตีหรือเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

4. **โครงสร้างการกำกับดูแล** (Governance Structure)

บริษัทกำหนดให้การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศเป็นความรับผิดชอบร่วมของทุกฝ่ายภายในองค์กร โดยได้จัดให้มีโครงสร้างการบริหารงานอย่างเป็นทางการ พร้อมทั้งกำหนดบทบาท หน้าที่ และความรับผิดชอบของหน่วยงานและบุคลากรที่เกี่ยวข้องไว้อย่างชัดเจน เพื่อให้กระบวนการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยดำเนินไปอย่างมีประสิทธิภาพ โปร่งใส และสามารถตรวจสอบย้อนกลับได้

การดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร เป็นไปตามหลักการ “Three Lines of Defense” ซึ่งเป็นแนวทางการแบ่งหน้าที่ความรับผิดชอบที่ได้รับการยอมรับในระดับสากล โดยมีวัตถุประสงค์เพื่อเสริมสร้างการกำกับดูแลกิจการที่ดี (Good Governance) ป้องกันความขัดแย้งทางผลประโยชน์ และเพิ่มประสิทธิภาพในการควบคุมภายใน โดยแบ่งออกเป็น 3 แนวป้องกัน ดังนี้

4.1 **แนวป้องกันที่หนึ่ง** (First Line of Defense): **หน่วยงานปฏิบัติด้านเทคโนโลยีสารสนเทศ**

หน่วยงานที่มีบทบาทในการปฏิบัติงานโดยตรงตามภารกิจหลักขององค์กร ซึ่งรวมถึงหน่วยงานผู้ใช้งานระบบเทคโนโลยีสารสนเทศ และหน่วยงานที่รับผิดชอบในการดำเนินงานด้านระบบสารสนเทศในระดับปฏิบัติการ โดยมีหน้าที่ในการระบุ ประเมิน ควบคุม และจัดการความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินงานประจำวันอย่างเหมาะสม รวมถึงต้องปฏิบัติงานให้เป็นไปตามนโยบาย มาตรการ และแนวทางปฏิบัติด้านความมั่นคงปลอดภัยขององค์กรอย่างเคร่งครัด

4.2 **แนวป้องกันที่สอง** (Second Line of Defense): **หน่วยงานกำกับและสนับสนุนการควบคุมความเสี่ยง**

หน่วยงานที่มีบทบาทในการกำกับ ติดตาม และประเมินความเพียงพอของกระบวนการบริหารจัดการความเสี่ยงตลอดจนสนับสนุนการปฏิบัติงานของแนวป้องกันที่หนึ่งให้สอดคล้องกับนโยบาย มาตรฐาน และข้อกำหนดด้านความมั่นคงปลอดภัยขององค์กร โดยมีหน้าที่ในการให้คำแนะนำเกี่ยวกับการจัดการความเสี่ยง การพัฒนากรอบการควบคุมภายใน การจัดทำแนวปฏิบัติและเครื่องมือช่วยในการบริหารความเสี่ยง การกำกับดูแลการปฏิบัติตามกฎระเบียบและการจัดทำรายงานเพื่อนำเสนอผู้บริหารระดับสูงหรือคณะกรรมการกำกับดูแลที่เกี่ยวข้อง

4.3 **แนวป้องกันที่สาม** (Third Line of Defense): **หน่วยงานที่ทำหน้าที่ตรวจสอบด้านเทคโนโลยีสารสนเทศ**

หน่วยงานตรวจสอบภายใน (Internal Audit) มีบทบาทในการตรวจสอบและประเมินระบบการควบคุมภายใน การบริหารจัดการความเสี่ยง และการปฏิบัติตามนโยบายด้านเทคโนโลยีสารสนเทศขององค์กรอย่างเป็นอิสระจากสายงานปฏิบัติการ ทั้งนี้ เพื่อให้การกำกับดูแลมีความรอบด้าน และสามารถให้ความเชื่อมั่นในประสิทธิผลของการควบคุมและการบริหารความเสี่ยงสารสนเทศได้อย่างเที่ยงธรรมและเชื่อถือได้

โครงสร้างดังกล่าวได้รับการออกแบบให้สอดคล้องกับกรอบการบริหารจัดการความเสี่ยงระดับองค์กร (Enterprise Risk Management: ERM) และหลักการกำกับดูแลที่ดี เพื่อให้การบริหารจัดการด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศมีประสิทธิผล มีความยืดหยุ่นต่อการเปลี่ยนแปลง และสามารถตอบสนองต่อภัยคุกคามที่ซับซ้อนในยุคดิจิทัลได้อย่างเหมาะสม

5. บทบาท หน้าที่และความรับผิดชอบตามโครงสร้างการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

เพื่อให้การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์กรเป็นไปอย่างมีประสิทธิภาพ เป็นระบบ และสามารถตรวจสอบได้ บริษัทได้กำหนดบทบาท หน้าที่ และความรับผิดชอบของหน่วยงานและบุคลากรในแต่ละระดับให้สอดคล้องกับโครงสร้างการกำกับดูแลและหลักการแบ่งแยกหน้าที่ความรับผิดชอบตามแนวทาง “Three Lines of Defense” ดังต่อไปนี้

5.1 คณะกรรมการนโยบายการบริหารจัดการความปลอดภัยสารสนเทศ (Information Security Management Committee: ISMC)

บริษัทกำหนดให้มีคณะกรรมการนโยบายการบริหารจัดการความปลอดภัยสารสนเทศ (Information Security Management Committee: ISMC) ทำหน้าที่เป็นกลไกหลักในการกำหนดทิศทางเชิงกลยุทธ์ กำกับดูแล และติดตามการดำเนินงานด้านเทคโนโลยีสารสนเทศและการรักษาความมั่นคงปลอดภัยของข้อมูลในระดับองค์กร (Governance Body) โดยคณะกรรมการชุดนี้ประกอบด้วยผู้บริหารระดับสูงจากหลายสายงานที่เกี่ยวข้อง และทำหน้าที่เป็นตัวกลางเชื่อมโยงนโยบายระดับคณะกรรมการบริษัทกับการดำเนินงานในระดับปฏิบัติการ โดยมีหน้าที่หลัก ดังนี้

- กำหนดนโยบายหลัก กลยุทธ์ และแนวทางในการบริหารจัดการเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยของข้อมูลให้สอดคล้องกับทิศทางองค์กร มาตรฐานสากล และข้อกำหนดของหน่วยงานกำกับดูแลที่เกี่ยวข้อง
- พิจารณา ให้ความเห็นชอบ และ/หรืออนุมัติแนวทางเชิงนโยบาย มาตรการควบคุมภายใน และโครงการที่มีความสำคัญเชิงกลยุทธ์ในด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity)
- กำกับและติดตามผลการดำเนินงานตามนโยบายความมั่นคงปลอดภัยสารสนเทศ รวมถึงการประเมินความเสี่ยงและการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย เพื่อให้มั่นใจว่าการดำเนินงานเป็นไปตามนโยบายและเป้าหมายที่กำหนด
- ส่งเสริมและสนับสนุนการจัดสรรทรัพยากรที่จำเป็น เช่น การพัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัย การดำเนินการฝึกอบรมบุคลากร เพื่อเสริมสร้างศักยภาพขององค์กรให้สามารถบริหารจัดการด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยได้อย่างมีประสิทธิภาพและยั่งยืน

5.2 หน่วยงานธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ (Enterprise IT Governance Office)

บริษัทกำหนดให้หน่วยงานธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ ทำหน้าที่เป็นแนวป้องกันลำดับที่สอง (Second Line of Defense) ในการกำกับ ติดตาม และสนับสนุนการดำเนินงานด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศในระดับองค์กร โดยมีบทบาทสำคัญในการส่งเสริมให้หน่วยงานปฏิบัติงาน (First Line of Defense) ดำเนินการตามนโยบายและมาตรการควบคุมที่กำหนดไว้อย่างมีประสิทธิภาพ และสอดคล้องกับกฎหมายและข้อกำหนดที่เกี่ยวข้อง โดยมีหน้าที่หลัก ดังนี้

- กำหนดแนวทางและพัฒนา ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ให้ครอบคลุมทั้งด้านนโยบาย มาตรการควบคุม และกระบวนการจัดการความเสี่ยง
- ติดตาม ตรวจสอบ และประเมินความเพียงพอของมาตรการควบคุม รวมถึงการปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยของหน่วยงานปฏิบัติ เพื่อให้มั่นใจว่ามีการบริหารจัดการความเสี่ยงอย่างเหมาะสม
- พัฒนาเครื่องมือ แนวปฏิบัติ และให้คำแนะนำแก่หน่วยงานต่าง ๆ ในการประเมินและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและปัญญาประดิษฐ์ (AI) อย่างครอบคลุม

- จัดทำรายงานวิเคราะห์และรายงานสรุปผลด้านความเสี่ยงสารสนเทศ เพื่อนำเสนอแก่คณะกรรมการนโยบายการบริหารจัดการความปลอดภัยสารสนเทศ (ISMC) ผู้บริหารระดับสูงหรือคณะกรรมการที่ได้รับมอบหมาย เพื่อประกอบการตัดสินใจ
- ส่งเสริมการสร้างวัฒนธรรมความตระหนักด้านความมั่นคงปลอดภัยผ่านการอบรมและการสื่อสารภายในองค์กรอย่างต่อเนื่อง

5.3 **เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล** (Data Protection Officer: DPO)

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เป็นบุคลากรที่ได้รับมอบหมายให้ทำหน้าที่ในฐานะแนวป้องกันระดับที่สอง (Second Line of Defense) โดยมีบทบาทในการกำกับดูแลและส่งเสริมการปฏิบัติตามกฎหมายและข้อกำหนดด้านการคุ้มครองข้อมูลส่วนบุคคล ทั้งในระดับองค์กรและระดับปฏิบัติการ เพื่อให้การจัดเก็บ การใช้ การเปิดเผย และการประมวลผลข้อมูลส่วนบุคคลเป็นไปอย่างถูกต้อง เหมาะสม และสอดคล้องกับกรอบกฎหมายที่เกี่ยวข้อง เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) ตลอดจนข้อกำหนดเฉพาะด้านข้อมูลสุขภาพส่วนบุคคล (Personal Health Information: PHI) ตามมาตรฐานที่เกี่ยวข้องในบริบทของการให้บริการด้านสุขภาพ และการประยุกต์ใช้เทคโนโลยีดิจิทัลหรือปัญญาประดิษฐ์ (AI) ที่เกี่ยวข้องกับข้อมูลอ่อนไหว โดยมีหน้าที่หลัก ดังนี้

- กำกับดูแลและติดตามการดำเนินงานขององค์กรให้สอดคล้องกับข้อกำหนดของ PDPA และมาตรฐานที่เกี่ยวข้องกับการคุ้มครองข้อมูลสุขภาพ
- ประเมินความเสี่ยงด้านข้อมูลส่วนบุคคลและสนับสนุนการดำเนินการประเมินผลกระทบด้านการคุ้มครองข้อมูล (Data Protection Impact Assessment: DPIA) โดยเฉพาะในกรณีที่มีการนำเทคโนโลยีปัญญาประดิษฐ์ (AI) มาใช้ในการประมวลผลข้อมูลสุขภาพส่วนบุคคล
- ให้คำปรึกษา แนะนำ และสนับสนุนหน่วยงานภายในองค์กรในเรื่องการปฏิบัติตามกฎหมายและแนวปฏิบัติที่เกี่ยวข้องกับข้อมูลส่วนบุคคล
- ดำเนินการตรวจสอบเบื้องต้น กำกับ ติดตาม และรายงานเหตุการณ์การละเมิดข้อมูล (Data Breach) ให้กับหน่วยงานที่มีหน้าที่รับผิดชอบ รวมถึงการรายงานต่อหน่วยงานกำกับดูแลภายนอกตามที่กฎหมายกำหนด
- ส่งเสริมการสร้างความตระหนักรู้ (Awareness) ด้านการคุ้มครองข้อมูลส่วนบุคคลให้แก่บุคลากรทุกระดับในองค์กร

5.4 **หน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ**

หน่วยงานปฏิบัติทำหน้าที่เป็นแนวป้องกันลำดับแรกขององค์กร (First Line of Defense) โดยมีบทบาทในการดำเนินการตามภารกิจที่ได้รับมอบหมายภายใต้กรอบนโยบาย มาตรการ และแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศขององค์กรอย่างเคร่งครัด ทั้งนี้ เพื่อให้สามารถควบคุมและจัดการความเสี่ยงได้อย่างมีประสิทธิภาพ โดยมีหน้าที่หลัก ดังนี้

- ปฏิบัติงานตามบทบาทและความรับผิดชอบที่ได้รับมอบหมาย โดยยึดถือหลักการด้านความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศอย่างเคร่งครัด และให้เป็นไปตามนโยบายและมาตรฐานที่องค์กรกำหนด
- ระบุ ประเมิน และจัดการความเสี่ยงที่เกี่ยวข้องกับการปฏิบัติงานประจำวันอย่างเหมาะสม พร้อมทั้งรายงานเหตุการณ์ผิดปกติ ช่องโหว่ หรือข้อบกพร่องที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูลหรือระบบต่อผู้มีหน้าที่กำกับดูแลโดยทันที เพื่อให้สามารถดำเนินการตรวจสอบ แก้ไข และจัดการความเสี่ยงได้อย่างทันท่วงที

