Data Privacy and Genetic Info Security

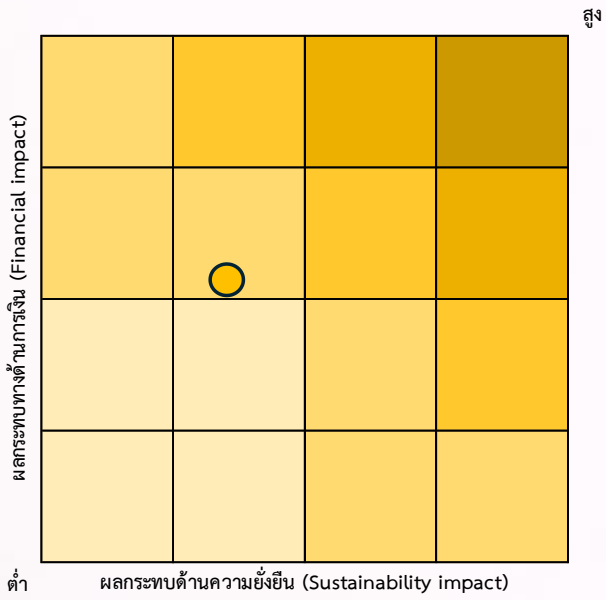
ความเป็นส่วนตัวและความปลอดภัยของข้อมูลสุขภาพ

บริษัทฯ ดำเนินธุรกิจธนาคารจัดเก็บเซลล์ต้นกำเนิดและธุรกิจชีวเภสัชภัณฑ์ การคุ้มครองความเป็นส่วนตัวของข้อมูลสุขภาพ (Health Data Privacy) และการรักษาความมั่นคงปลอดภัยของข้อมูลสุขภาพ (Health Data Security) ถือเป็นประเด็นที่บริษัทฯ ให้ความสำคัญเป็นอย่างสูง ข้อมูลที่จัดเก็บมีความอ่อนไหวและเกี่ยวข้องกับรหัสพันธุกรรมเฉพาะบุคคล ข้อมูลเหล่านี้จัดอยู่ในกลุ่มข้อมูลอ่อนไหวมาก (Highly Sensitive Data) เนื่องจากเป็นข้อมูลทางชีวมาตรและพันธุกรรมที่ไม่สามารถเปลี่ยนแปลงได้ หากเกิดการรั่วไหลจะส่งผลกระทบอย่างรุนแรงต่อความเป็นส่วนตัวและสิทธิส่วนบุคคล บริษัทฯ ยึดมั่นในการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) อย่างเคร่งครัด โดยบูรณาการระบบบริหารความเสี่ยงองค์กร (Enterprise Risk Management: ERM) ตามกรอบแนวทาง COSO มาบูรณาการเข้ากับการบริหารจัดการด้านเทคโนโลยีสารสนเทศ เพื่อสร้างระบบการรักษาความปลอดภัยที่มีประสิทธิภาพ มุ่งเน้นการใช้เทคโนโลยีขั้นสูงในการปกป้องข้อมูล เช่น การเข้ารหัสข้อมูลระดับสูง (Encryption) และการเตรียมความพร้อมผ่านแผนจำลองสถานการณ์วิกฤต (Scenario Simulation) รวมถึงการบูรณาการกำกับดูแลการใช้ปัญญาประดิษฐ์ (AI Governance) เพื่อกำกับดูแลการเข้าถึงและใช้ข้อมูลให้เป็นไปตามหลักจริยธรรมชีวภาพ (Bioethics) ความปลอดภัยของข้อมูลพันธุกรรมไม่ได้เป็นเพียงเรื่องของมาตรฐานทางเทคนิคสำหรับ องค์กร แต่เป็นหัวใจหลักของ ความน่าเชื่อถือ (Trust) ซึ่งเป็นรากฐานสำคัญในการขับเคลื่อนธุรกิจสู่การเป็นองค์กรสุขภาพที่ยั่งยืนแห่งอนาคต

ผลการดำเนินงานที่สำคัญ

- จำนวนเหตุการณ์ข้อมูลรั่วไหล เป็น 0 กรณี
- จำนวนพนักงานที่ผ่านการอบรมด้าน PDPA ร้อยละ 100
- จำนวนเหตุการณ์ที่ถูกโจมตีทางไซเบอร์เป็น 0 กรณี
- จำนวนเหตุการณ์ที่ไม่ปฏิบัติตามกฎระเบียบด้านความปลอดภัยเป็น 0 กรณี
- จำนวนพนักงานที่ผ่านการอบรมด้านความปลอดภัยเทคโนโลยีสารสนเทศ ร้อยละ 100

ความท้าทายและโอกาสทางธุรกิจ



การดำเนินธุรกิจด้านเวชศาสตร์ฟื้นฟูและชีวเภสัชภัณฑ์จำเป็นต้องอาศัยข้อมูลสุขภาพและข้อมูลชีวภาพ อาทิ ข้อมูลทางการแพทย์ ข้อมูลพันธุกรรม และข้อมูลการรักษาเฉพาะบุคคล ซึ่งก่อให้เกิดความท้าทายด้านการคุ้มครองความเป็นส่วนตัวและความมั่นคงปลอดภัยของข้อมูล ท่ามกลางกฎระเบียบที่เข้มงวดขึ้น เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) รวมถึงความคาดหวังของผู้รับบริการและพันธมิตรที่ต้องการความโปร่งใสและความเชื่อมั่นในการจัดการข้อมูล ครอบคลุมถึง ความเสี่ยงจากการโจมตีทางไซเบอร์ เช่น การสูญหายของข้อมูล การขโมยข้อมูล การทำลายระบบ การเรียกค่าไถ่ การรั่วไหลของข้อมูล หรือการใช้ข้อมูลเกินขอบเขตความยินยอม อาจส่งผลกระทบต่อความน่าเชื่อถือขององค์กร สถานะทางการเงิน ความต่อเนื่องทางธุรกิจ และความสามารถในการแข่งขันในระยะยาว บริษัทฯ นำความท้าทายเหล่านี้มาเปลี่ยนเป็นโอกาสทางธุรกิจในการสร้างความได้เปรียบทางการแข่งขันโดยการยกระดับระบบการกำกับดูแลและความปลอดภัยของข้อมูลสุขภาพให้สอดคล้องกับมาตรฐานสากล ถือเป็นโอกาสเชิงกลยุทธ์ในการสร้างความแตกต่างทางธุรกิจ นำไปสู่การสร้างความเชื่อมั่น (Trust) จากผู้รับบริการ โรงพยาบาล พันธมิตร และนักลงทุน พร้อมรองรับการขยายระบบนิเวศสุขภาพ การใช้เทคโนโลยีดิจิทัล และการพัฒนานวัตกรรมการแพทย์แบบเฉพาะบุคคลได้อย่างยั่งยืน อันจะนำไปสู่การสร้างคุณค่าทางสุขภาพและคุณค่าทางเศรษฐกิจควบคู่กันในระยะยาวต่อผู้มีส่วนได้เสีย และขับเคลื่อนการเติบโตที่ยั่งยืนในเวทีระดับโลก

