นโยบายการคุ้มครองข้อมูลส่วนบุคคล

ฉบับที่ 1/2568 VNG-GOV-PDP-PL-01
วันที่มีผลบังคับใช้: 11 พฤศจิกายน 2568

VANACHAI GROUP

นโยบายการคุ้มครองข้อมูลส่วนบุคคล
บริษัท วนชัย กรุ๊ป จำกัด (มหาชน) และบริษัทย่อย

บริษัท วนชัย กรุ๊ป จำกัด (มหาชน) และบริษัทย่อย ("บริษัท") ตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลของผู้มีส่วนได้เสียทุกกลุ่ม ทั้งพนักงาน ลูกค้า คู่ค้า ผู้ถือหุ้น และบุคคลที่เกี่ยวข้องกับการดำเนินธุรกิจของบริษัท การเก็บรวบรวม การใช้ การเปิดเผย หรือการประมวลผลข้อมูลส่วนบุคคลใด ๆ ต้องดำเนินการอย่างโปร่งใส ถูกต้องตามกฎหมาย และเคารพสิทธิความเป็นส่วนตัวของเจ้าของข้อมูลทุกคน

บริษัทมีความมุ่งมั่นในการดำเนินธุรกิจอย่างมีธรรมาภิบาล โปร่งใส และรับผิดชอบต่อสังคม ภายใต้กรอบของกฎหมายคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และมาตรฐานสากลที่เกี่ยวข้อง รวมถึงหลักเกณฑ์ของ FTSE Russell Social Pillar (SHR07: Data Privacy) เพื่อให้มั่นใจว่าการบริหารจัดการข้อมูลส่วนบุคคลเป็นไปอย่างเหมาะสม มีมาตรการป้องกันความเสี่ยงด้านความปลอดภัยของข้อมูลอย่างรัดกุม และลดโอกาสในการเกิดการละเมิดข้อมูล (Data Breach)

นโยบายฉบับนี้จัดทำขึ้นเพื่อกำหนดแนวทางการบริหารจัดการข้อมูลส่วนบุคคลให้สอดคล้องกับหลักเกณฑ์สากลด้านความเป็นส่วนตัวของข้อมูล และใช้เป็นกรอบกำกับดูแลสำหรับพนักงานและผู้ที่เกี่ยวข้องทุกฝ่าย โดยมีจุดมุ่งหมายเพื่อสร้างความมั่นใจให้แก่ผู้มีส่วนได้เสียว่าข้อมูลส่วนบุคคลของตนจะถูกเก็บรวบรวม ใช้ และเปิดเผยอย่างถูกต้องตามวัตถุประสงค์ที่กำหนดไว้ พร้อมทั้งป้องกันการเข้าถึง การใช้ หรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

บริษัทมุ่งส่งเสริมให้เกิดวัฒนธรรมองค์กรที่ให้ความสำคัญต่อความปลอดภัยและความเป็นส่วนตัวของข้อมูล ควบคู่ไปกับการกำหนดบทบาทและความรับผิดชอบของบุคลากรทุกระดับ โดยได้แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) เพื่อทำหน้าที่กำกับดูแลและติดตามให้การดำเนินงานเป็นไปตามกฎหมายอย่างเคร่งครัด ทั้งนี้ บริษัทได้บูรณาการนโยบายการคุ้มครองข้อมูลส่วนบุคคลฉบับนี้เข้ากับนโยบายการรักษาความลับของข้อมูลและนโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ เพื่อสร้างระบบการบริหารจัดการข้อมูลที่ครอบคลุมทั้งด้านความปลอดภัย ความถูกต้อง และความเป็นส่วนตัวอย่างสมบูรณ์

1) วัตถุประสงค์

นโยบายการคุ้มครองข้อมูลส่วนบุคคลฉบับนี้มีวัตถุประสงค์เพื่อกำหนดกรอบการบริหารจัดการข้อมูลส่วนบุคคลของบริษัทให้เป็นไปตามหลักเกณฑ์ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) และมาตรฐานสากล ซึ่งมุ่งเน้นให้บริษัทดำเนินการเก็บรวบรวม ใช้ เปิดเผย และจัดเก็บข้อมูลส่วนบุคคลอย่างถูกต้อง โปร่งใส และมีความรับผิดชอบต่อผู้มีส่วนได้เสียทุกฝ่าย

รวมทั้งให้เกิดความสอดคล้องและเชื่อมโยงกับ นโยบายการรักษาความลับของข้อมูล (Confidentiality Policy) และ นโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy) บริษัทได้กำหนดวัตถุประสงค์หลักดังต่อไปนี้

- เพื่อให้การบริหารจัดการข้อมูลส่วนบุคคลเป็นไปตามกฎหมายและมาตรฐานสากล
- เพื่อสร้างระบบควบคุมและมาตรการป้องกันความเสี่ยงด้านข้อมูลส่วนบุคคลอย่างมีประสิทธิภาพ
- เพื่อกำหนดสิทธิและหน้าที่ของเจ้าของข้อมูลส่วนบุคคลอย่างชัดเจน
- เพื่อกำหนดบทบาทและความรับผิดชอบของบุคลากรทุกระดับในองค์กร
- เพื่อส่งเสริมวัฒนธรรมองค์กรด้านความปลอดภัยและความเป็นส่วนตัวของข้อมูล