- บันทึกและจัดเก็บหลักฐาน ข้อมูล หรือรายการควบคุมที่เกี่ยวข้องกับการดำเนินงานด้านการควบคุมภายใน เพื่อสนับสนุนการตรวจสอบ การประเมินผล และการปรับปรุงมาตรการควบคุมอย่างต่อเนื่อง

5.5 **ฝ่ายตรวจสอบภายใน** (Internal Audit)

บริษัทกำหนดให้ฝ่ายตรวจสอบภายในทำหน้าที่เป็นแนวป้องกันระดับที่สาม (Third Line of Defense) โดยมีบทบาทในการประเมินระบบการควบคุมภายใน การบริหารจัดการความเสี่ยง และระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอย่างอิสระจากสายงานปฏิบัติ เพื่อสร้างความมั่นใจแก่คณะกรรมการตรวจสอบและผู้บริหารระดับสูงในการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กร โดยมีหน้าที่และความรับผิดชอบหลัก ดังนี้

- ดำเนินการตรวจสอบระบบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ การบริหารความเสี่ยง และกระบวนการควบคุมภายใน เพื่อประเมินความเพียงพอและประสิทธิผลของการควบคุมภายใน และความสอดคล้องของการดำเนินงานกับนโยบาย มาตรฐาน และข้อกำหนดที่เกี่ยวข้อง
- จัดทำรายงานผลการตรวจสอบเพื่อนำเสนอข้อตรวจพบและข้อเสนอแนะในการปรับปรุงแก้ไข ต่อคณะกรรมการตรวจสอบ (Audit Committee) โดยตรงและนำส่งผู้บริหารระดับสูงที่เกี่ยวข้องต่อไป เพื่อใช้ประกอบการตัดสินใจเชิงกลยุทธ์
- ให้ข้อเสนอแนะเชิงปรับปรุงที่มุ่งเน้นการยกระดับประสิทธิภาพและประสิทธิผลของระบบควบคุมภายในและกระบวนการบริหารความเสี่ยงขององค์กร
- สนับสนุนการเสริมสร้างวัฒนธรรมการควบคุมภายในและธรรมาภิบาลที่ดี (Good Governance) ภายในองค์กรอย่างต่อเนื่อง

6. **แนวทางปฏิบัติในการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ**

นโยบายฉบับนี้จัดทำขึ้นโดยอ้างอิงตามมาตรฐานสากลด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ได้แก่ ISO/IEC 27001:2022 และ ISO 27799:2016 ตลอดจนข้อกำหนดตามกฎหมาย กฎระเบียบ และแนวทางปฏิบัติที่ออกโดยหน่วยงานกำกับดูแลที่เกี่ยวข้อง เพื่อให้เป็นกรอบการดำเนินงานในการคุ้มครองและบริหารจัดการทรัพย์สินสารสนเทศของ องค์กรเป็นไปอย่างมีประสิทธิภาพ

แนวทางปฏิบัติในนโยบายนี้ครอบคลุมการบริหารจัดการในมิติต่าง ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศขององค์กร โดยมีวัตถุประสงค์เพื่อป้องกันความเสียหาย การสูญหาย หรือการเข้าถึงโดยไม่ได้รับอนุญาต ซึ่งอาจส่งผลกระทบต่อความน่าเชื่อถือความต่อเนื่องทางธุรกิจ และการคุ้มครองข้อมูลส่วนบุคคลของผู้รับบริการ ทั้งนี้ แนวทางปฏิบัติที่กำหนดไว้ครอบคลุมประเด็นสำคัญ 4 หมวดหมู่หลัก ดังนี้

6.1 **มาตรการควบคุมด้านองค์กร** (Organizational Controls)

มาตรการควบคุมด้านองค์กร หมายถึง การกำหนดนโยบาย กระบวนการ และกรอบการกำกับดูแลที่เป็นระบบ เพื่อสนับสนุนการบริหารจัดการด้านความมั่นคงปลอดภัยของสารสนเทศในระดับองค์รวมขององค์กร โดยมุ่งเน้นการวางรากฐานด้านธรรมาภิบาล (Governance) การปฏิบัติตามกฎหมายที่เกี่ยวข้อง มาตรฐานสากล และข้อกำหนดของหน่วยงานกำกับดูแล

มาตรการเหล่านี้มีบทบาทสำคัญในการกำหนดวิสัยทัศน์ ทิศทาง และกลยุทธ์ด้านความมั่นคงปลอดภัยของสารสนเทศ เชื่อมโยงบทบาทและความรับผิดชอบของหน่วยงานต่าง ๆ ตลอดจนกำกับดูแลและควบคุมความเสี่ยงในภาพรวมขององค์กรอย่างมีประสิทธิภาพ ทั้งนี้ แนวทางการควบคุมด้านองค์กรครอบคลุมประเด็นสำคัญ ดังต่อไปนี้

6.1.1 **การกำหนดบทบาทและความรับผิดชอบในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ** (Organization of information technology security)

เพื่อให้การบริหารจัดการความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศขององค์กรเป็นไปอย่างมีประสิทธิภาพ โปร่งใส และสามารถตรวจสอบย้อนหลังได้อย่างเหมาะสม องค์กรต้องกำหนดบทบาทและความรับผิดชอบของหน่วยงานและบุคลากรที่เกี่ยวข้องไว้อย่างชัดเจน ครอบคลุมทั้งในระดับนโยบาย และระดับปฏิบัติการ โดยพิจารณาตามหลักเกณฑ์สำคัญ ดังต่อไปนี้

6.1.1.1 องค์กรต้องกำหนดบทบาทหน้าที่และความรับผิดชอบของบุคลากรที่เกี่ยวข้องกับการบริหารจัดการและการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศให้ชัดเจน เป็นลายลักษณ์อักษร และต้องมีการสื่อสารไปยังทุกระดับขององค์กรอย่างทั่วถึง เพื่อเสริมสร้างความเข้าใจร่วมกัน และส่งเสริมให้การปฏิบัติงานเป็นไปอย่างมีประสิทธิภาพและสอดคล้องกับเป้าหมายด้านความมั่นคงปลอดภัยขององค์กร

6.1.1.2 จัดตั้งคณะกรรมการหรือคณะทำงานที่มีอำนาจหน้าที่ในการกำกับดูแล ทบทวนนโยบาย มาตรการและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าการดำเนินงานสอดคล้องกับมาตรฐาน กฎหมาย และข้อกำหนดที่เกี่ยวข้อง รวมทั้งสนับสนุนการตัดสินใจเชิงกลยุทธ์และการบริหารความเสี่ยงเชิงระบบ

6.1.1.3 กำหนดให้มีการแบ่งแยกบทบาท หน้าที่ และอำนาจในการดำเนินงานที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศอย่างเหมาะสม เพื่อป้องกันความขัดแย้งทางผลประโยชน์ (Conflict of Interest) และลดความเสี่ยงจากข้อผิดพลาดหรือการกระทำที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัย เช่น การแยกหน้าที่ของผู้พัฒนาระบบ (Developer) ออกจากผู้ที่มีสิทธิอนุมัติการนำระบบขึ้นใช้งานจริง (Production Deployment Authorizer)

6.1.1.4 จัดให้มีกระบวนการติดตาม ตรวจสอบ และประเมินผลการปฏิบัติงานของบุคลากรที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างสม่ำเสมอ และต่อเนื่อง โดยมุ่งเน้นการประเมินความสอดคล้องกับนโยบาย มาตรการควบคุม และข้อกำหนดที่องค์กรกำหนดไว้ รวมทั้งสามารถใช้เป็นข้อมูลในการปรับปรุงและพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยให้ตอบสนองต่อความเสี่ยงที่เปลี่ยนแปลงได้อย่างทันท่วงที

6.1.2 **การบริหารจัดการนโยบายความมั่นคงสารสนเทศ** (Policies for Information Security)

บริษัทตระหนักถึงความจำเป็นในการกำหนดนโยบายด้านความมั่นคงปลอดภัยสารสนเทศอย่างชัดเจน ครอบคลุม และเหมาะสมกับบริบทขององค์กร เพื่อใช้เป็นแนวทางในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ตลอดจนการใช้ข้อมูลและระบบสารสนเทศอย่างปลอดภัย โดยมีแนวทางปฏิบัติดังต่อไปนี้

6.1.2.1 องค์กรต้องจัดทำนโยบายด้านความมั่นคงปลอดภัยสารสนเทศที่ครอบคลุมประเด็นสำคัญ เช่น การควบคุมการเข้าถึงข้อมูล การจัดการภัยคุกคามไซเบอร์ การใช้เทคโนโลยีสารสนเทศอย่างปลอดภัย การบริหารจัดการความเสี่ยง และการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย

6.1.2.2 นโยบายดังกล่าวต้องได้รับการอนุมัติจากผู้บริหารระดับสูง และมีการเผยแพร่ให้บุคลากรทุกระดับรับทราบ เข้าใจ และถือปฏิบัติอย่างเคร่งครัด โดยอาจใช้ช่องทางภายใน เช่น เอกสารอิเล็กทรอนิกส์ อินทราเน็ต หรือการฝึกอบรม

6.1.2.3 องค์กรต้องมีการทบทวน ปรับปรุง และอนุมัตินโยบายอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญด้านเทคโนโลยี กฎหมาย หรือข้อกำหนดจากหน่วยงานกำกับดูแล ทั้งนี้ เพื่อให้แน่ใจว่านโยบายยังคงมีความเหมาะสม ทันสมัย และรองรับความเสี่ยงที่อาจเกิดขึ้นได้อย่างมีประสิทธิภาพ

6.1.2.4 การบริหารจัดการนโยบายด้านความมั่นคงปลอดภัยสารสนเทศต้องดำเนินการภายใต้หลักธรรมาภิบาลและความโปร่งใส โดยต้องมีการบันทึกเวอร์ชันของนโยบาย ติดตามการรับทราบของผู้ใช้งาน และสามารถตรวจสอบย้อนหลังได้

6.1.2.5 องค์กรต้องจัดให้มีระบบหรือกลไกสนับสนุนการปฏิบัติตามนโยบาย เช่น คู่มือแนวปฏิบัติ ขั้นตอนการดำเนินงาน และการกำกับติดตามการปฏิบัติอย่างต่อเนื่อง เพื่อส่งเสริมการบังคับใช้นโยบายอย่างเป็นรูปธรรม

6.1.3 **การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ** (IT Asset Management)

บริษัทตระหนักว่าทรัพย์สินด้านเทคโนโลยีสารสนเทศมีความสำคัญต่อความมั่นคงปลอดภัยของระบบงานและข้อมูล โดยเฉพาะในยุคที่องค์กรมีการใช้งานระบบดิจิทัลและเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) อย่างแพร่หลาย จึงกำหนดให้มีการบริหารจัดการทรัพย์สินสารสนเทศอย่างเป็นระบบครอบคลุมทั้งฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล เครือข่าย สัญญา และบริการจากภายนอก ตลอดจนโค้ด โมเดล และแพลตฟอร์ม AI โดยมีข้อกำหนดสำคัญ ดังนี้

6.1.3.1 องค์กรต้องดำเนินการจัดทำและบำรุงรักษาทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Asset Register) อย่างเป็นระบบ โดยระบุรายละเอียดที่จำเป็น เช่น ประเภทของทรัพย์สิน หมายเลขประจำทรัพย์สิน ผู้รับผิดชอบดูแล สถานะการใช้งาน และตำแหน่งที่ตั้ง เพื่อให้สามารถติดตาม ตรวจสอบ และควบคุมการใช้ทรัพย์สินได้อย่างมีประสิทธิภาพ

6.1.3.2 ต้องมีการการระบุเจ้าของหรือผู้ครอบครองทรัพย์สินอย่างชัดเจนสำหรับทรัพย์สินแต่ละรายการ ทั้งนี้ เจ้าของทรัพย์สินมีหน้าที่รับผิดชอบหลักในการควบคุม ดูแล และบริหารจัดการทรัพย์สินดังกล่าวให้มีความมั่นคงปลอดภัยและสอดคล้องกับนโยบายขององค์กร

6.1.3.3 การใช้งานทรัพย์สินด้านเทคโนโลยีสารสนเทศขององค์กรต้องอยู่ภายใต้ข้อกำหนดที่ชัดเจน และเป็นไปเพื่อวัตถุประสงค์ในการดำเนินธุรกิจขององค์กร เท่านั้น ห้ามนำทรัพย์สินไปใช้ส่วนตัว หรือใช้ผิดวัตถุประสงค์ หรือภายนอกขอบเขตที่ได้รับอนุญาตอย่างเด็ดขาด

6.1.3.4 องค์กรต้องจัดให้มีมาตรการควบคุมการเข้าถึง การเคลื่อนย้าย และการนำทรัพย์สินออกนอกสถานที่อย่างเหมาะสม โดยเฉพาะในกรณีของทรัพย์สินที่บรรจุข้อมูลสำคัญหรือข้อมูลอ่อนไหว ทั้งนี้เพื่อป้องกันการสูญหาย การรั่วไหล หรือการเข้าถึงโดยไม่ได้รับอนุญาต

6.1.3.5 การดำเนินการซ่อมบำรุง การอัปเกรด หรือการทำลายทรัพย์สิน ต้องเป็นไปตามขั้นตอนที่กำหนด และอยู่ภายใต้มาตรการควบคุมความมั่นคงปลอดภัย โดยต้องมีการบันทึกข้อมูลที่เกี่ยวข้องอย่างครบถ้วนเพื่อให้สามารถตรวจสอบย้อนหลังได้