ทิศทางและความมุ่งมั่นขององค์กร

ความมุ่งมั่นด้านการคุ้มครองความเป็นส่วนตัวของข้อมูลสุขภาพ

บริษัทฯ มุ่งมั่นในการคุ้มครองความเป็นส่วนตัวของข้อมูลสุขภาพ (Health Data Privacy) และการรักษาความมั่นคงปลอดภัยของข้อมูลสุขภาพ (Health Data Security) เป็นหลักสำคัญในการดำเนินธุรกิจด้วยความรับผิดชอบ โดยมุ่งเน้นการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) และมาตรฐานสากลอย่างเคร่งครัด ครอบคลุมการจัดการข้อมูลทุกรูปแบบทั้งรหัสพันธุกรรม เวชระเบียนดิจิทัล และบันทึกการรักษา โดยถือว่าการเคารพในสิทธิเหนือข้อมูลของผู้ป่วยคือการให้เกียรติในสิทธิมนุษยชนขั้นพื้นฐานที่ผู้รับบริการทุกคนพึงได้รับอย่างเท่าเทียมและเป็นธรรม นอกจากนี้ บริษัทฯ ยังให้ความสำคัญกับความโปร่งใสในทุกกระบวนการผ่านระบบการขอความยินยอม (Consent Management) ที่ชัดเจนเพื่อเปิดโอกาสให้ผู้ป่วยเข้าถึงและตรวจสอบข้อมูลของตนเองได้ตามระเบียบที่กำหนด ควบคู่ไปกับการสื่อสารและการตลาดเชิงจริยธรรมที่ปราศจากการละเมิดความเป็นส่วนตัว เพื่อสร้างความเชื่อมั่นและธรรมาภิบาลข้อมูล (Data Governance) ที่มั่นคง อันเป็นรากฐานสำคัญในการขับเคลื่อนนวัตกรรมการแพทย์ที่ยั่งยืน

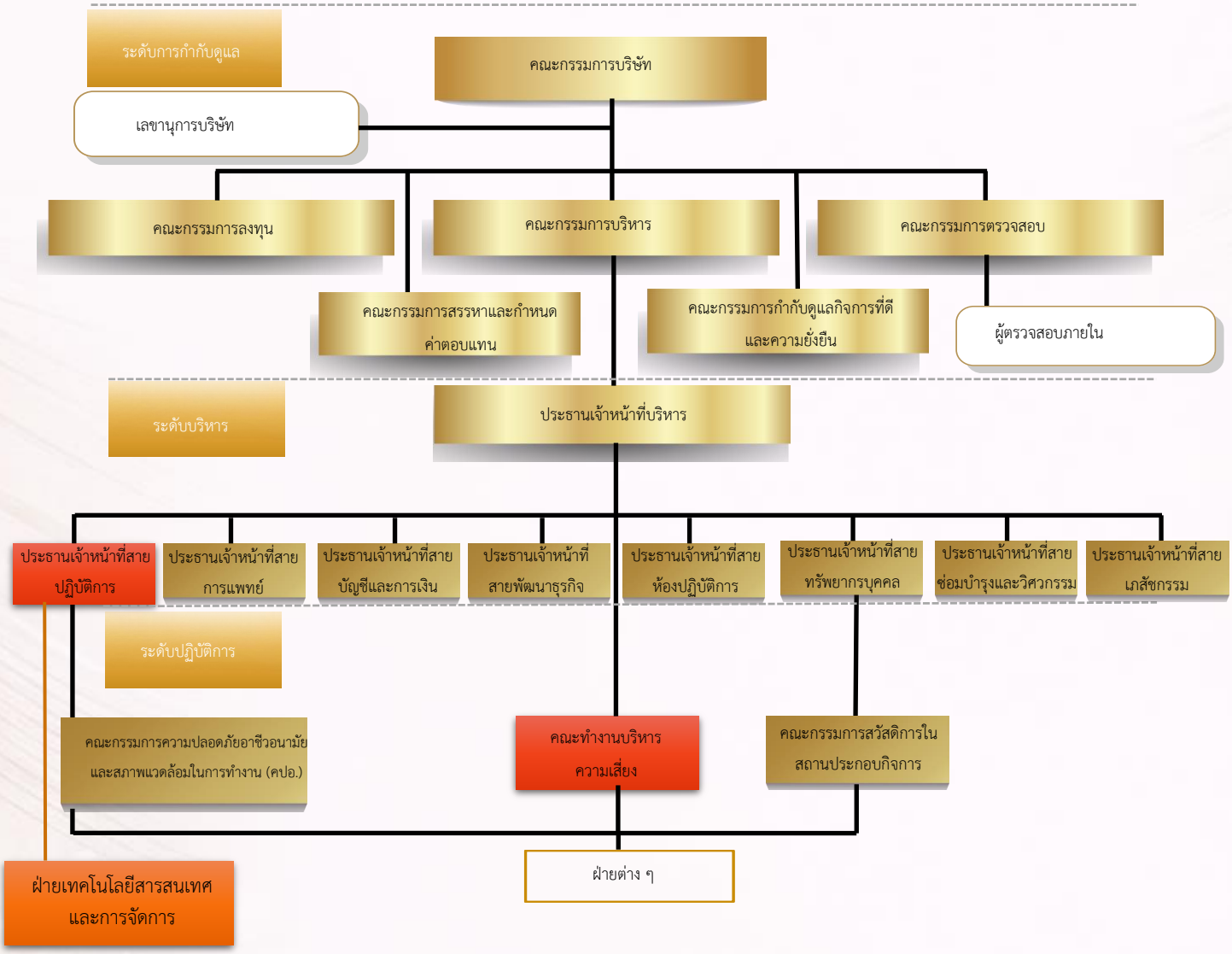
ตัวชี้วัดและเป้าหมายด้านการคุ้มครองความเป็นส่วนตัวของข้อมูลสุขภาพ

ตัวชี้วัด	เป้าหมายระยะสั้น ภายในปี 2570	เป้าหมายระยะยาว ภายในปี 2575
จำนวนเหตุการณ์ข้อมูลรั่วไหล	0 กรณี ต่อเนื่อง	0 กรณี ต่อเนื่อง
จำนวนพนักงานที่ผ่านการอบรมด้าน PDPA	ร้อยละ 100 ต่อเนื่อง	ร้อยละ 100 ต่อเนื่อง

โครงสร้างการบริหารจัดการด้านการคุ้มครองความเป็นส่วนตัวของข้อมูลสุขภาพ

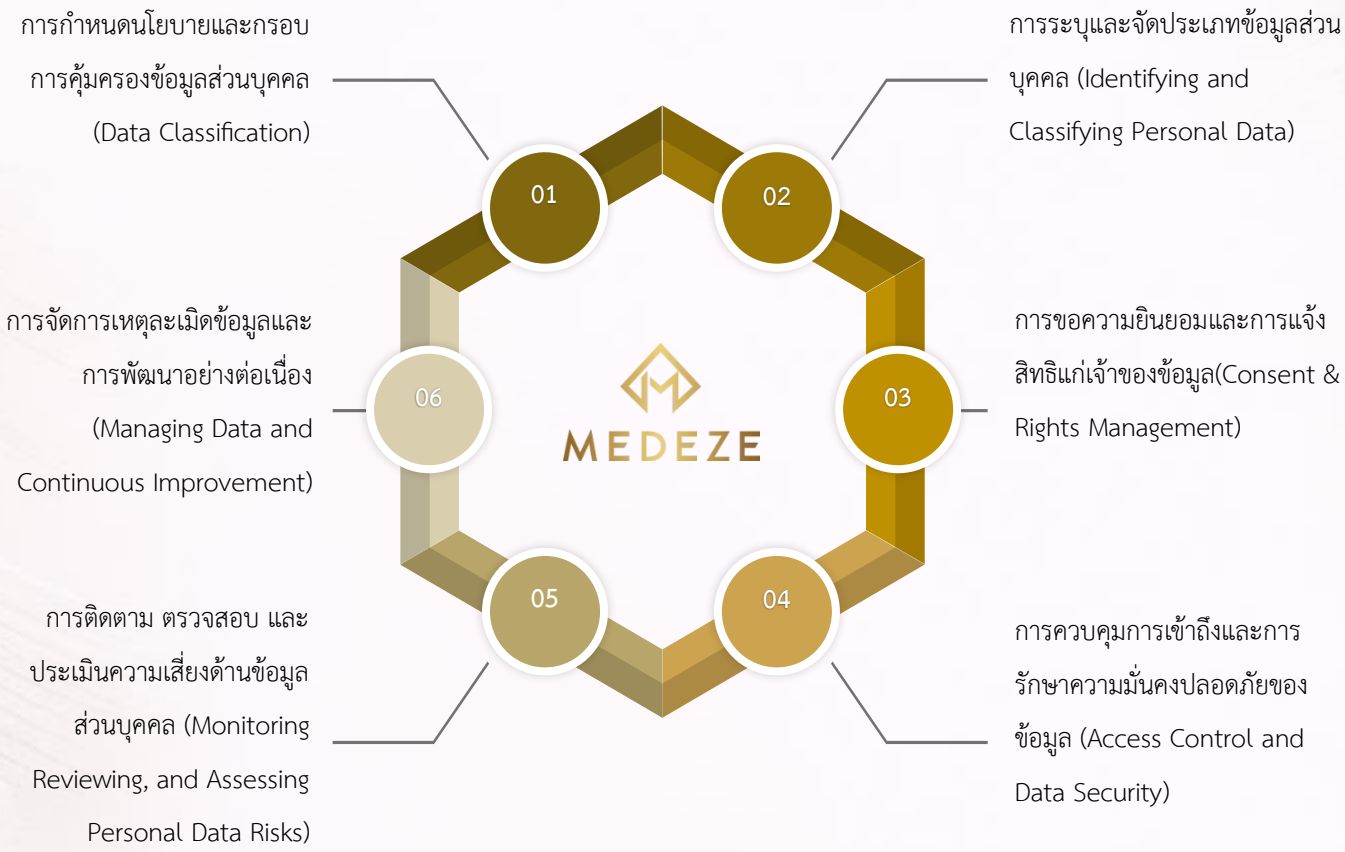
บริษัทฯ กำหนดโครงสร้างการกำกับดูแลด้านการคุ้มครองความเป็นส่วนตัวของข้อมูลสุขภาพอย่างเป็นระบบ เพื่อสร้างความเชื่อมั่นให้แก่ผู้รับบริการ ผู้มีส่วนได้เสีย และพันธมิตรทางธุรกิจ โดยแบ่งบทบาทหน้าที่ตามระดับการบริหารจัดการ ประกอบด้วย ประกอบด้วย 1) ระดับการกำกับดูแล (Board Level - Oversight) โดยคณะกรรมการบริษัท (Board of Directors) มีหน้าที่กำหนดทิศทางและกำกับดูแลนโยบายธรรมาภิบาลข้อมูล (Data Governance) และการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA) อย่างมีประสิทธิภาพ โดยติดตามรายงานสรุปเหตุการณ์และความคืบหน้าด้านความปลอดภัยสารสนเทศทุกไตรมาส เพื่อให้มั่นใจว่าองค์กรมีความพร้อมต่อภัยคุกคามทางไซเบอร์ในทุกรูปแบบ 2) ระดับบริหาร (Executive Level - Management) โดยคณะกรรมการบริหารและประธานเจ้าหน้าที่บริหารทำหน้าที่กำหนดนโยบายและกลยุทธ์ความมั่นคงปลอดภัยสารสนเทศตามมาตรฐานสากล จัดสรรทรัพยากรสำหรับการติดตั้งเทคโนโลยีการเข้ารหัสข้อมูลขั้นสูง (Data Encryption) และระบบควบคุมการเข้าถึงข้อมูลตามลำดับชั้นความลับ (Access Control) เพื่อปกป้องข้อมูลสุขภาพของผู้รับบริการ และ 3) ระดับปฏิบัติการ (Operational Level - Implementation) โดยฝ่ายเทคโนโลยีสารสนเทศและการจัดการ มีบทบาทสำคัญในการดูแลและปกป้องข้อมูลสุขภาพ การดำเนินการเฝ้าระวัง การตรวจสอบ และการตอบสนองต่อเหตุการณ์ด้านความปลอดภัยของข้อมูล (Incident Response Plan) อย่างเป็นระบบ รวมถึงการบริหารจัดการความยินยอมของเจ้าของข้อมูล (Consent Management) เพื่อให้มั่นใจว่าการเก็บรวบรวม ใช้ และเปิดเผยข้อมูล