6.1.3.6 องค์กรต้องดำเนินการตรวจสอบความถูกต้องของรายการทรัพย์สินอย่างน้อยปีละหนึ่งครั้ง และจัดให้มีการทบทวนทะเบียนทรัพย์สินอย่างต่อเนื่อง เพื่อให้มั่นใจว่าข้อมูลในทะเบียนยังคงถูกต้องครบถ้วน และสอดคล้องกับสถานะการใช้งานจริงของทรัพย์สิน

6.1.4 **การรักษาความมั่นคงปลอดภัยของข้อมูล** (Information Security)

บริษัทตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ (Information Security) อันเป็นทรัพยากรหลักที่มีมูลค่าสูงและมีบทบาทสำคัญต่อความต่อเนื่องทางธุรกิจ ความเชื่อมั่นของลูกค้า และการปฏิบัติตามข้อกำหนดตามกฎหมาย มาตรฐาน และข้อกำกับภายนอก โดยเฉพาะในบริบทของการใช้ เทคโนโลยีดิจิทัล และ ระบบปัญญาประดิษฐ์ (Artificial Intelligence: AI) ซึ่งมีความซับซ้อนและอ่อนไหวมากยิ่งขึ้น บริษัทจึงกำหนดแนวทางในการควบคุมและปกป้องข้อมูลอย่างรอบด้าน ดังนี้

6.1.4.1 องค์กรต้องดำเนินการกำหนดระดับความสำคัญของข้อมูล (Information Classification) อย่างเป็นระบบ โดยพิจารณาจากระดับความอ่อนไหวและผลกระทบที่อาจเกิดขึ้นจากการเข้าถึงหรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต พร้อมทั้งกำหนดมาตรการควบคุมการจัดเก็บ การใช้งาน และการส่งต่อข้อมูลให้สอดคล้องกับระดับความสำคัญของข้อมูลแต่ละประเภท

6.1.4.2 องค์กรต้องจัดให้มีมาตรการควบคุมการเข้าถึงข้อมูลที่เหมาะสมและเพียงพอ โดยอ้างอิงตามบทบาทหน้าที่ของผู้ใช้งาน (Role-Based Access Control) และจำกัดการเข้าถึงข้อมูลเฉพาะบุคคลที่ได้รับอนุญาตจากเจ้าของข้อมูลหรือผู้มีอำนาจที่เกี่ยวข้อง ทั้งนี้เพื่อป้องกันการเข้าถึง การแก้ไข หรือการเปิดเผยข้อมูลโดยมิชอบ

6.1.4.3 การจัดเก็บ การรับส่ง และการประมวลผลข้อมูลที่มีความสำคัญหรืออ่อนไหว ต้องดำเนินการโดยใช้เทคโนโลยีที่ปลอดภัยและได้รับการรับรองตามมาตรฐานสากล เช่น การเข้ารหัสข้อมูล (Data Encryption) การสำรองข้อมูล (Backup and Recovery) และการควบคุมสิทธิ์การเข้าถึง (Access Control Mechanism) เพื่อให้มั่นใจว่าข้อมูลจะได้รับการปกป้องตลอดวงจรชีวิตของข้อมูล

6.1.4.4 จัดให้มีการใช้เทคนิคการปกปิดข้อมูล (Data Masking) สำหรับข้อมูลที่มีความอ่อนไหวหรือข้อมูลส่วนบุคคล โดยเฉพาะในการพัฒนา ทดสอบระบบ หรือวิเคราะห์ข้อมูลในสภาพแวดล้อมที่ไม่ใช่ระบบที่ใช้งานจริง (non-production environment) เพื่อป้องกันการเปิดเผยข้อมูลที่สามารถระบุตัวบุคคลได้ ทั้งนี้ต้องเลือกใช้วิธีการปกปิดที่เหมาะสมกับลักษณะของข้อมูลและวัตถุประสงค์ของการใช้งาน

6.1.4.5 ต้องดำเนินการควบคุมความเสี่ยงด้านการรั่วไหลของข้อมูล (Data Leakage Prevention – DLP) อย่างครอบคลุมและเป็นระบบ โดยบูรณาการการใช้เครื่องมือควบคุม เช่น ระบบตรวจจับและป้องกันการรั่วไหลของข้อมูลผ่านช่องทางต่าง ๆ (DLP Agents) การเข้ารหัสข้อมูลที่ส่งออก (Data

Encryption at Transit) และการตั้งค่าควบคุมสิทธิ์การใช้งานสื่อจัดเก็บข้อมูลแบบพกพา (Removable Media Control)

6.1.4.6 จัดให้มีการตรวจสอบความมั่นคงปลอดภัยของข้อมูลอย่างสม่ำเสมอ รวมถึงการติดตั้งระบบตรวจสอบและติดตามการใช้งานข้อมูล (Monitoring and Logging) และระบบแจ้งเตือนความเสี่ยง (Security Alert) เช่น Splunk, Symantec DLP, Elastic Stack เพื่อให้สามารถตรวจพบความผิดปกติหรือภัยคุกคามที่อาจกระทบต่อข้อมูลได้อย่างทันท่วงที

6.1.4.7 องค์กรต้องดำเนินการรักษาความมั่นคงปลอดภัยของข้อมูลที่ใช้หรือจัดเก็บภายนอกระบบองค์กร เช่น ระบบคลาวด์ หรือระบบของผู้ให้บริการภายนอก โดยต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยในสัญญา และประเมินความเสี่ยงเป็นระยะ

6.1.4.8 องค์กรต้องจัดให้มีการอบรมและให้ความรู้กับบุคลากรทุกระดับเกี่ยวกับนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยของข้อมูล เช่น การใช้รหัสผ่านอย่างปลอดภัย การจัดการเอกสารสำคัญ และการรายงานเหตุการณ์ผิดปกติ

6.1.4.9 ในกรณีที่เกิดเหตุการณ์ละเมิดข้อมูล (Data Breach) หรือพบความผิดปกติที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูล องค์กรต้องดำเนินการแจ้งเหตุและตอบสนองตามแผนการจัดการเหตุการณ์ (Incident Response Plan) อย่างเป็นระบบ รวดเร็ว และมีประสิทธิภาพ โดยต้องดำเนินการตรวจสอบ สืบค้นสาเหตุ และจัดทำแผนป้องกันการเกิดเหตุซ้ำอย่างเหมาะสม

6.1.4.10 ต้องดำเนินการลบหรือทำลายข้อมูล (Information Deletion) อย่างเหมาะสมเมื่อข้อมูลหมดอายุการใช้งาน สิ้นสุดวัตถุประสงค์ทางธุรกิจ หรือมีการเปลี่ยนแปลงสถานะของข้อมูล ทั้งนี้ต้องใช้วิธีการที่ปลอดภัย เชื่อถือได้ และไม่สามารถกู้คืนข้อมูลได้ เพื่อป้องกันการรั่วไหล การเข้าถึงโดยมิชอบ และเพื่อให้สอดคล้องกับข้อกำหนดของกฎหมายที่เกี่ยวข้อง

6.1.5 **การควบคุมการเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศ** (Access Control)

บริษัทตระหนักว่าการควบคุมการเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศอย่างเหมาะสมและสอดคล้องกับหน้าที่ความรับผิดชอบของผู้ใช้งานเป็นกลไกสำคัญในการรักษาความมั่นคงปลอดภัยของสารสนเทศ และลดความเสี่ยงจากการเข้าถึงโดยมิชอบหรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต โดยกำหนดแนวทางและข้อกำหนดในการควบคุมการเข้าถึง ดังนี้

6.1.5.1 องค์กรต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศตามหลักการ Least Privilege และ Need-to-Know เพื่อให้มั่นใจว่าผู้ใช้งานสามารถเข้าถึงเฉพาะข้อมูล ระบบ หรือทรัพยากรที่จำเป็นต่อการปฏิบัติงานเท่านั้น โดยจำกัดการเข้าถึงส่วนอื่นที่ไม่เกี่ยวข้อง เพื่อป้องกันความเสี่ยงจากการเข้าถึงโดยมิชอบ

6.1.5.2 การกำหนดสิทธิ์การเข้าถึงและบทบาทของผู้ใช้งานในระบบสารสนเทศ ต้องได้รับการอนุมัติจากเจ้าของระบบหรือเจ้าของข้อมูล (System Owner/Data Owner) อย่างชัดเจน โดยมีหลักฐานประกอบการอนุมัติ และต้องสอดคล้องกับหน้าที่ความรับผิดชอบของผู้ใช้งานแต่ละราย

6.1.5.3 ผู้ใช้งานทุกคนควรได้รับรหัสผู้ใช้งานประจำตัวที่ไม่สามารถใช้ร่วมกันได้ และต้องผ่านกระบวนการพิสูจน์ตัวตน (Authentication) ด้วยวิธีการที่เหมาะสมกับระดับความเสี่ยงของระบบ เช่น รหัสผ่านที่มีความซับซ้อน หรือการยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) สำหรับระบบที่มีความสำคัญหรือมีข้อมูลอ่อนไหว

6.1.5.4 การเข้าถึงระบบของผู้ให้บริการภายนอก หรือบุคคลที่มิใช่พนักงานประจำขององค์กร ต้องอยู่ภายใต้เงื่อนไขที่ชัดเจน โดยกำหนดระยะเวลาการเข้าถึงอย่างจำกัด และอยู่ภายใต้การควบคุมของผู้รับผิดชอบภายในองค์กรตลอดระยะเวลาที่ได้รับอนุญาตให้เข้าถึง

6.1.5.5 องค์กรต้องจัดให้มีระบบการบันทึกข้อมูล (Log) และตรวจสอบกิจกรรมที่เกี่ยวข้องกับการเข้าถึงระบบเทคโนโลยีสารสนเทศอย่างต่อเนื่อง เพื่อให้สามารถตรวจสอบย้อนหลังได้ในกรณีที่เกิดเหตุการณ์ผิดปกติ รวมถึงต้องดำเนินการตรวจสอบความถูกต้องและความเหมาะสมของสิทธิ์การเข้าถึงของผู้ใช้งานอย่างน้อยปีละหนึ่งครั้ง

6.1.5.6 กรณีที่มีการเปลี่ยนแปลงสถานะของผู้ใช้งาน เช่น การลาออก การโยกย้ายตำแหน่ง การสิ้นสุดสัญญาการจ้าง หรือการเปลี่ยนบทบาทหน้าที่ องค์กร ต้องดำเนินการปรับเปลี่ยนหรือยกเลิกสิทธิ์การเข้าถึงของผู้ใช้งานรายนั้นโดยทันที เพื่อป้องกันการเข้าถึงระบบโดยไม่มีอำนาจหรือโดยไม่จำเป็น

6.1.5.7 ในกรณีที่มีการเข้าถึงระบบหรือข้อมูลจากบุคคลภายนอก เช่น ผู้ให้บริการภายนอก หรือการใช้ระบบ AI ต้องมีการกำหนดขอบเขตการเข้าถึงอย่างชัดเจน และควบคุมตามระดับความเสี่ยงที่ประเมินไว้ โดยต้องจัดทำบันทึกข้อตกลงหรือสัญญาที่มีข้อกำหนดด้านความมั่นคงปลอดภัยอย่างรัดกุม

6.1.6 การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (IT Security Incident Management)

บริษัทตระหนักว่าการตอบสนองต่อเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ (IT Incident) อย่างทันท่วงทีเป็นปัจจัยสำคัญต่อการรักษาความมั่นคงปลอดภัย ความต่อเนื่องในการให้บริการ และความเชื่อมั่นของผู้มีส่วนได้ส่วนเสียทุกฝ่าย โดยมีแนวทางและข้อกำหนดที่สำคัญ ดังนี้

6.1.6.1 องค์กรต้องจัดให้มีระบบและช่องทางในการแจ้งเหตุการณ์ผิดปกติที่รวดเร็ว ปลอดภัย และเข้าถึงได้ง่าย พร้อมทั้งดำเนินการประเมินผลกระทบเบื้องต้นต่อความต่อเนื่องทางธุรกิจ ความมั่นคงปลอดภัยของข้อมูล และผู้มีส่วนได้ส่วนเสียอย่างเป็นระบบ เพื่อให้สามารถกำหนดระดับความรุนแรงและแนวทางการตอบสนองได้อย่างเหมาะสม

6.1.6.2 ต้องจัดตั้งทีมตอบสนองเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ (Incident Response Team) ที่มีความสามารถในการบริหารจัดการเหตุการณ์อย่างมีประสิทธิภาพ พร้อมทั้งจัดทำคู่มือแนวทางปฏิบัติ (Incident Response Playbook) สำหรับเหตุการณ์แต่ละประเภท เพื่อใช้เป็นแนวทางในการดำเนินการตอบสนองอย่างรวดเร็ว เหมาะสม และสอดคล้องกับลักษณะของเหตุการณ์

6.1.6.3 กำหนดกระบวนการสื่อสารที่ชัดเจน ครอบคลุมช่องทางการสื่อสาร ผู้รับผิดชอบ และข้อความมาตรฐานสำหรับการแจ้งเหตุการณ์ที่มีระดับความรุนแรงสูง เพื่อให้มั่นใจว่าข้อมูลที่เผยแพร่มีความถูกต้อง ทันเวลา และเหมาะสมกับผู้รับสารแต่ละกลุ่ม

6.1.6.4 ดำเนินการบันทึกรายละเอียดของเหตุการณ์ผิดปกติทุกกรณีอย่างครบถ้วน รวมถึงข้อมูลที่เกี่ยวข้องกับระยะเวลา สาเหตุ ผลกระทบ มาตรการที่ดำเนินการ และสถานะการกู้คืนระบบ พร้อมทั้งจัดทำรายงานนำเสนอผู้บริหารระดับสูง หน่วยงานกำกับดูแล และหน่วยงานที่เกี่ยวข้อง เพื่อใช้เป็นข้อมูลในการประเมินและปรับปรุงระบบอย่างต่อเนื่อง