เป็นไปอย่างถูกต้องตามกฎหมาย นอกจากนี้ บริษัทฯ ยังให้ความสำคัญกับการบริหารจัดการข้อมูลสุขภาพภายใต้หลักความถูกต้อง โปร่งใส และตรวจสอบได้ โดยมีการกำหนดมาตรการควบคุมภายในและการตรวจสอบอย่างสม่ำเสมอ เพื่อป้องกันความเสี่ยงจากการรั่วไหล การเข้าถึงโดยไม่ได้รับอนุญาต และการนำข้อมูลไปใช้ในทางที่ไม่เหมาะสม ตลอดจนสร้างความเชื่อมั่นให้แก่ผู้มีส่วนได้เสียในด้านการคุ้มครองข้อมูลส่วนบุคคลอย่างยั่งยืน



แนวทางการบริหารจัดการด้านการคุ้มครองความเป็นส่วนตัวของข้อมูลสุขภาพ

บริษัทฯ ดำเนินธุรกิจในอุตสาหกรรมชีวเวชภัณฑ์ ซึ่งมีความเกี่ยวข้องโดยตรงกับข้อมูลด้านสุขภาพของผู้รับบริการ และข้อมูลการวินิจฉัยทางการแพทย์จัดเป็นข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Personal Data) การคุ้มครองความเป็นส่วนตัวของข้อมูลสุขภาพและการเคารพสิทธิความเป็นส่วนตัวถือเป็นหัวใจสำคัญในการดำเนินธุรกิจอย่างมีความรับผิดชอบ และเป็นรากฐานในการสร้างความไว้วางใจต่อองค์กรในระยะยาว บริษัทฯ จึงกำหนดแนวทางการบริหารจัดการข้อมูลสุขภาพอย่างเป็นระบบครอบคลุมตั้งแต่การเก็บรวบรวม การใช้ การเปิดเผย จนถึงการจัดเก็บรักษา โดยยึดมั่นในหลักความโปร่งใส ความถูกต้อง และความมั่นคงปลอดภัยตามมาตรฐานสากล สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) และกฎระเบียบที่เกี่ยวข้องอย่างเคร่งครัด ดังนี้



1. การบูรณาการนโยบายความเป็นส่วนตัว

บริษัทฯ กำหนดและประกาศนโยบายความเป็นส่วนตัวโดยให้ความสำคัญลำดับแรกกับคุณภาพการรักษาและความปลอดภัยของข้อมูลโดยบูรณาการการกำกับดูแลกิจการที่ดีภายใต้ระบบคุ้มครองข้อมูลส่วนบุคคลและรักษาความมั่นคงปลอดภัยสารสนเทศสุขภาพที่เข้มงวดตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA) เพื่อคุ้มครองข้อมูลสุขภาพและข้อมูลส่วนบุคคลของผู้รับบริการ โดยมีนโยบายชัดเจนในการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูล และจัดตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) เพื่อดูแลความปลอดภัย ตามมาตรฐานกฎหมาย

ผลการดำเนินงานที่สำคัญ

บริษัทฯ ให้ความสำคัญกับการคุ้มครองความเป็นส่วนตัวและความมั่นคงปลอดภัยของข้อมูลสุขภาพในฐานะปัจจัยพื้นฐานในการสร้างความเชื่อมั่นและความไว้วางใจจากผู้รับบริการ โดยได้พัฒนาระบบการบริหารจัดการข้อมูลให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) และมาตรฐานความปลอดภัยสารสนเทศในระดับสากลอย่างต่อเนื่อง บริษัทฯ ได้กำหนดแนวทางการบริหารจัดการข้อมูลสุขภาพครอบคลุมทั้งด้านการคุ้มครองความเป็นส่วนตัว (Health Data Privacy) และความมั่นคงปลอดภัยของข้อมูล (Health Data Security) โดยดำเนินการให้สอดคล้องกับข้อกำหนดของกฎหมายและมาตรฐานที่เกี่ยวข้องอย่างเคร่งครัด

เป้าหมาย	ผลลัพธ์การดำเนินงานปี 2568
จำนวนเหตุการณ์ข้อมูลรั่วไหล	0 กรณี
จำนวนพนักงานที่ผ่านการอบรมด้าน PDPA	ร้อยละ 100

จำนวนเหตุการณ์ข้อมูลรั่วไหล

บริษัทฯ ให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลและข้อมูลสำคัญขององค์กร โดยกำหนดมาตรการควบคุม ดูแล และป้องกันความเสี่ยงด้านข้อมูลอย่างเหมาะสม ครอบคลุมทั้งด้านนโยบาย กระบวนการปฏิบัติงาน ระบบเทคโนโลยีสารสนเทศ และการสร้างความตระหนักรู้แก่บุคลากรในทุกระดับ เพื่อป้องกันการเข้าถึง การใช้ หรือการเปิดเผยข้อมูลโดยมิชอบ ตลอดจนลดความเสี่ยงจากเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งนี้ บริษัทฯ มีการติดตาม เฝ้าระวัง และทบทวนประสิทธิผลของมาตรการที่เกี่ยวข้องอย่างสม่ำเสมอ ส่งผลให้ในปี 2568 ไม่พบกรณีหรือเหตุการณ์ข้อมูลรั่วไหลเป็น 0 กรณี