6.1.6.5 ดำเนินการวิเคราะห์หาสาเหตุของเหตุการณ์ (Root Cause Analysis) อย่างเป็นระบบสำหรับเหตุการณ์ทุกรายการ และจัดให้มีการกำหนดและดำเนินการตามแผนการปรับปรุงเพื่อป้องกันการเกิดเหตุซ้ำ (Corrective Action Plan) โดยนำผลการวิเคราะห์และข้อเสนอแนะจากทุกฝ่ายที่เกี่ยวข้องมาปรับใช้เพื่อยกระดับมาตรการควบคุมภายในและเสริมสร้างความมั่นคงปลอดภัยของระบบในระยะยาว

6.1.7 **การจัดการความต่อเนื่องทางธุรกิจ** (Business Continuity Management)

บริษัทตระหนักถึงความสำคัญของการเตรียมความพร้อมและความสามารถในการตอบสนองต่อเหตุการณ์ฉุกเฉินที่ส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศ โดยเฉพาะอย่างยิ่งระบบที่เกี่ยวข้องกับการให้บริการด้านสุขภาพและระบบที่ใช้เทคโนโลยีดิจิทัลหรือปัญญาประดิษฐ์ (AI) ดังนั้น บริษัทจึงกำหนดแนวทางในการจัดทำและบังคับใช้แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) ดังนี้

6.1.7.1 องค์กรต้องจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศให้ครอบคลุมถึงการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) การกู้คืนระบบและข้อมูลที่สำคัญ การบริหารความต่อเนื่องของบริการ (Business Continuity) และการสื่อสารในภาวะวิกฤตอย่างมีประสิทธิภาพ

6.1.7.2 ต้องมีการกำหนดบทบาท หน้าที่ และความรับผิดชอบของหน่วยงานและบุคลากรที่เกี่ยวข้องในการเตรียมความพร้อมและการดำเนินการตามแผนฉุกเฉินอย่างชัดเจน เพื่อให้สามารถตอบสนองต่อเหตุการณ์ได้อย่างรวดเร็วและประสานงานได้อย่างมีประสิทธิผล

6.1.7.3 แผนฉุกเฉินต้องได้รับการทดสอบและฝึกซ้อมเป็นประจำอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เพื่อประเมินประสิทธิภาพของแผน ความพร้อมของบุคลากร และเพื่อระบุช่องว่างที่ต้องปรับปรุง

6.1.7.4 ต้องมีการจัดอบรมและเผยแพร่ความรู้เกี่ยวกับแผนฉุกเฉินให้แก่บุคลากรทุกระดับ เพื่อให้สามารถปฏิบัติตามขั้นตอนที่กำหนดไว้ในแผนได้อย่างถูกต้องและทันต่อเหตุการณ์

6.1.7.5 แผนฉุกเฉินต้องได้รับการทบทวนและปรับปรุงให้ทันสมัยอยู่เสมอ โดยคำนึงถึงการเปลี่ยนแปลงของระบบเทคโนโลยี ภัยคุกคาม ความเสี่ยงใหม่ ๆ รวมถึงข้อกำหนดด้านกฎระเบียบและมาตรฐานที่เกี่ยวข้องทั้งในระดับประเทศและระดับสากล

6.1.8 **การจัดการภัยคุกคามไซเบอร์** (Threat Intelligence Management)

บริษัทตระหนักถึงความสำคัญของการบริหารจัดการข้อมูลข่าวสารด้านภัยคุกคามทางไซเบอร์ (Cyber Threat Intelligence – CTI) ซึ่งเป็นองค์ประกอบสำคัญในการป้องกันและลดความเสี่ยงจากการถูกโจมตีทางไซเบอร์ในรูปแบบต่าง ๆ โดยเฉพาะในบริบทของธุรกิจด้านสุขภาพที่มีการใช้ข้อมูลสุขภาพส่วนบุคคลและระบบ AI ที่มีความอ่อนไหวสูง จึงกำหนดแนวทางปฏิบัติดังต่อไปนี้

6.1.8.1 องค์กรต้องจัดให้มีระบบการติดตามและรวบรวมข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์อย่างต่อเนื่อง จากแหล่งที่เชื่อถือได้ทั้งภายในและภายนอกองค์กร เช่น หน่วยงาน CERT, Threat Feeds, ระบบ SIEM และผู้ให้บริการด้านความมั่นคงปลอดภัยสารสนเทศ

6.1.8.2 ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามที่รวบรวมได้ต้องได้รับการวิเคราะห์และประเมินความเสี่ยงในเชิงรุก โดยคำนึงถึงผลกระทบที่อาจเกิดขึ้นต่อระบบสำคัญ ข้อมูลสุขภาพ และโครงสร้างพื้นฐานดิจิทัลขององค์กร

6.1.8.3 องค์กรต้องนำข้อมูลภัยคุกคามที่วิเคราะห์แล้วมาประยุกต์ใช้เพื่อเสริมสร้างมาตรการป้องกันระบบ เช่น การอัปเดตนโยบายและกฎเกณฑ์ของระบบป้องกันภัย การตั้งค่าการตรวจจับ (Detection Rules) หรือการปรับเปลี่ยนพฤติกรรมการเข้าถึงระบบที่มีความเสี่ยง

6.1.8.4 องค์กรควรจัดให้มีการแบ่งปันข้อมูลภัยคุกคามที่สำคัญภายในองค์กรในลักษณะที่เหมาะสม เพื่อเพิ่มการรับรู้และการตอบสนองของบุคลากรและหน่วยงานที่เกี่ยวข้อง รวมถึงอาจพิจารณาแลกเปลี่ยนข้อมูลกับพันธมิตรหรือเครือข่ายความร่วมมือด้านไซเบอร์ (Cybersecurity Information Sharing Networks)

6.1.8.5 ต้องมีการบันทึกและจัดเก็บข้อมูลข่าวสารภัยคุกคามที่ได้รับ รวมถึงผลการวิเคราะห์และการดำเนินการที่เกี่ยวข้อง เพื่อให้สามารถตรวจสอบย้อนหลังได้ และใช้ในการปรับปรุงแนวทางบริหารจัดการภัยคุกคามอย่างต่อเนื่อง

6.1.9 **การบริหารจัดการบุคคลภายนอก (IT Third-party Management)**

บริษัทตระหนักถึงความสำคัญของการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับบุคคลภายนอกและห่วงโซ่อุปทานด้านเทคโนโลยีสารสนเทศ ซึ่งมีบทบาทในการให้บริการสนับสนุน หรือพัฒนาโครงสร้างพื้นฐาน ระบบงาน และข้อมูลขององค์กร ไม่ว่าจะเป็นในรูปแบบของการจัดจ้างโดยตรง การว่าจ้างช่วง (Subcontracting) หรือการใช้บริการแบบดิจิทัล เช่น Cloud, SaaS, AI Platform หรือ API ที่เชื่อมต่อจากภายนอก เพื่อให้มั่นใจว่าบุคคลภายนอกและห่วงโซ่อุปทานที่เกี่ยวข้องสามารถดำเนินงานได้อย่างปลอดภัย เชื่อถือได้ และสอดคล้องกับนโยบายขององค์กร ตลอดจนข้อกำหนดของกฎหมายและมาตรฐานสากล บริษัทจึงกำหนดแนวทางการควบคุมและบริหารจัดการดังต่อไปนี้

6.1.9.1 องค์กรต้องดำเนินการประเมินความเสี่ยงของบุคคลภายนอกอย่างรอบด้านก่อนการว่าจ้างหรือการทำสัญญา โดยพิจารณาจากลักษณะการเข้าถึงข้อมูล ความสำคัญของระบบ และผลกระทบที่อาจเกิดขึ้น พร้อมทั้งกำหนดมาตรการควบคุมที่เหมาะสมตามระดับความเสี่ยงที่ประเมินได้

6.1.9.2 กำหนดให้กระบวนการจัดหาและคัดเลือกระบบเทคโนโลยีสารสนเทศต้องดำเนินการด้วยความโปร่งใส เป็นระบบ ตรวจสอบได้ และสอดคล้องกับระเบียบว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุขององค์กรอย่างเคร่งครัด

6.1.9.3 การจัดหาระบบหรือผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ ต้องเริ่มต้นจากการวิเคราะห์ความต้องการ (Requirements Analysis) และการประเมินทางเลือก (Option Evaluation) อย่าง

รอบด้าน โดยครอบคลุมมิติด้านเทคโนโลยี ความมั่นคงปลอดภัยไซเบอร์ การปฏิบัติตามข้อกฎหมายและกฎระเบียบที่เกี่ยวข้อง รวมถึงความคุ้มค่าในการลงทุน

6.1.9.4 ในกระบวนการจัดหาและคัดเลือกระบบสารสนเทศ(System Acquisition) องค์กรต้องรวมข้อกำหนดด้านความมั่นคงปลอดภัยของสารสนเทศไว้ในทุกขั้นตอนของกระบวนการจัดหาและคัดเลือกระบบสารสนเทศ ทั้งในกรณีจัดซื้อระบบสำเร็จรูปหรือจัดจ้างพัฒนาใหม่ โดยต้องพิจารณาความเสี่ยงด้านความมั่นคงตั้งแต่ต้นทาง และระบุข้อกำหนดดังกล่าวในเอกสาร TOR, RFP หรือสัญญาให้ชัดเจน รวมถึงการทดสอบระบบ การควบคุมสิทธิ์ และการตรวจสอบความปลอดภัยก่อนนำระบบมาใช้งาน

6.1.9.5 องค์กรต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยของสารสนเทศในสัญญาหรือข้อตกลงกับบุคคลภายนอกอย่างชัดเจน โดยครอบคลุมประเด็นสำคัญ เช่น การคุ้มครองข้อมูลส่วนบุคคล ความลับของข้อมูล สิทธิในการตรวจสอบ และข้อกำหนดในการจัดการเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย

6.1.9.6 ควบคุมสิทธิ์การเข้าถึงข้อมูล ระบบ และโครงสร้างพื้นฐานขององค์กรโดยบุคคลภายนอกอย่างเหมาะสม โดยจำกัดเฉพาะข้อมูลและทรัพยากรที่จำเป็น พร้อมทั้งมีการกำกับ ตรวจสอบ และทบทวนสิทธิ์การเข้าถึงอย่างต่อเนื่อง

6.1.9.7 ดำเนินการติดตาม ตรวจสอบ และประเมินผลการให้บริการของบุคคลภายนอกอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าผู้ให้บริการปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยและเงื่อนไขในสัญญาตลอดจนสามารถตอบสนองต่อเหตุการณ์ผิดปกติได้อย่างมีประสิทธิภาพ

6.1.9.8 จัดให้มีแนวทางในการบริหารจัดการเหตุการณ์ผิดปกติหรือการละเมิดข้อกำหนดด้านความมั่นคงปลอดภัยที่เกิดจากบุคคลภายนอก โดยรวมถึงขั้นตอนการแจ้งเตือน การวิเคราะห์ผลกระทบ มาตรการแก้ไข และการรายงานต่อหน่วยงานที่เกี่ยวข้อง

6.1.9.9 ดำเนินการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยตลอดห่วงโซ่อุปทาน ICT อย่างครอบคลุม โดยครอบคลุมถึงผู้ให้บริการทางตรงและทางอ้อม ผู้รับช่วง (subcontractors) และแหล่งทรัพยากรด้านเทคโนโลยี เพื่อป้องกันภัยคุกคามในลักษณะ end-to-end supply chain attack

6.1.9.10 กำกับดูแลการใช้ซอฟต์แวร์หรือบริการจากแหล่งที่ไม่สามารถตรวจสอบแหล่งที่มาได้อย่างเคร่งครัด โดยจัดให้มีการตรวจสอบความถูกต้องของแหล่งที่มา การประเมินความน่าเชื่อถือ และการควบคุมการนำมาใช้งาน เพื่อหลีกเลี่ยงความเสี่ยงจากการฝังโค้ดอันตรายหรือการโจมตีผ่านช่องทางซัพพลายเชน

6.1.9.11 จัดให้มีขั้นตอนที่เหมาะสมในการเพิกถอนสิทธิ์การเข้าถึง และการจัดการเมื่อสิ้นสุดความสัมพันธ์กับบุคคลภายนอก โดยรวมถึงการลบข้อมูล การส่งคืนหรือทำลายทรัพย์สินขององค์กร และการปิดช่องทางการเข้าถึงระบบ เพื่อป้องกันการนำข้อมูลหรือทรัพยากรไปใช้งานโดยไม่ได้รับอนุญาต

6.2 **มาตรการควบคุมด้านบุคลากร** (People Controls)

มาตรการควบคุมด้านบุคลากร หมายถึง แนวทางการบริหารจัดการบุคคลในทุกระดับขององค์กรที่มีบทบาทเกี่ยวข้องกับข้อมูล ระบบสารสนเทศ หรือโครงสร้างพื้นฐานทางเทคโนโลยีขององค์กร โดยมุ่งเน้นการส่งเสริมให้บุคลากรปฏิบัติงานอย่างมีความรับผิดชอบ มีจริยธรรม และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของสารสนเทศ

มาตรการเหล่านี้ครอบคลุมตลอดวงจรชีวิตของการจ้างงาน ตั้งแต่การคัดเลือกบุคลากร การกำหนดหน้าที่และสิทธิ์ในการเข้าถึง การฝึกอบรม การควบคุมการปฏิบัติงาน ไปจนถึงการเพิกถอนสิทธิ์และการจัดการเมื่อพ้นสภาพการจ้างงาน โดยมีวัตถุประสงค์เพื่อป้องกันความเสี่ยงจากพฤติกรรมที่ไม่เหมาะสม การละเมิดนโยบาย หรือการกระทำโดยรู้เท่าไม่ถึงการณ์ ซึ่งอาจก่อให้เกิดผลกระทบต่อความมั่นคงปลอดภัยขององค์กร แนวทางการควบคุมที่สำคัญภายใต้มาตรการด้านบุคลากรประกอบด้วยประเด็นสำคัญ ดังต่อไปนี้

6.2.1 **การคัดกรองบุคลากรและจัดการสิทธิ์เข้าถึงข้อมูล** (Personnel Screening and Access Management)

องค์กรต้องดำเนินการควบคุมด้านบุคลากรตั้งแต่กระบวนการคัดเลือก จนถึงการควบคุมสิทธิ์การเข้าถึงข้อมูลที่เหมาะสมตามหน้าที่ความรับผิดชอบ ดังนี้

6.2.1.1 องค์กรต้องกำหนดหลักเกณฑ์และกระบวนการคัดเลือกบุคลากรให้เหมาะสมกับลักษณะงานและหน้าที่ความรับผิดชอบ โดยเฉพาะตำแหน่งที่เกี่ยวข้องกับการเข้าถึงข้อมูลสำคัญหรือระบบสารสนเทศที่มีความอ่อนไหว อาจรวมถึงการตรวจสอบประวัติ (Background Check) เพื่อประเมินความน่าเชื่อถือและลดความเสี่ยงที่อาจเกิดขึ้นต่อองค์กร

6.2.1.2 บุคลากรทุกคนต้องลงนามในข้อตกลงว่าด้วยการรักษาความลับของข้อมูล (Non-Disclosure Agreement: NDA) ก่อนเริ่มปฏิบัติงาน และต้องได้รับการฝึกอบรมความรู้พื้นฐานด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับหน้าที่รับผิดชอบ

6.2.1.3 การกำหนดสิทธิ์ในการเข้าถึงระบบสารสนเทศและข้อมูลขององค์กร ต้องเป็นไปตามหลักการควบคุมตามบทบาทหน้าที่ (Role-Based Access Control: RBAC) โดยพิจารณาจากภารกิจ หน้าที่ และความรับผิดชอบของผู้ใช้งานแต่ละราย ทั้งนี้ ต้องมีการทบทวนความเหมาะสมของสิทธิ์การเข้าถึงอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบ เพื่อให้มั่นใจว่าสิทธิ์ที่กำหนดยังคงเหมาะสม สอดคล้องกับสถานะการปฏิบัติงาน และไม่ก่อให้เกิดความเสี่ยงต่อความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศขององค์กร

6.2.1.4 องค์กรต้องมีการประเมินผลการปฏิบัติงานของบุคลากรในด้านความมั่นคงปลอดภัยสารสนเทศอย่างสม่ำเสมอ พร้อมทั้งจัดให้มีช่องทางที่ปลอดภัยและเป็นความลับสำหรับการรายงานพฤติกรรมที่อาจก่อให้เกิดความเสี่ยงหรือขัดต่อหลักความมั่นคงปลอดภัยขององค์กร

6.2.1.5 เมื่อบุคลากรพ้นสภาพการเป็นพนักงาน ไม่ว่าจะด้วยเหตุผลใดก็ตาม องค์กร ต้องดำเนินการเพิกถอนสิทธิ์การเข้าถึงระบบสารสนเทศ ยกเลิกบัญชีผู้ใช้งาน (User Account) และระงับการเข้าถึงข้อมูลหรือทรัพยากรขององค์กรโดยทันที เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตและลดความเสี่ยงที่อาจเกิดขึ้นในภายหลัง

6.2.2 **การจัดการความตระหนักรู้และฝึกอบรม** (Awareness and Training)

บริษัทตระหนักถึงความสำคัญของการส่งเสริมให้บุคลากรทุกระดับมีความรู้ ความเข้าใจ และตระหนักถึงบทบาทของตนในการรักษาความมั่นคงปลอดภัยของสารสนเทศ โดยเฉพาะข้อมูลด้านสุขภาพ (PHI) และข้อมูลส่วนบุคคล (PII) ที่มีความอ่อนไหวสูง จึงกำหนดแนวทางปฏิบัติดังต่อไปนี้

6.2.2.1 องค์กรต้องจัดให้มีโปรแกรมการอบรมและสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศอย่างเป็นระบบอย่างน้อยปีละหนึ่งครั้ง สำหรับบุคลากรทุกระดับ โดยครอบคลุมประเด็น เช่น

- นโยบายและมาตรการความมั่นคงปลอดภัยขององค์กร
- การจัดการข้อมูลส่วนบุคคลและข้อมูลสุขภาพตาม PDPA
- การป้องกันภัยคุกคามทางไซเบอร์ เช่น Phishing, Ransomware
- วิธีการปฏิบัติเมื่อพบเหตุการณ์ผิดปกติ (Incident Response)
- ความปลอดภัยของระบบ AI และ Digital Health ที่นำมาใช้งาน

6.2.2.2 พนักงานใหม่ทุกคนต้องผ่านการอบรมความมั่นคงปลอดภัยสารสนเทศเบื้องต้น (Onboarding Security Awareness) ภายใน 30 วันหลังเริ่มงาน และต้องลงนามรับทราบนโยบายที่เกี่ยวข้อง

6.2.2.3 องค์กรต้องจัดให้มีสื่อการเรียนรู้ที่เข้าถึงง่าย เช่น E-learning, Video, Infographic หรือบทความภายใน พร้อมอัปเดตประเด็นภัยคุกคามใหม่ ๆ อย่างสม่ำเสมอ เพื่อให้พนักงานสามารถเรียนรู้ได้ด้วยตนเอง (Self-paced learning)

6.2.2.4 องค์กรต้องมีการติดตามและประเมินผลการฝึกอบรม โดยอาจใช้วิธีแบบ Pre-test / Post-test, แบบประเมินความพึงพอใจ หรือสถิติการเข้าร่วมอบรม เพื่อนำมาปรับปรุงหลักสูตรและแนวทางให้เหมาะสมอย่างต่อเนื่อง

6.2.2.5 ผู้บริหารระดับสูงและหัวหน้าหน่วยงานต้องเข้าร่วมฝึกอบรมด้านความมั่นคงปลอดภัยในประเด็นเฉพาะ เช่น การบริหารความเสี่ยง IT, Cyber Incident Response, ความรับผิดทางกฎหมายด้านข้อมูลส่วนบุคคล เพื่อเสริมสร้างบทบาทผู้นำด้านความมั่นคงปลอดภัยในองค์กร

6.3 **มาตรการการควบคุมทางกายภาพ** (Physical Controls)

มาตรการควบคุมทางกายภาพ หมายถึง มาตรการที่ใช้ในการปกป้องพื้นที่ อาคาร สิ่งปลูกสร้าง และสิ่งแวดล้อมที่เกี่ยวข้องกับการจัดเก็บหรือประมวลผลข้อมูลและระบบสารสนเทศขององค์กร โดยมุ่งเน้นการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การโจรกรรม การทำลาย หรือความเสียหายจากภัยคุกคามทางกายภาพและสิ่งแวดล้อม ไม่ว่าจะเป็นภัยธรรมชาติ อัคคีภัย น้ำท่วม หรือเหตุร้ายอื่นใดที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูล

มาตรการเหล่านี้มีบทบาทสำคัญในการควบคุมการเข้าถึงระบบ สถานที่ตั้งของศูนย์ข้อมูล (Data Center) และอุปกรณ์สำคัญต่าง ๆ ขององค์กร ทั้งในส่วนที่เป็นพื้นที่ควบคุมและพื้นที่สนับสนุน แนวทางการควบคุมที่สำคัญครอบคลุมประเด็น ดังต่อไปนี้

6.3.1 **การรักษาความมั่นคงปลอดภัยของพื้นที่ทางกายภาพ** (Physical Security)

บริษัทตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของสถานที่ปฏิบัติงาน โดยเฉพาะพื้นที่ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศที่มีความสำคัญต่อการดำเนินธุรกิจ การให้บริการด้านสุขภาพ และการปกป้องข้อมูลส่วนบุคคลและข้อมูลสุขภาพของผู้ใช้บริการ บริษัทจึงกำหนดแนวทางปฏิบัติในการควบคุมและบริหารจัดการความมั่นคงปลอดภัยของพื้นที่ทางกายภาพ ดังนี้

6.3.1.1 องค์กรต้องดำเนินการควบคุมการเข้าถึงพื้นที่สำคัญ เช่น ศูนย์ข้อมูล (Data Center) ห้องควบคุมระบบ (Server Room) และพื้นที่จัดเก็บอุปกรณ์สารสนเทศ โดยใช้ระบบควบคุมการเข้าถึงที่เหมาะสม เช่น บัตรผ่านประตู ระบบสแกนลายนิ้วมือ หรือระบบจดจำใบหน้า เพื่อจำกัดการเข้าถึงเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

6.3.1.2 พื้นที่ที่มีการติดตั้งระบบเทคโนโลยีสารสนเทศสำคัญ ต้องมีมาตรการด้านความปลอดภัยทางกายภาพที่เพียงพอ เช่น การติดตั้งกล้องวงจรปิด (CCTV) ระบบตรวจจับการเคลื่อนไหว (Motion Detection) ระบบสัญญาณเตือนภัย (Alarm System) และระบบดับเพลิงอัตโนมัติ (Fire Suppression System) เพื่อเฝ้าระวังและป้องกันเหตุการณ์ผิดปกติ

6.3.1.3 องค์กรต้องแบ่งระดับพื้นที่ตามระดับความเสี่ยง เช่น พื้นที่สาธารณะ (Public Zone) พื้นที่ควบคุม (Controlled Zone) และพื้นที่จำกัดพิเศษ (Restricted Zone) โดยกำหนดสิทธิ์การเข้าถึงที่แตกต่างกันตามบทบาทหน้าที่และความจำเป็นในการปฏิบัติงาน

6.3.1.4 บุคลากรขององค์กร รวมถึงผู้ให้บริการภายนอกที่มีความจำเป็นต้องเข้าถึงพื้นที่ที่มีความสำคัญ ต้องได้รับการอนุญาตอย่างเป็นทางการจากผู้มีอำนาจ และต้องลงทะเบียนในระบบหรือปฏิบัติตามขั้นตอนที่องค์กรกำหนดไว้ โดยในระหว่างที่อยู่ในพื้นที่ บุคคลดังกล่าวต้องอยู่ภายใต้การควบคุม กำกับดูแล และติดตามโดยเจ้าหน้าที่หรือผู้มีอำนาจที่ได้รับมอบหมายอย่างเคร่งครัด

6.3.1.5 บุคลากรขององค์กร และผู้ให้บริการภายนอกที่มีความจำเป็นต้องเข้าถึงพื้นที่ที่มีความสำคัญ ต้องได้รับการอนุญาตอย่างเป็นทางการ ลงทะเบียนไว้ในระบบ และอยู่ภายใต้การควบคุมดูแลของผู้มีอำนาจที่ได้รับมอบหมายตลอดระยะเวลาที่อยู่ในพื้นที่ดังกล่าว

6.3.1.6 องค์กรต้องมีระบบบันทึกการเข้า–ออกพื้นที่สำคัญโดยอัตโนมัติ (Access Logs) เพื่อสนับสนุนการตรวจสอบย้อนหลัง และต้องมีการจัดเก็บข้อมูลดังกล่าวอย่างน้อย 90 วัน หรือตามข้อกำหนดของหน่วยงานกำกับดูแลที่เกี่ยวข้อง

6.3.1.7 ดำเนินการตรวจสอบและประเมินความเพียงพอของมาตรการรักษาความมั่นคงปลอดภัยของพื้นที่ทางกายภาพอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีเหตุการณ์ผิดปกติที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของสถานที่และระบบที่เกี่ยวข้อง

6.3.1.8 องค์กรต้องมีแผนป้องกันและรับมือเหตุฉุกเฉินที่ครอบคลุมสถานการณ์ด้านกายภาพ เช่น ไฟไหม้ น้ำท่วม การบุกรุกหรือก่อวินาศกรรม และจัดให้มีการฝึกซ้อมตามแผนอย่างน้อยปีละหนึ่งครั้ง เพื่อสร้างความพร้อมในการตอบสนองต่อเหตุการณ์ต่าง ๆ อย่างมีประสิทธิภาพ

6.3.2 **การจัดการอุปกรณ์และสิ่งแวดล้อมที่เกี่ยวข้องกับระบบสารสนเทศ** (Equipment and Environment Security)

บริษัทตระหนักถึงความสำคัญของการบริหารจัดการอุปกรณ์เทคโนโลยีสารสนเทศ และการควบคุมสภาพแวดล้อมที่เกี่ยวข้อง เพื่อให้มั่นใจได้ว่าทรัพยากรด้านเทคโนโลยีที่ใช้ในการให้บริการด้านสุขภาพมีความปลอดภัย มีประสิทธิภาพ และสามารถรองรับการดำเนินงานขององค์กรได้อย่างต่อเนื่อง บริษัทจึงกำหนดแนวทางปฏิบัติในการจัดการอุปกรณ์และสิ่งแวดล้อมระบบสารสนเทศ ดังนี้

6.3.2.1 องค์กรต้องควบคุมการติดตั้ง การจัดวาง และการใช้งานอุปกรณ์เทคโนโลยีสารสนเทศในพื้นที่ที่เหมาะสม เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต และลดความเสี่ยงจากการรบกวนทางกายภาพ เช่น ความร้อน ความชื้น ฝุ่น หรือแรงดันไฟฟ้าที่ไม่เสถียร

6.3.2.2 พื้นที่ที่ติดตั้งอุปกรณ์สารสนเทศสำคัญ เช่น ห้องศูนย์ข้อมูล ห้องควบคุมระบบ หรือห้องเก็บข้อมูลสำรอง ควรมีการควบคุมสภาพแวดล้อมอย่างเหมาะสม เช่น ระบบปรับอากาศเฉพาะ ระบบควบคุมความชื้น ระบบไฟฟ้าสำรอง (UPS/Generator) ระบบป้องกันไฟฟ้ากระชาก และระบบตรวจจับอัคคีภัย

6.3.2.3 อุปกรณ์ที่เลิกใช้งานหรือเสื่อมสภาพต้องได้รับการจัดการอย่างปลอดภัย โดยต้องลบข้อมูลออกจากสื่อบันทึกตามแนวทางที่ปลอดภัย เช่น การล้างข้อมูล (Data Wiping) การเขียนทับหลายรอบ (Overwriting) หรือการทำลายทางกายภาพ (Physical Destruction) ตามมาตรฐาน NIST SP 800-88 หรือเทียบเท่า

6.3.2.4 ควบคุมการเคลื่อนย้ายอุปกรณ์เทคโนโลยีสารสนเทศ โดยกำหนดให้มีการขออนุมัติล่วงหน้า พร้อมจัดทำแบบฟอร์มบันทึกรายละเอียดการเคลื่อนย้าย และดำเนินการตรวจสอบความถูกต้องหลังจากการเคลื่อนย้ายเสร็จสิ้น

6.3.2.5 สำหรับอุปกรณ์เคลื่อนที่ เช่น Notebook, Tablet, Mobile Device หรือ External Storage ต้องมีการควบคุมโดยใช้มาตรการป้องกัน เช่น การเข้ารหัส (Encryption) การยืนยันตัวตน (Authentication) และการตั้งค่าระบบติดตาม (Device Tracking)

6.3.2.6 กำหนดมาตรการควบคุมการเชื่อมต่ออุปกรณ์ต่อพ่วงจากภายนอก เช่น USB Flash Drive หรือ External Hard Disk โดยใช้ระบบ Device Control หรือ Endpoint Protection เพื่อลดความเสี่ยงจากมัลแวร์และการรั่วไหลของข้อมูล

6.3.2.7 ดำเนินการตรวจสอบและทวนสอบทรัพย์สินเทคโนโลยีสารสนเทศอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงระบบ เพื่อให้มั่นใจว่าทรัพย์สินทั้งหมดอยู่ในสถานะที่ถูกต้อง ครบถ้วน และสามารถตรวจสอบย้อนหลังได้

6.4 **มาตรการควบคุมด้านเทคโนโลยี** (Technological Controls)

มาตรการควบคุมด้านเทคโนโลยี หมายถึง มาตรการควบคุมด้านเทคนิคที่องค์กรนำมาใช้โดยอาศัยเครื่องมือ เทคโนโลยี ระบบ และกระบวนการอัตโนมัติเพื่อสนับสนุนการป้องกัน ตรวจจับ ตอบสนอง และฟื้นฟูจากภัยคุกคามที่อาจส่งผลกระทบต่อระบบสารสนเทศและข้อมูลสำคัญขององค์กร

มาตรการเหล่านี้มุ่งเน้นการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูลตามหลักการของความมั่นคงปลอดภัยสารสนเทศ (CIA Triad) โดยนำเทคโนโลยีและกลไกการควบคุมมาประยุกต์ใช้ให้เหมาะสมกับความเสี่ยง ลักษณะการใช้งาน และบริบทขององค์กร แนวทางการควบคุมที่สำคัญภายใต้มาตรการด้านเทคโนโลยี ประกอบด้วยประเด็นสำคัญ ดังต่อไปนี้

6.4.1 **การควบคุมการเข้ารหัสและปกป้องข้อมูล** (Encryption and Data Protection)

บริษัทตระหนักถึงความสำคัญของการปกป้องข้อมูลที่มีความอ่อนไหวและข้อมูลส่วนบุคคล โดยเฉพาะข้อมูลสุขภาพของผู้ป่วย (PHI) ซึ่งถือเป็นข้อมูลสำคัญที่อยู่ภายใต้ข้อกำหนดของกฎหมายและข้อบังคับต่าง ๆ เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) และ ISO/IEC 27001:2022 บริษัทจึงกำหนดแนวทางปฏิบัติดังต่อไปนี้:

6.4.1.1 องค์กรต้องดำเนินการจำแนกประเภทของข้อมูลที่จำเป็นต้องเข้ารหัส และกำหนดวิธีการเข้ารหัสที่สอดคล้องกับระดับความสำคัญและระดับความอ่อนไหวของข้อมูลแต่ละประเภท โดยคำนึงถึงความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากการเข้าถึงหรือรั่วไหลของข้อมูลโดยไม่ได้รับอนุญาต

6.4.1.2 การเข้ารหัสข้อมูล (Encryption) และการสร้างค่าแฮช (Hashing) ต้องดำเนินการโดยใช้อัลกอริธึมที่เป็นไปตามมาตรฐานสากลที่ได้รับการยอมรับในระดับวิชาชีพ เช่น AES, RSA, ECC และ SHA-2 โดยอัลกอริธึมและเครื่องมือที่เลือกใช้ต้องผ่านการรับรองจากหน่วยงานที่เชื่อถือได้ในระดับสากล เช่น Federal Information Processing Standard (FIPS) 140-3 หรือมาตรฐานที่เทียบเท่า เพื่อให้มั่นใจว่าการปกป้องข้อมูลมีความปลอดภัยและเชื่อถือได้

6.4.1.3 สำหรับการเข้ารหัสข้อมูล องค์กรต้องเลือกใช้อัลกอริธึมที่เหมาะสมกับระดับความสำคัญของข้อมูล โดยกำหนดความยาวของรหัส (Key Length) ให้เพียงพอต่อการป้องกันภัยคุกคาม เพื่อให้แน่ใจว่าข้อมูลจะได้รับการปกป้องอย่างเหมาะสมและมีประสิทธิภาพ

6.4.1.4 ในบางกรณี เช่น การจัดเก็บรหัสผ่าน หรือการตรวจสอบความถูกต้องของข้อมูล องค์กรควรใช้เทคนิคการแฮช (Hashing) ซึ่งเป็นกระบวนการแปลงข้อมูลให้เป็นค่าที่ไม่สามารถย้อนกลับไปยังข้อมูลต้นฉบับได้ โดยต้องใช้อัลกอริธึมที่มีความปลอดภัยและได้รับการยอมรับในระดับสากล เช่น SHA-2 หรือ SHA-3 เพื่อป้องกันการเข้าถึงหรือดัดแปลงข้อมูลโดยไม่ได้รับอนุญาต ทั้งนี้ องค์กรต้องหลีกเลี่ยงการใช้อัลกอริธึมที่ล้าสมัยหรือมีช่องโหว่ เช่น MD5 และ SHA-1

6.4.1.5 องค์กรต้องดำเนินการจัดการวงจรชีวิตของคีย์เข้ารหัส (Cryptographic Key Lifecycle Management) อย่างเป็นระบบและปลอดภัย ครอบคลุมทุกขั้นตอน ได้แก่ การสร้าง การแจกจ่าย การจัดเก็บ การใช้งาน การเปลี่ยนแปลง และการทำลาย โดยพิจารณาใช้ Hardware Security Module (HSM) หรือระบบที่มีความปลอดภัยระดับสูง

6.4.1.6 การเข้ารหัสข้อมูลต้องครอบคลุมข้อมูลในทุกสถานะ ไม่ว่าจะเป็นข้อมูลที่จัดเก็บ (Data at Rest) ข้อมูลที่ส่งผ่านเครือข่าย (Data in Transit) และข้อมูลที่อยู่ระหว่างการประมวลผล (Data in Use) โดยรวมถึงข้อมูลที่อยู่บนอุปกรณ์พกพา ฐานข้อมูล ระบบคลาวด์ (Cloud) และอุปกรณ์ที่เชื่อมต่อกับเครือข่ายขององค์กร

6.4.1.7 องค์กรต้องควบคุมการถ่ายโอนข้อมูลที่มีความอ่อนไหวผ่านอุปกรณ์บันทึกข้อมูลแบบพกพา (Portable Media) เช่น USB Drive, External Hard Disk โดยต้องมีมาตรการเข้ารหัสไฟล์หรือดิสก์ และจำกัดการใช้งานเฉพาะอุปกรณ์ที่ได้รับอนุญาตตามนโยบายขององค์กร

6.4.1.8 องค์กรต้องจัดให้มีมาตรการในการปกป้องข้อมูลบนอุปกรณ์เคลื่อนที่และอุปกรณ์ส่วนตัวที่นำมาใช้ในการทำงาน (BYOD) โดยใช้นโยบาย Mobile Device Management (MDM) ที่สามารถควบคุมการเข้าถึงข้อมูล บังคับใช้การเข้ารหัส และลบข้อมูลจากระยะไกลได้ในกรณีสูญหายหรือถูกโจรกรรม

6.4.1.9 องค์กรต้องกำหนดให้มีการทบทวนประสิทธิภาพของกระบวนการเข้ารหัสข้อมูลและมาตรการป้องกันข้อมูลอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงระบบสารสนเทศที่เกี่ยวข้อง เพื่อให้แน่ใจว่ายังคงมีความเพียงพอและสอดคล้องกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร

6.4.2 **การรักษาความปลอดภัยระบบเครือข่ายและการสื่อสารข้อมูล** (Network and Communication Security)

บริษัทตระหนักถึงความสำคัญของระบบเครือข่ายและการสื่อสารข้อมูลที่มั่นคงปลอดภัยในการสนับสนุนการดำเนินงาน การให้บริการสุขภาพ และการรักษาความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานของข้อมูล โดยเฉพาะข้อมูลส่วนบุคคลและข้อมูลสุขภาพที่มีความอ่อนไหว บริษัทจึงกำหนดแนวทางการควบคุมความมั่นคงปลอดภัยของระบบเครือข่ายและการสื่อสารข้อมูล ดังนี้:

6.4.2.1 องค์กรต้องจัดให้มีมาตรการควบคุมการเข้าถึงระบบเครือข่ายสื่อสาร ทั้งภายในและภายนอกองค์กร โดยใช้อุปกรณ์และกลไกควบคุมที่เหมาะสม เช่น ระบบไฟร์วอลล์ (Firewall) การแบ่งส่วนเครือข่าย (Network Segmentation) และรายการควบคุมการเข้าถึง (Access Control Lists: ACLs) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

6.4.2.2 ต้องมีการกำหนดนโยบายและการควบคุมการใช้งานเครือข่ายไร้สาย (Wireless Network Security) เช่น การใช้รหัสผ่านที่เข้มแข็ง การใช้มาตรฐานการเข้ารหัส (WPA3 หรือเทียบเท่า) และการแยกเครือข่ายสำหรับผู้มาเยือน (Guest Wi-Fi)

6.4.2.3 การเชื่อมต่อกับระบบเครือข่ายภายนอก หรือการเข้าถึงระบบโดยบุคคลภายนอก เช่น ผู้ให้บริการหรือคู่สัญญา ต้องได้รับการอนุมัติล่วงหน้าจากหน่วยงานที่รับผิดชอบ และต้องปฏิบัติตามข้อกำหนดและมาตรการด้านความมั่นคงปลอดภัยขององค์กร อย่างเคร่งครัด

6.4.2.4 การส่งข้อมูลที่มีความสำคัญ เช่น ข้อมูลสุขภาพ ข้อมูลส่วนบุคคล หรือข้อมูลทางการแพทย์ ต้องมีการเข้ารหัสข้อมูล (Encryption) ทั้งในขณะส่งผ่านเครือข่าย (Data in Transit) และขณะจัดเก็บ (Data at Rest) โดยใช้มาตรฐานการเข้ารหัสที่ปลอดภัย เช่น TLS, AES-256

6.4.2.5 ดำเนินการจัดเก็บ บันทึก และตรวจสอบข้อมูลจราจรทางเครือข่าย (Network Logs)เพื่อสนับสนุนการวิเคราะห์เหตุการณ์ด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

6.4.2.6 องค์กรควรดำเนินการตรวจสอบการใช้งานเครือข่ายอย่างต่อเนื่อง เช่น ใช้ระบบตรวจจับและป้องกันการบุกรุก (Intrusion Detection and Prevention Systems: IDS/IPS) ตลอดจนระบบวิเคราะห์

พฤติกรรมการใช้งานเครือข่าย (Network Behavior Analysis) เพื่อให้สามารถตรวจพบและตอบสนองต่อเหตุการณ์ผิดปกติได้อย่างทันท่วงที

6.4.2.7 ต้องมีมาตรการควบคุมการเข้าถึงระยะไกล (Remote Access Control) เช่น VPN ที่ใช้การยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication – MFA) การจำกัดสิทธิ์ตามบทบาท และการตรวจสอบอุปกรณ์ปลายทางก่อนอนุญาตการเชื่อมต่อ