การอบรมคุ้มครองข้อมูลส่วนบุคคล (PDPA)

บริษัทฯ ให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลและการพัฒนาศักยภาพบุคลากรอย่างต่อเนื่อง โดยกำหนดให้พนักงานทุกคนต้องผ่านการปฐมนิเทศและเข้ารับการอบรมด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA) นโยบายการคุ้มครองข้อมูลของบริษัทฯ ตลอดจนการพัฒนาความรู้และทักษะตามหลักสูตรที่กำหนดไว้สำหรับแต่ละตำแหน่งงานอย่างเคร่งครัด ทั้งนี้ ผลการเข้ารับการอบรมยังถูกนำมาใช้เป็นส่วนหนึ่งของการประเมินผลการปฏิบัติงานและการพิจารณาเลื่อนตำแหน่ง เพื่อส่งเสริมให้บุคลากรทุกระดับปฏิบัติงานอย่างมีความรับผิดชอบ สอดคล้องกับมาตรฐานขององค์กร และสามารถดูแลข้อมูลสำคัญได้อย่างเหมาะสม โดยในปี 2568 พนักงานเข้ารับการอบรมครบถ้วนคิดเป็นร้อยละ 100

ผลลัพธ์การปรับปรุงอย่างต่อเนื่อง

บริษัทฯ มุ่งยกระดับการบริหารจัดการด้านธรรมาภิบาลและความยั่งยืนให้สอดคล้องกับมาตรฐานสากล ในการสร้างความเชื่อมั่นให้แก่ผู้มีส่วนได้เสียและยกระดับขีดความสามารถในการแข่งขันในระยะยาวในด้านธรรมาภิบาล (Good Governance) โดยให้ความสำคัญกับการบริหารจัดการเชิงกลยุทธ์ ประกอบด้วย 1) ธรรมาภิบาลและการกำกับดูแลข้อมูลสุขภาพ โดยมุ่งเน้นการกำกับดูแลข้อมูล (Data Governance) ที่ครอบคลุมทั้งการคุ้มครองความเป็นส่วนตัวของข้อมูลสุขภาพ (Health Data Privacy) และ การรักษาความมั่นคงปลอดภัยของข้อมูลสุขภาพ (Health Data Security) ในการรักษามาตรฐานสูงสุดในการรักษาความลับและความปลอดภัยของข้อมูลทางชีวภาพของผู้รับบริการ และ 2) การขับเคลื่อนนวัตกรรมและเทคโนโลยีที่รับผิดชอบ โดยมีแผนนำเทคโนโลยีขั้นสูงและปัญญาประดิษฐ์มาประยุกต์ใช้เพื่อเพิ่มประสิทธิภาพและความแม่นยำในการดำเนินงาน ตลอดจนการตัดสินใจเชิงกลยุทธ์ โดยยึดหลักจริยธรรม ความโปร่งใส และความรับผิดชอบในการใช้เทคโนโลยี ควบคู่ไปกับการวางโครงสร้างพื้นฐานด้านความปลอดภัยทางไซเบอร์ที่ล้ำสมัย เพื่อป้องกันความเสี่ยงและคุ้มครองสิทธิข้อมูลส่วนบุคคลอย่างเข้มงวด

ทิศทางและความมุ่งมั่นขององค์กร

ความมุ่งมั่นด้านการรักษาความมั่นคงปลอดภัยของข้อมูลสุขภาพ

บริษัทฯ มุ่งมั่นยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลสุขภาพสู่ระดับสากล ผ่านการวางรากฐานโครงสร้างพื้นฐานเทคโนโลยีที่ทันสมัยในการป้องกันภัยคุกคามทางไซเบอร์เชิงรุก โดยยึดกรอบมาตรฐานระดับโลกในการรักษาความลับ (Confidentiality) ความถูกต้อง (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูลผู้รับบริการ นอกจากนี้ บริษัทฯ บูรณาการระบบการควบคุมการเข้าถึงข้อมูลตามลำดับชั้นความลับ (Access Control) และเทคโนโลยีการเข้ารหัสข้อมูลขั้นสูง (Data Encryption) มาใช้ควบคู่กับกระบวนการเฝ้าระวังภัยคุกคามแบบเรียลไทม์โดยทีมผู้เชี่ยวชาญเฉพาะด้าน (IT Security) และ บริษัทฯ ยังให้ความสำคัญกับระบบธรรมาภิบาลที่โปร่งใสผ่านการตรวจสอบโดยคณะกรรมการบริษัทเป็นประจำทุกปี และมีการจัดทำแผนฉุกเฉินรวมถึงแผนตอบสนองที่มีประสิทธิภาพสอดคล้องกับข้อกำหนดของกฎหมายในการสร้างความเชื่อมั่นต่อผู้มีส่วนได้เสียทุกกลุ่มเกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูลสุขภาพที่อ่อนไหวจะได้รับการปกป้องภายใต้มาตรฐานความปลอดภัยระดับสูงสุด