6.4.2.8 การใช้งานโปรโตคอลที่ไม่ปลอดภัย (Insecure Protocols) ต้องถูกจำกัด หรือยกเลิกใช้งาน และแทนที่ด้วยโปรโตคอลที่เข้ารหัส เช่น SFTP, SSH, HTTPS

6.4.2.9 องค์กรต้องดำเนินการทดสอบความมั่นคงปลอดภัยของระบบเครือข่าย (Network Penetration Testing) และการตรวจสอบช่องโหว่ (Vulnerability Assessment) อย่างน้อยปีละหนึ่งครั้ง และเมื่อมีการเปลี่ยนแปลงโครงสร้างเครือข่ายที่สำคัญ

6.4.2.10 ต้องมีแผนตอบสนองเหตุการณ์ด้านความปลอดภัยไซเบอร์ที่เกี่ยวข้องกับระบบเครือข่าย เช่น การโจมตี DDoS การบุกรุกระบบ (Intrusion) หรือการสูญหายของข้อมูลผ่านช่องทางเครือข่าย โดยรวมถึงขั้นตอนแจ้งเตือนและรายงานต่อผู้เกี่ยวข้อง

6.4.2.11 องค์กรต้องดำเนินการทบทวน และประเมินความมั่นคงปลอดภัยของระบบเครือข่ายอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญทางด้านเทคโนโลยี โครงสร้างพื้นฐาน หรือการกำหนดนโยบาย เพื่อให้สามารถรักษาความมั่นคงปลอดภัยของระบบเครือข่ายได้อย่างต่อเนื่องและสอดคล้องกับสถานการณ์ปัจจุบัน

6.4.3 **การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ** (IT Operations Security)

บริษัทตระหนักถึงความสำคัญของการควบคุมและกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศให้เป็นไปอย่างมั่นคงปลอดภัย มีความต่อเนื่อง และสามารถตรวจสอบได้ เพื่อป้องกันความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินงานที่ผิดพลาดหรือถูกแทรกแซงโดยมิชอบ โดยกำหนดแนวทางการดำเนินงานที่สำคัญ ดังนี้

6.4.3.1 องค์กรต้องดำเนินการบริหารจัดการการตั้งค่าระบบเทคโนโลยีสารสนเทศ (Configuration) อย่างเป็นระบบและมีแบบแผนที่ชัดเจน เพื่อให้มั่นใจว่าการตั้งค่าดังกล่าวมีความมั่นคงปลอดภัย สอดคล้องกับนโยบายและมาตรฐานขององค์กร และสามารถตรวจสอบย้อนหลังได้อย่างโปร่งใส โดยต้องจัดทำทะเบียนการตั้งค่าพื้นฐานของระบบ (Configuration Baseline) กำหนดสิทธิในการเปลี่ยนแปลง บันทึกและตรวจสอบการเปลี่ยนแปลงอย่างต่อเนื่อง รวมถึงป้องกันการเปลี่ยนแปลงโดยไม่ได้รับอนุญาต เพื่อรักษาความมั่นคงปลอดภัย ความถูกต้องของการตั้งค่า และความพร้อมใช้งานของระบบสารสนเทศขององค์กรในทุกสถานการณ์

6.4.3.2 องค์กรต้องจัดให้มีกระบวนการควบคุมการเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศ (Change Management) อย่างเป็นระบบ โดยต้องผ่านการอนุมัติที่เหมาะสม ครอบคลุมการวิเคราะห์ผลกระทบ การทดสอบก่อนใช้งานจริง การบันทึกการเปลี่ยนแปลง และการแก้ไขเมื่อเกิดปัญหา ทั้งนี้เพื่อให้การเปลี่ยนแปลงเป็นไปอย่างปลอดภัย ตรวจสอบได้ และไม่กระทบต่อความมั่นคงปลอดภัยและความต่อเนื่องทางธุรกิ

6.4.3.3 องค์กรต้องจัดให้มีแนวทางการบริหารจัดการขีดความสามารถของระบบเทคโนโลยีสารสนเทศ (Capacity Management) อย่างเป็นระบบ เพื่อให้สามารถรองรับการใช้งานได้อย่างมีประสิทธิภาพและต่อเนื่อง โดยต้องดำเนินการวิเคราะห์แนวโน้ม ตรวจสอบประสิทธิภาพระบบอย่างสม่ำเสมอ และวางแผนการเพิ่มขยายทรัพยากรล่วงหน้า เพื่อป้องกันความเสี่ยงจากความล้มเหลวหรือการหยุดชะงักของระบบที่อาจกระทบต่อการดำเนินธุรกิจ

6.4.3.4 องค์กรต้องกำหนดมาตรการในการปกป้องเครื่องแม่ข่าย (Servers) และอุปกรณ์ปลายทาง (Endpoints) ให้มีความมั่นคงปลอดภัย โดยดำเนินการติดตั้งระบบปฏิบัติการและซอฟต์แวร์ที่ได้รับอนุมัติ ปรับแต่งค่าความปลอดภัย (Hardening) ใช้โปรแกรมป้องกันมัลแวร์ และควบคุมสิทธิ์การเข้าถึง เพื่อป้องกันการโจมตีหรือการใช้งานโดยไม่ได้รับอนุญาต

6.4.3.5 องค์กรต้องกำหนดมาตรการควบคุมด้านความมั่นคงปลอดภัยสำหรับการใช้งานระบบจากระยะไกล อุปกรณ์เคลื่อนที่ และอุปกรณ์ส่วนบุคคล (BYOD) อย่างชัดเจน โดยครอบคลุมการพิสูจน์ตัวตน การเข้ารหัสข้อมูล การควบคุมสิทธิ์การเข้าถึง และการจัดการความเสี่ยงจากอุปกรณ์หรือเครือข่ายที่อยู่นอกเหนือการควบคุมขององค์กร เพื่อป้องกันการรั่วไหลของข้อมูลและการเข้าถึงระบบโดยไม่ได้รับอนุญาต

6.4.3.6 องค์กรต้องดำเนินการสำรองข้อมูล (Information Backup) ที่สำคัญอย่างเป็นระบบ ครอบคลุมข้อมูลผู้ใช้งาน ข้อมูลระบบ และข้อมูลการกำหนดค่าที่สำคัญ โดยต้องกำหนดความถี่ในการสำรองข้อมูล กำหนดสถานที่จัดเก็บที่ปลอดภัย และดำเนินการทดสอบการกู้คืนข้อมูลเป็นระยะ เพื่อให้สามารถรองรับเหตุการณ์ฉุกเฉินและฟื้นฟูระบบได้อย่างมีประสิทธิภาพ

6.4.3.7 องค์กรต้องจัดให้มีการบันทึกและจัดเก็บเหตุการณ์การใช้งานระบบเทคโนโลยีสารสนเทศ (Logging) อย่างเหมาะสม โดยครอบคลุมเหตุการณ์สำคัญที่จำเป็นต่อการติดตาม ตรวจสอบ และวิเคราะห์ย้อนหลัง พร้อมกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล Log เพื่อให้สามารถตรวจสอบความถูกต้องและป้องกันการแก้ไขโดยไม่ได้รับอนุญาต

6.4.3.8 จัดให้มีระบบและ/หรือกระบวนการในการติดตาม ตรวจสอบ และวิเคราะห์พฤติกรรมของระบบเทคโนโลยีสารสนเทศอย่างต่อเนื่อง เพื่อให้สามารถระบุภัยคุกคามหรือเหตุผิดปกติที่อาจกระทบต่อความมั่นคงปลอดภัยของระบบ พร้อมทั้งกำหนดมาตรการตอบสนองเบื้องต้นเพื่อจำกัดความเสียหายและลดผลกระทบที่อาจเกิดขึ้น

6.4.3.9 องค์กรต้องดำเนินการประเมินช่องโหว่ทางเทคนิค (Vulnerability Assessment) ของระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ โดยใช้เครื่องมือและวิธีการที่เหมาะสม เพื่อตรวจสอบจุดอ่อนที่อาจถูกโจมตี จัดลำดับความเสี่ยงตามระดับความรุนแรง และดำเนินการแก้ไขหรือบรรเทาผลกระทบอย่างเป็นระบบและตรวจสอบได้

6.4.3.10 องค์กรต้องดำเนินการทดสอบการเจาะระบบ (Penetration Testing) อย่างสม่ำเสมอสำหรับระบบที่มีความเสี่ยงสูง โดยให้ดำเนินการโดยผู้เชี่ยวชาญภายใต้การอนุมัติที่เหมาะสม พร้อมจัดทำรายงาน

ผล วิเคราะห์ช่องโหว่ ดำเนินการแก้ไข และจัดเก็บหลักฐานเพื่อการตรวจสอบ รวมถึงทบทวนแผนการทดสอบให้สอดคล้องกับสถานการณ์ภัยคุกคามที่เปลี่ยนแปลง

6.4.3.11 องค์กรต้องดำเนินการตรวจสอบ ประเมิน และติดตั้งโปรแกรมแก้ไขช่องโหว่ (Patch Management) ที่จำเป็นต่อระบบอย่างเป็นระบบและทันเวลา โดยต้องมีการทดสอบก่อนใช้งานจริง จัดทำบันทึกการดำเนินการอย่างครบถ้วน เพื่อให้สามารถตรวจสอบย้อนหลังได้ และลดความเสี่ยงจากการโจมตีที่อาจเกิดขึ้นจากช่องโหว่ดังกล่าว

6.4.3.12 กำหนดมาตรการควบคุมการเข้าถึงเว็บไซต์ (Web Filtering) เพื่อป้องกันการเข้าถึงเว็บไซต์ที่ไม่เหมาะสม มีความเสี่ยง หรืออาจเป็นแหล่งแพร่กระจายมัลแวร์ ฟิชชิ่ง และภัยคุกคามอื่น ๆ โดยต้องใช้ระบบกรองเว็บไซต์หรือ Secure Web Gateway ที่สามารถจัดกลุ่มเว็บไซต์ตามหมวดหมู่และกำหนดระดับการเข้าถึงได้อย่างชัดเจน พร้อมทั้งดำเนินการบันทึก ติดตาม และวิเคราะห์การใช้งานอินเทอร์เน็ตของผู้ใช้งานในระบบเครือข่ายขององค์กรอย่างเหมาะสม เพื่อให้สามารถตรวจสอบเหตุผิดปกติ ป้องกันการรั่วไหลของข้อมูล และควบคุมการใช้ทรัพยากรสารสนเทศขององค์กรให้เป็นไปตามวัตถุประสงค์และนโยบายที่กำหนด

6.4.4 การพัฒนาและบำรุงรักษาระบบสารสนเทศและ AI อย่างมั่นคงปลอดภัย (Secure Development and Maintenance)

บริษัทตระหนักถึงความสำคัญของการออกแบบ พัฒนา และบำรุงรักษาระบบสารสนเทศ รวมถึงระบบที่ใช้เทคโนโลยี AI ให้เป็นไปอย่างมั่นคงปลอดภัยตั้งแต่ระยะเริ่มต้น โดยครอบคลุมทุกขั้นตอนในวงจรชีวิตระบบ (System Development Life Cycle – SDLC) และต้องคำนึงถึงความปลอดภัยของข้อมูลสุขภาพ (PHI) และข้อมูลส่วนบุคคล (PII) อย่างเคร่งครัด จึงกำหนดแนวทางปฏิบัติดังต่อไปนี้

6.4.4.1 องค์กรต้องกำหนดให้มีการพัฒนาและบำรุงรักษาระบบเทคโนโลยีสารสนเทศตามกระบวนการที่เป็นระบบและสอดคล้องกับแนวทางมาตรฐานสากล เช่น วงจรการพัฒนาระบบ (Software Development Life Cycle: SDLC) หรือแนวทาง DevSecOps ซึ่งผนวกการรักษาความมั่นคงปลอดภัยเข้าไว้ในทุกขั้นตอนของกระบวนการพัฒนา

6.4.4.2 การออกแบบและพัฒนาระบบต้องดำเนินการโดยยึดหลัก “Security by Design” สำหรับทุกโครงการพัฒนาและบำรุงรักษาระบบสารสนเทศ โดยกำหนดขั้นตอนด้านความมั่นคงปลอดภัยในแต่ละระยะของการพัฒนา ได้แก่ การวางแผน การออกแบบ การพัฒนา การทดสอบ การติดตั้งใช้งาน และการบำรุงรักษา

6.4.4.3 ในการออกแบบระบบหรือแอปพลิเคชัน ต้องใช้แนวทาง “Security by Design” และ “Privacy by Design” โดยรวมถึงการควบคุมการเข้าถึง การเข้ารหัส การบันทึกและตรวจสอบการใช้งานระบบ และการจัดการข้อมูลส่วนบุคคลอย่างปลอดภัยตามข้อกำหนดของ PDPA

6.4.4.4 ต้องใช้หลักการพัฒนาแบบปลอดภัย (Secure Coding Practices) ตามแนวทางของ OWASP โดยทีมพัฒนาต้องได้รับการฝึกอบรมที่เหมาะสม

6.4.4.5 ระบบที่พัฒนาและนำมาใช้งานต้องผ่านกระบวนการตรวจสอบช่องโหว่ (Vulnerability Assessment) และการทดสอบการเจาะระบบ (Penetration Testing) อย่างสม่ำเสมอ โดยเฉพาะก่อนการปรับปรุงหรืออัปเดตที่มีผลกระทบต่อระบบสำคัญขององค์กร

6.4.4.6 สำหรับระบบที่มีการใช้ AI หรือ Machine Learning องค์กร ต้องดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยและจริยธรรมของ AI (AI Risk and Ethical Assessment) เช่น ความลำเอียงของข้อมูล (Bias) การตีความผลลัพธ์ (Explainability) และความโปร่งใสในการใช้งาน AI