ตัวชี้วัดและเป้าหมายด้านการรักษาความมั่นคงปลอดภัยของข้อมูลสุขภาพ

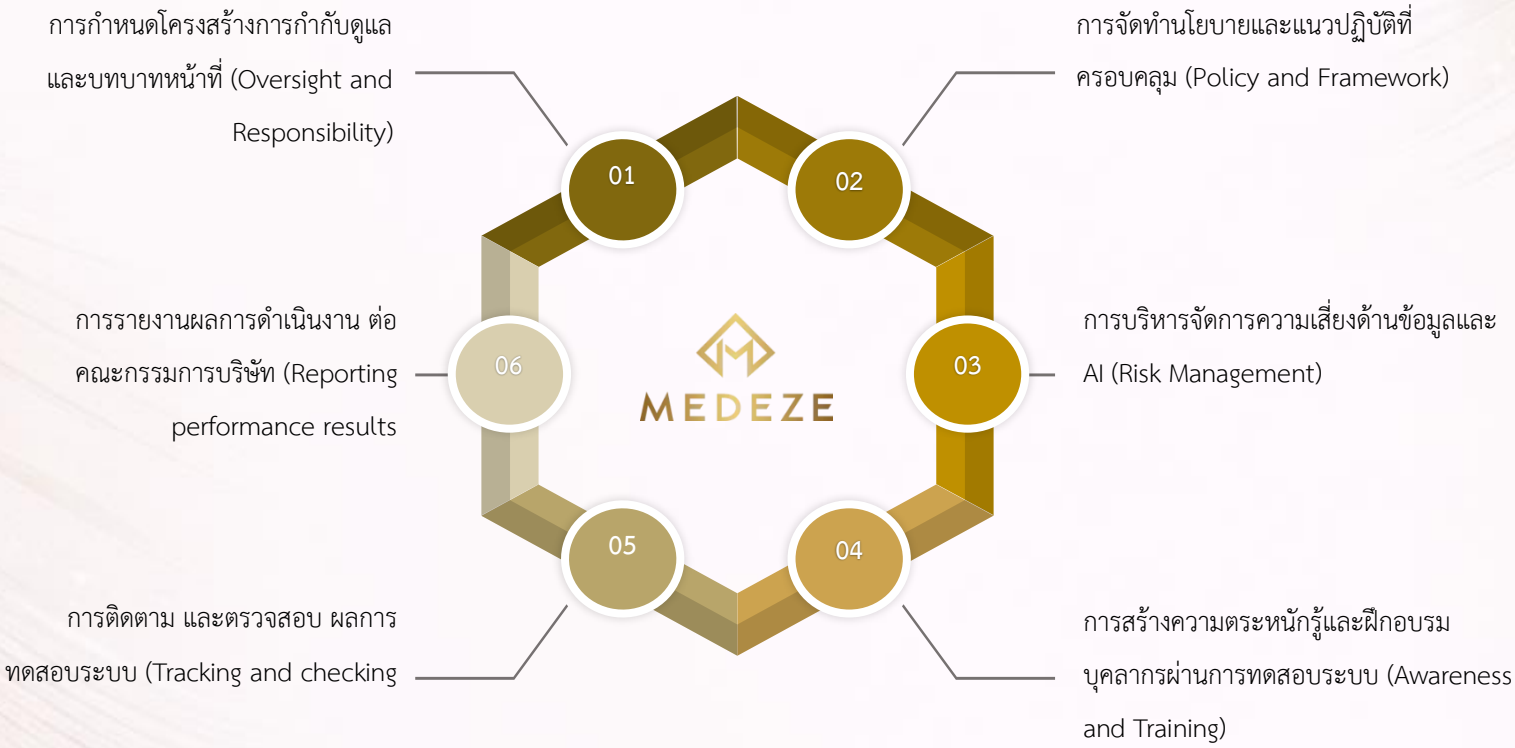
ตัวชี้วัด	เป้าหมายระยะสั้น ภายในปี 2570	เป้าหมายระยะยาว ภายในปี 2575
จำนวนเหตุการณ์ที่บริษัทถูกโจมตีทางไซเบอร์	0 กรณี ต่อเนื่อง	0 กรณี ต่อเนื่อง
จำนวนเหตุการณ์ที่ไม่ปฏิบัติตามกฎระเบียบด้านความปลอดภัย	0 กรณี ต่อเนื่อง	0 กรณี ต่อเนื่อง
จำนวนพนักงานที่ผ่านการอบรมด้านความปลอดภัยเทคโนโลยีสารสนเทศ	ร้อยละ 100 ต่อเนื่อง	ร้อยละ 100 ต่อเนื่อง

โครงสร้างการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยของข้อมูลสุขภาพ

บริษัทฯ กำหนดให้มีโครงสร้างการบริหารจัดการรักษาความมั่นคงปลอดภัยของข้อมูลสุขภาพและเป็นระบบในการรองรับกระบวนการเก็บรวบรวม การใช้ การเปิดเผย และการจัดเก็บข้อมูลให้เป็นไปอย่างเหมาะสมภายใต้กฎหมาย มาตรฐานสากล และหลักการกำกับดูแลกิจการที่ดี และการรักษาความมั่นคงปลอดภัยของข้อมูลสุขภาพให้เป็นไปอย่างเหมาะสมภายใต้กฎหมาย มาตรฐานที่เกี่ยวข้อง และหลักการกำกับดูแลกิจการที่ดี โดยแบ่งบทบาทหน้าที่ตามระดับการบริหารจัดการ ประกอบด้วย 1) ระดับการกำกับดูแล (Board Level- Oversight) โดยคณะกรรมการบริษัท (Board of Directors) ทำหน้าที่กำกับดูแล อนุมัติ และให้ความเห็นชอบ ทิศทางและกรอบการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยของข้อมูลสุขภาพ รวมถึงติดตามและประเมินผลการดำเนินงานของฝ่ายบริหารอย่างต่อเนื่อง เพื่อให้มั่นใจว่าการบริหารจัดการความเสี่ยงและระบบควบคุมภายในมีความเพียงพอ เหมาะสม และสอดคล้องกับกฎหมายและมาตรฐานที่เกี่ยวข้อง กำหนดทิศทางและกำกับดูแลกรอบการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยของข้อมูลสุขภาพ รวมถึงติดตามประเด็นสำคัญด้านความมั่นคงปลอดภัยสารสนเทศ ความเสี่ยงที่มีนัยสำคัญ และความก้าวหน้าในการดำเนินมาตรการต่าง ๆ อย่างต่อเนื่อง เพื่อให้มั่นใจว่าบริษัทฯ มีระบบควบคุมภายในที่เพียงพอ เหมาะสม และพร้อมรองรับภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น 2) ระดับบริหาร (Executive Level - Management) โดยคณะกรรมการบริหารและประธานเจ้าหน้าที่บริหารทำหน้าที่กำหนดนโยบาย ขับเคลื่อนนโยบายและมาตรการด้านความมั่นคงปลอดภัยของข้อมูลสุขภาพ ให้สอดคล้องกับความเสี่ยงขององค์กรและกรอบที่คณะกรรมการบริษัทให้ความเห็นชอบ พร้อมทั้งกำหนดแนวทางการดำเนินงาน ระบบควบคุม และนำเทคโนโลยีที่เหมาะสมมาใช้ เช่น การเข้ารหัสข้อมูล (Data Encryption) การควบคุมสิทธิการเข้าถึงข้อมูล (Access Control) การสำรองข้อมูล และการบริหารจัดการสิทธิผู้ใช้งาน เพื่อให้การดำเนินงานเป็นไปอย่างมีประสิทธิภาพและสามารถนำไปปฏิบัติได้จริง และ 3) ระดับปฏิบัติการ (Operational Level) ฝ่ายเทคโนโลยีสารสนเทศและการจัดการ ทำหน้าที่ดำเนินการตามมาตรการที่กำหนด ติดตาม ตรวจสอบ ทดสอบประสิทธิผลของมาตรการด้านความปลอดภัย จัดทำและทบทวนแผนตอบสนองต่อเหตุการณ์ (Incident Response Plan) และฟื้นฟูระบบกรณีเกิดเหตุการณ์ เฝ้าระวังความเสี่ยงด้านข้อมูลอย่างใกล้ชิด ประเมินประสิทธิผลของระบบรักษาความมั่นคงปลอดภัยอย่างสม่ำเสมอ และจัดทำแผนรองรับเหตุการณ์ด้านความมั่นคงปลอดภัย (Incident Response Plan) เพื่อให้สามารถตอบสนองและฟื้นฟูระบบได้อย่างทันท่วงที เพื่อจำกัดผลกระทบที่อาจเกิดขึ้นต่อข้อมูลสุขภาพและการดำเนินธุรกิจให้อยู่ในระดับที่เหมาะสม นอกจากนี้ บริษัทฯ ยังให้ความสำคัญกับการพัฒนาและยกระดับระบบการบริหารจัดการด้านความมั่นคงปลอดภัยของข้อมูลสุขภาพอย่างต่อเนื่อง ผ่านการกำหนดแนวปฏิบัติ การติดตามตรวจสอบ และการประเมินประสิทธิผลของมาตรการควบคุม เพื่อให้การดำเนินงานเป็นไปอย่างถูกต้อง โปร่งใส และสอดคล้องกับมาตรฐานสากล อันจะนำไปสู่การเสริมสร้างความเชื่อมั่นให้แก่ผู้มีส่วนได้เสีย และสนับสนุนการเติบโตอย่างยั่งยืนขององค์กรในระยะยาว

แนวทางการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยของข้อมูลสุขภาพ

บริษัทฯ ให้ความสำคัญกับการพัฒนาระบบและมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลสุขภาพอย่างเป็นระบบ ครอบคลุมทั้งด้านนโยบาย เทคโนโลยี กระบวนการทำงาน และการพัฒนาศักยภาพบุคลากร เพื่อป้องกันความเสี่ยงจากการรั่วไหล การเข้าถึงโดยมิชอบ การนำข้อมูลไปใช้ในทางที่ไม่เหมาะสม และภัยคุกคามไซเบอร์ จึงได้กำหนดแนวทางการบริหารจัดการขึ้นภายใต้ธรรมาภิบาลและการกำกับดูแลเทคโนโลยีปัญญาประดิษฐ์ (AI Governance) เพื่อเป็นกรอบการดำเนินงานที่มีประสิทธิภาพ โปร่งใส และสอดคล้องกับกฎหมายและมาตรฐานสากล



1. การกำหนดโครงสร้างการกำกับดูแลและบทบาทหน้าที่ที่ชัดเจน (Oversight and Responsibility)

บริษัทฯ กำหนดโครงสร้างการกำกับดูแลด้านข้อมูลสุขภาพและเทคโนโลยีปัญญาประดิษฐ์อย่างชัดเจน โดยระบุบทบาทหน้าที่ และความรับผิดชอบของคณะกรรมการบริษัท ผู้บริหาร และหน่วยงานที่เกี่ยวข้อง เพื่อให้การกำกับดูแลเป็นไปอย่างมีประสิทธิภาพ โปร่งใส และสามารถตรวจสอบได้ บริษัทฯ ให้ความสำคัญต่อการคุ้มครองข้อมูลสุขภาพ โดยบูรณาการนโยบายความปลอดภัยของข้อมูลเข้ากับการดำเนินงานในทุกระดับ เพื่อให้สอดคล้องกับกฎหมายและมาตรฐานสากล กำหนดมาตรการควบคุมการเข้าถึง การจัดเก็บ และการส่งต่อข้อมูลอย่างปลอดภัย พร้อมทั้งติดตามและประเมินความเสี่ยงอย่างอย่างต่อเนื่อง เพื่อเสริมสร้างความเชื่อมั่นแก่ผู้มีส่วนได้เสีย และสนับสนุนการดำเนินธุรกิจอย่างยั่งยืน

2. การจัดทำนโยบาย กรอบการดำเนินงาน และแนวปฏิบัติที่ครอบคลุม (Policy and Framework)

บริษัทฯ จัดทำนโยบาย กรอบการบริหารจัดการ และแนวปฏิบัติที่ครอบคลุมการคุ้มครองข้อมูลสุขภาพ ความมั่นคงปลอดภัยไซเบอร์ และการใช้ AI อย่างรับผิดชอบ เพื่อใช้เป็นแนวทางในการดำเนินงานให้สอดคล้องกับกฎหมาย ข้อกำหนดและมาตรฐานที่เกี่ยวข้อง

3. **การบริหารจัดการความเสี่ยงด้านข้อมูลและเทคโนโลยีปัญญาประดิษฐ์ (Risk Management)**

บริษัทฯ บูรณาการการบริหารความเสี่ยงด้านข้อมูลและ AI เข้ากับกระบวนการบริหารความเสี่ยงขององค์กร โดยครอบคลุมการระบุ การประเมิน การควบคุม และการติดตามความเสี่ยงที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูลความเป็นส่วนตัว และการดำเนินธุรกิจ

4. **การสร้างความตระหนักรู้และการพัฒนาศักยภาพบุคลากรผ่านการฝึกอบรมและการทดสอบระบบ (Awareness and Training)**

บริษัทฯ ส่งเสริมความรู้ ความเข้าใจ และความตระหนักรู้ของบุคลากรในด้านการคุ้มครองข้อมูล ความมั่นคงปลอดภัยไซเบอร์ และการใช้ AI อย่างเหมาะสม ผ่านการฝึกอบรม การสื่อสารภายใน และการทดสอบระบบอย่างต่อเนื่อง เพื่อเสริมสร้างวัฒนธรรมองค์กรด้านความปลอดภัยของข้อมูล

5. **การติดตาม ตรวจสอบ และประเมินผลจากการทดสอบระบบอย่างสม่ำเสมอ (Monitoring, Review and Testing Evaluation)**

บริษัทฯ จัดให้มีกระบวนการติดตาม ตรวจสอบ และประเมินผลการทดสอบระบบอย่างต่อเนื่อง เพื่อประเมินประสิทธิภาพของมาตรการควบคุมภายใน ระบุช่องโหว่หรือประเด็นที่ต้องปรับปรุง และยกระดับความพร้อมในการรับมือกับความเสี่ยงที่อาจเกิดขึ้น

6. **การรายงานผลการดำเนินงานต่อคณะกรรมการบริษัทและผู้บริหารระดับสูง (Reporting Performance Results)**

บริษัทฯ กำหนดให้มีการรายงานผลการดำเนินงาน ประเด็นความเสี่ยง เหตุการณ์สำคัญ และผลการปรับปรุงมาตรการที่เกี่ยวข้องต่อคณะกรรมการบริษัทและผู้บริหารระดับสูงอย่างสม่ำเสมอ เพื่อสนับสนุนการกำกับดูแล การตัดสินใจเชิงกลยุทธ์และการพัฒนาระบบอย่างต่อเนื่อง

ผลการดำเนินงานที่สำคัญ

บริษัทฯ ให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยของข้อมูลสุขภาพภายใต้บริบทของภัยคุกคามทางไซเบอร์ที่มีความซับซ้อนและเปลี่ยนแปลงอย่างต่อเนื่อง โดยมุ่งเน้นการพัฒนาระบบบริหารจัดการและมาตรการควบคุมที่ทันสมัยในการปกป้องความลับ ความถูกต้อง และความพร้อมใช้งานของข้อมูลผู้รับบริการอย่างมีประสิทธิภาพสูงสุด

เป้าหมาย	ผลลัพธ์การดำเนินงานปี 2568
จำนวนเหตุการณ์ที่บริษัทถูกโจมตีทางไซเบอร์	0 กรณี
จำนวนเหตุการณ์ที่ไม่ปฏิบัติตามกฎระเบียบด้านความปลอดภัย	0 กรณี
จำนวนพนักงานที่ผ่านการอบรมด้านความปลอดภัยเทคโนโลยีสารสนเทศ	ร้อยละ 100

เหตุการณ์ที่บริษัทถูกโจมตีทางไซเบอร์

บริษัทฯ ให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์และการปกป้องข้อมูลสารสนเทศขององค์กรอย่างต่อเนื่อง โดยมีการกำหนดมาตรการเฝ้าระวัง ป้องกัน และติดตามความเสี่ยงด้านไซเบอร์อย่างเหมาะสม ทั้งนี้ ในปี 2568 บริษัทฯ ไม่พบกรณีหรือเหตุการณ์การถูกโจมตีทางไซเบอร์ที่มีนัยสำคัญ โดยมีจำนวนเหตุการณ์ที่เกี่ยวข้องเป็น 0 กรณี

เหตุการณ์ที่ไม่ปฏิบัติตามกฎระเบียบด้านความปลอดภัย

บริษัทฯ ตั้งเป้าหมายให้จำนวนกรณีหรือเหตุการณ์ที่ไม่ปฏิบัติตามกฎระเบียบด้านความปลอดภัยเป็นศูนย์ และในปี 2568 บริษัทฯ ไม่พบกรณีการไม่ปฏิบัติตามกฎระเบียบด้านความปลอดภัย เป็น 0 กรณี แสดงถึงความมุ่งมั่นในการกำกับดูแลการดำเนินงานให้เป็นไปตามกฎหมาย มาตรฐาน และข้อกำหนดด้านความปลอดภัยอย่างเคร่งครัด เพื่อสร้างสภาพแวดล้อมการทำงานที่ปลอดภัยและลดความเสี่ยงที่อาจส่งผลกระทบต่อพนักงาน ผู้มีส่วนได้เสีย และการดำเนินธุรกิจโดยรวม

พนักงานที่ผ่านการอบรมด้านความปลอดภัยเทคโนโลยีสารสนเทศ

บริษัทฯ ให้ความสำคัญกับการพัฒนาความรู้และความตระหนักด้านความปลอดภัยเทคโนโลยีสารสนเทศแก่พนักงานทุกระดับ เพื่อเสริมสร้างความสามารถในการป้องกันภัยคุกคามทางไซเบอร์ การใช้ระบบสารสนเทศอย่างเหมาะสม และการดูแลข้อมูลขององค์กรอย่างปลอดภัย โดยในปี 2568 พนักงานที่ผ่านการอบรมด้านความปลอดภัยเทคโนโลยีสารสนเทศคิดเป็นร้อยละ 100 ของพนักงานทั้งหมด

ผลลัพธ์การปรับปรุงอย่างต่อเนื่อง

บริษัทฯ ให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยของข้อมูลสุขภาพ โดยมุ่งปกป้องความลับ ความถูกต้องและความพร้อมใช้งานของข้อมูลผู้รับบริการ ท่ามกลางความเสี่ยงด้านไซเบอร์ที่มีความซับซ้อนและทวีความรุนแรงมากขึ้นอย่างต่อเนื่อง ทั้งนี้ บริษัทฯ ได้กำหนดมาตรการและแนวปฏิบัติด้านความปลอดภัยของข้อมูลที่สอดคล้องกับกฎหมายและมาตรฐานที่เกี่ยวข้อง และมาตรฐานสากลด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อให้มั่นใจว่าข้อมูลของผู้รับบริการได้รับการคุ้มครองอย่างรอบด้านและมีประสิทธิภาพ บริษัทฯ ยังคงมุ่งมั่นพัฒนาและปรับปรุงกระบวนการบริหารจัดการอย่างต่อเนื่อง เพื่อยกระดับมาตรฐานการดำเนินธุรกิจอย่างมีจริยธรรมและสนับสนุนการเติบโตอย่างยั่งยืนในระยะยาว