6.4.4.7 องค์กรต้องจัดเก็บซอร์สโค้ดในระบบควบคุมเวอร์ชันที่มีความมั่นคงปลอดภัย เช่น GitLab หรือ GitHub Enterprise และต้องกำหนดสิทธิ์การเข้าถึงอย่างเหมาะสม รวมถึงมีการบันทึกกิจกรรมของผู้พัฒนา

6.4.4.8 ต้องดำเนินการตรวจสอบโค้ดและผลกระทบด้านความมั่นคงปลอดภัยทุกครั้งก่อนปล่อย (Release) เวอร์ชันใหม่ของระบบ และมีขั้นตอนอนุมัติจากเจ้าของระบบและฝ่ายที่เกี่ยวข้อง (Change Control and Security Approval)

6.4.4.9 ต้องมีการจัดทำเอกสารระบบให้ครบถ้วนและถูกต้อง เช่น เอกสารกระบวนการทางธุรกิจ (Business Process) โครงสร้างทางเทคนิค (Technical Architecture) ชุดคำสั่งโปรแกรม (Source Code) และคู่มือผู้ใช้งาน (User Manual) เพื่อให้สามารถดูแลและตรวจสอบระบบได้อย่างมีประสิทธิภาพ

6.4.4.10 องค์กรต้องกำหนดแผนงานที่ชัดเจนในการบำรุงรักษา ทดแทนระบบ และการยุติการใช้งานระบบที่หมดอายุการใช้งานอย่างปลอดภัย โดยให้คำนึงถึงความต่อเนื่องทางธุรกิจ ความมั่นคงปลอดภัยของข้อมูล และข้อกำหนดตามกฎหมายหรือกฎระเบียบที่เกี่ยวข้อง

6.4.5 **การจัดการรหัสผ่านและการยืนยันตัวตน** (Authentication and Identity Management)

บริษัทตระหนักถึงความสำคัญของการพิสูจน์ตัวตนและการบริหารจัดการสิทธิ์ในการเข้าถึงระบบสารสนเทศ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต และลดความเสี่ยงจากการละเมิดข้อมูลหรือระบบที่สำคัญ โดยกำหนดแนวทางปฏิบัติดังต่อไปนี้

6.4.5.1 องค์กรต้องกำหนดให้ระบบที่มีการเข้าถึงโดยผู้ใช้ต้องมีการพิสูจน์ตัวตนอย่างเหมาะสมตามระดับความเสี่ยงของระบบ โดยให้ความสำคัญกับการใช้ การยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) สำหรับระบบที่เกี่ยวข้องกับข้อมูลสำคัญ หรือระบบที่เข้าถึงจากภายนอกเครือข่ายองค์กร

6.4.5.2 องค์กรต้องกำหนดนโยบายและข้อกำหนดด้าน รหัสผ่าน (Password Policy) ที่เหมาะสม เช่น ความยาวขั้นต่ำ การใช้ตัวอักษรพิเศษ การเปลี่ยนรหัสผ่านอย่างสม่ำเสมอ และไม่อนุญาตให้ใช้รหัสผ่านที่เคยใช้ซ้ำ โดยต้องใช้มาตรการเชิงเทคนิคเพื่อบังคับใช้ (Enforcement) ตามนโยบายดังกล่าว

6.4.5.3 ผู้ใช้งานต้องเก็บรักษารหัสผ่านและข้อมูลยืนยันตัวตนอื่น ๆ ไว้อย่างปลอดภัย ห้ามเปิดเผยรหัสผ่านแก่บุคคลอื่น และห้ามใช้รหัสผ่านเดียวกันกับระบบอื่นที่ไม่เกี่ยวข้องกับงานในองค์กร โดยองค์กรอาจมีการอบรมหรือให้คำแนะนำเกี่ยวกับการตั้งรหัสผ่านที่ปลอดภัยอย่างสม่ำเสมอ

6.4.5.4 องค์กรควรจัดให้มีเครื่องมือหรือกระบวนการในการควบคุม ตรวจสอบ และจัดการสิทธิ์ของผู้ใช้งานในระบบต่าง ๆ ให้สอดคล้องกับบทบาทหน้าที่ (Role-Based Access Control – RBAC) และหลักการสิทธิ์ขั้นต่ำที่จำเป็น (Least Privilege)

6.4.5.5 ทุกระบบต้องมีการบันทึก Log การเข้าสู่ระบบ (Login Audit Trail) และกิจกรรมที่เกี่ยวข้องกับการพิสูจน์ตัวตนอย่างครบถ้วน และต้องสามารถตรวจสอบย้อนหลังได้ตามข้อกำหนดของนโยบายด้านความมั่นคงปลอดภัยและหน่วยงานกำกับดูแล

6.4.5.6 บัญชีผู้ใช้งานที่ไม่มีการใช้งานเกินระยะเวลาที่กำหนด หรือไม่ได้ใช้งานตามบทบาทหน้าที่ ต้องถูกระงับหรือยกเลิกอย่างเหมาะสม เพื่อป้องกันความเสี่ยงจากบัญชีที่ไม่มีผู้ใช้งานรับผิดชอบ (Dormant Accounts)

7. **การวัด ติดตาม วิเคราะห์และประเมินผล** (Performance Monitoring and Evaluation)

บริษัทตระหนักถึงความสำคัญของกระบวนการวัดผล ติดตาม วิเคราะห์ และประเมินประสิทธิภาพในการบริหารจัดการด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศอย่างเป็นระบบและต่อเนื่อง เพื่อให้สามารถประเมินความสอดคล้องกับนโยบาย มาตรฐาน และแนวทางที่องค์กรกำหนด ตลอดจนสามารถระบุจุดอ่อนหรือช่องว่างในการดำเนินงาน และนำไปสู่การปรับปรุงมาตรการควบคุมและการบริหารจัดการด้านความมั่นคงปลอดภัยได้อย่างมีประสิทธิภาพ โดยมีแนวทางในการดำเนินการ ดังนี้

7.1 กำหนดตัวชี้วัดที่เหมาะสม (Key Performance Indicators: KPIs) เพื่อประเมินประสิทธิภาพและผลสัมฤทธิ์ของการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศในประเด็นที่สำคัญ เช่น ระดับการปฏิบัติตามนโยบาย อัตราการตอบสนองเหตุการณ์ผิดปกติ และความพร้อมใช้งานของระบบที่สำคัญ

7.2 จัดเก็บข้อมูลและดำเนินการวิเคราะห์ผลการดำเนินงานตามเกณฑ์ที่กำหนดไว้อย่างเป็นระบบ เพื่อให้สามารถประเมินแนวโน้มของความเสี่ยงและเหตุการณ์ด้านความมั่นคงปลอดภัย

7.3 จัดทำรายงานผลการประเมินและนำเสนอแก่ผู้บริหารระดับสูงหรือคณะกรรมการที่เกี่ยวข้องตามรอบระยะเวลาที่กำหนด เพื่อสนับสนุนการตัดสินใจเชิงกลยุทธ์ในการวางแผนและปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

8. **การสื่อสารและการฝึกอบรม** (Awareness and Training)

บริษัทตระหนักถึงความสำคัญของการส่งเสริมความตระหนักรู้และการพัฒนาทักษะด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศให้แก่บุคลากรทุกระดับอย่างต่อเนื่องและเป็นระบบ เพื่อให้บุคลากรสามารถใช้งานระบบสารสนเทศขององค์กรได้อย่างมั่นคงปลอดภัย มีความรับผิดชอบ และปฏิบัติตามกฎหมาย นโยบายภายใน และข้อกำหนดที่เกี่ยวข้องอย่างเคร่งครัด

ทั้งนี้ องค์กรควรกำหนดให้มีการสื่อสารและฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศที่ครอบคลุม ทั้งการเผยแพร่ข้อมูลข่าวสาร การจัดกิจกรรมสร้างการเรียนรู้ การฝึกอบรมทั้งในรูปแบบภาคทฤษฎีและเชิงปฏิบัติ รวมถึงการประเมินผลความรู้ความเข้าใจของบุคลากรอย่างสม่ำเสมอ เพื่อเสริมสร้างวัฒนธรรมความมั่นคงปลอดภัยในองค์กรอย่างยั่งยืน

9. **การทบทวนและปรับปรุงนโยบาย** (Policy Review and Updates)

บริษัทตระหนักถึงความสำคัญของการทบทวนและปรับปรุงนโยบายด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ เพื่อให้มั่นใจว่านโยบายดังกล่าวมีความเหมาะสม ทันสมัย สอดคล้องกับความเปลี่ยนแปลงของเทคโนโลยี ภัยคุกคาม กฎหมาย ข้อกำหนด และแนวทางปฏิบัติตามมาตรฐานสากล

บริษัทกำหนดให้มีการทบทวนและปรับปรุงนโยบายอย่างน้อยปีละหนึ่งครั้ง หรือทันทีเมื่อมีเหตุปัจจัยสำคัญที่อาจมีผลกระทบต่อความมั่นคงปลอดภัย เช่น การเปลี่ยนแปลงโครงสร้างองค์กร การเปลี่ยนแปลงกฎหมายหรือข้อบังคับใหม่ หรือเหตุการณ์ด้านความมั่นคงปลอดภัยที่สำคัญ เพื่อให้แน่ใจว่านโยบายยังคงมีประสิทธิภาพและสามารถนำไปปฏิบัติได้จริง

10. **การบังคับใช้และบทลงโทษ** (Enforcement and Penalties)

บริษัทกำหนดให้บุคลากรทุกระดับต้องปฏิบัติตามนโยบาย มาตรการ ขั้นตอนการปฏิบัติงาน และแนวทางที่อยู่ภายใต้กรอบการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างเคร่งครัด ทั้งนี้ เพื่อให้การดำเนินงานด้านระบบสารสนเทศ โครงสร้างพื้นฐานดิจิทัล และกระบวนการที่เกี่ยวข้องกับเทคโนโลยีขององค์กรเป็นไปอย่างมีประสิทธิภาพ ปลอดภัย โปร่งใส และสามารถตรวจสอบได้

การกระทำใด ๆ อันเป็นการละเมิด ฝ่าฝืน ละเลย ไม่ปฏิบัติตามนโยบาย มาตรการ ขั้นตอน แนวทางปฏิบัติที่กำหนดไว้หรือเอกสารที่เกี่ยวข้องกับการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์กร หรือปฏิบัติอย่างไม่เหมาะสม ไม่ว่าจะโดยเจตนา หรือประมาทเลินเล่อ ที่อาจส่งผลให้เกิดความเสี่ยงต่อความมั่นคงปลอดภัยของระบบสารสนเทศ ตลอดจนกระทบต่อความ ต่อเนื่องทางธุรกิจ ชื่อเสียง และความเชื่อมั่นของผู้มีส่วนได้ส่วนเสีย องค์กรจะดำเนินการตามมาตรการทางวินัยที่กำหนดไว้ในระเบียบหรือข้อบังคับของบริษัท กรุงเทพดุสิตเวชการ จำกัด (มหาชน) หรือบทลงโทษอื่นใดตามที่ระบุไว้ในข้อบังคับขององค์กร นโยบายด้านทรัพยากรบุคคล และ/หรือกฎหมายที่เกี่ยวข้อง

ในกรณีที่เป็นบุคคลภายนอก เช่น คู่สัญญา ผู้รับจ้าง หรือพันธมิตรทางธุรกิจ องค์กรอาจดำเนินการยกเลิกสัญญา ยุติความร่วมมือ หรือดำเนินการทางกฎหมายตามที่กำหนดไว้ในข้อตกลง

11. **เอกสารอ้างอิง** (Reference).

1. International Organization for Standardization & International Electrotechnical Commission. (2022). *ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. Geneva, Switzerland: ISO/IEC.
2. International Organization for Standardization & International Electrotechnical Commission. (2022). *ISO/IEC 27002:2022 — Information security, cybersecurity and privacy protection — Code of practice for information security controls*. Geneva, Switzerland: ISO/IEC.
3. International Organization for Standardization. (2016). *ISO 27799:2016 — Health informatics — Information security management in health using ISO/IEC 27002*. Geneva, Switzerland: ISO.
4. ISACA. (2018). *COBIT® 2019 framework: Governance and management objectives*. ISACA.
5. National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations (NIST Special Publication 800-53 Revision 5)*. Gaithersburg, MD: U.S. Department of Commerce.

6. สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์. (2562). แนวทางการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี (IT Governance Practice).
7. สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์. (2567). การกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ (Information Technology Governance) (แนบท้ายประกาศ สธ. 33/2567).

12. เอกสารที่เกี่ยวข้อง (Related documents)

1. เอกสารแนบท้าย 1: รายชื่อบริษัท กรุงเทพดุสิตเวชการ จำกัด (มหาชน) และบริษัทย่อย
2. นโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ (IT Governance Policy)

13. เอกสารแนบท้าย 1: รายชื่อบริษัท กรุงเทพดุสิตเวชการ จำกัด (มหาชน) และบริษัทย่อย

1. ธุรกิจโรงพยาบาลเอกชน (Healthcare Business)

   https://investor.bdms.co.th/th/general/bdms-at-a-glance

   20250513-bdms-he
   althcare-business-th

2. ธุรกิจที่เกี่ยวเนื่องกับการรักษาพยาบาล (Business Related to Medical Services)

   https://investor.bdms.co.th/th/general/bdms-at-a-glance

   20240313-businessr
   elated-to-medicalse