2) ความสอดคล้องของนโยบายและมาตรฐานสากล

กำหนดความสอดคล้องกับกรอบการกำกับดูแลกิจการที่ดี *(Good Corporate Governance)* และมาตรฐานสากลด้านสิทธิมนุษยชน ความเป็นส่วนตัว และความมั่นคงของข้อมูล โดยมุ่งให้การบริหารจัดการข้อมูลส่วนบุคคลของบริษัทเป็นไปอย่างโปร่งใส ตรวจสอบได้ และเคารพในสิทธิของผู้มีส่วนได้เสียทุกกลุ่ม เพื่อสร้างความเชื่อมั่นและความไว้วางใจต่อองค์กรในระยะยาว บริษัทได้อ้างอิงกรอบแนวทางและมาตรฐานสำคัญ ดังนี้

- **มาตรฐาน GRI** *(Global Reporting Initiative)***:**
  - **GRI 418:** Customer Privacy – การบริหารจัดการข้อมูลส่วนบุคคลของลูกค้าและผู้มีส่วนได้เสีย การตอบสนองต่อเหตุการณ์ละเมิดข้อมูล (Data Breach) และการเปิดเผยผลการดำเนินงานด้านการคุ้มครองข้อมูลส่วนบุคคล
  - **GRI 102-43, 102-44:** การมีส่วนร่วมกับผู้มีส่วนได้เสีย และการรับฟังข้อร้องเรียนที่เกี่ยวข้องกับข้อมูลส่วนบุคคล
- **กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย** (Personal Data Protection Act B.E. 2562 – PDPA): กำหนดหลักเกณฑ์ในการเก็บรวบรวม ใช้ เปิดเผย และเก็บรักษาข้อมูลส่วนบุคคลอย่างถูกต้องตามกฎหมาย พร้อมระบุสิทธิของเจ้าของข้อมูลและบทลงโทษในกรณีที่มีการละเมิด
- **ISO/IEC 27701:** Privacy Information Management System (PIMS): มาตรฐานระบบการจัดการความเป็นส่วนตัวของข้อมูลที่ต่อยอดจาก ISO/IEC 27001 ด้านการรักษาความมั่นคงปลอดภัยของสารสนเทศ เพื่อสร้างระบบบริหารจัดการข้อมูลส่วนบุคคลอย่างมีประสิทธิภาพและตรวจสอบได้
- **OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**: แนวทางสากลในการคุ้มครองข้อมูลส่วนบุคคลและการส่งต่อข้อมูลข้ามพรมแดนอย่างปลอดภัย โปร่งใส และอยู่ภายใต้การกำกับดูแลที่เหมาะสม

- **UN Global Compact – Principle 1 และ Principle 10**: สนับสนุนสิทธิมนุษยชนขั้นพื้นฐาน รวมถึงการปกป้องความเป็นส่วนตัวของบุคคล และการดำเนินธุรกิจอย่างมีความรับผิดชอบและโปร่งใส
- **Securities and Exchange Commission (SEC) & SET Governance Code**: สนับสนุนให้บริษัทจดทะเบียนดำเนินการตามหลักธรรมาภิบาล โดยคำนึงถึงการบริหารจัดการข้อมูลสารสนเทศอย่างโปร่งใส ปลอดภัย และเป็นธรรมต่อผู้มีส่วนได้เสีย
- **เกณฑ์ ESG ของ FTSE Russell:**
  - **SHR07:** Social Pillar Data Privacy – กำหนดให้บริษัทมีนโยบายและกระบวนการบริหารจัดการข้อมูลส่วนบุคคลที่ชัดเจน ครอบคลุมการเก็บรวบรวม การใช้ การเข้าถึง การเก็บรักษา การลบ หรือการโอนข้อมูลอย่างปลอดภัย มีระบบร้องเรียนและตรวจสอบในกรณีเกิดเหตุละเมิดข้อมูล รวมถึงมี Data Protection Officer (DPO) กำกับดูแลการดำเนินงานตามกฎหมายและมาตรฐานที่เกี่ยวข้อง

  (สอดคล้องกับเกณฑ์ FTSE Russell SHR07, GRI 418, ISO/IEC 27701, PDPA พ.ศ. 2562, OECD Guidelines, UNGC Principles 1 & 10 และ SDGs 9, 12, 16, 17)

3) ขอบเขตของนโยบาย

นโยบายนี้ครอบคลุม:

- **พนักงานทุกระดับของบริษัท:** รวมถึงกรรมการ ผู้บริหาร พนักงานประจำ พนักงานสัญญาจ้าง พนักงานรายวัน และพนักงานฝึกหัดทุกกลุ่ม รวมทั้งบุคคลที่ปฏิบัติงานในนามของบริษัท เช่น ที่ปรึกษา หรือผู้รับจ้างภายนอกที่มีการเข้าถึงหรือจัดการข้อมูลส่วนบุคคลในกระบวนการทำงานของบริษัท
- **หน่วยงานและสถานประกอบการทั้งหมด:** ครอบคลุมโรงงาน สำนักงานใหญ่ ศูนย์กระจายสินค้า หน่วยงานสนับสนุน และหน่วยงานย่อยของบริษัททั้งในประเทศและต่างประเทศ รวมถึงระบบเทคโนโลยีสารสนเทศและคลาวด์ที่ใช้ในการจัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล
- **ผู้มีส่วนได้เสียทุกกลุ่มที่เกี่ยวข้องกับข้อมูลส่วนบุคคลของบริษัทโดยตรงและโดยอ้อม:** ได้แก่ ผู้ถือหุ้น พนักงาน ลูกค้า ผู้บริโภค ผู้สมัครงาน คู่ค้า ผู้จัดหา เจ้าหนี้ หน่วยงานภาครัฐ ชุมชน ผู้ติดต่อทางธุรกิจ และบุคคลภายนอกที่บริษัทมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
- **ทุกกิจกรรมของบริษัทที่เกี่ยวข้องกับการเก็บรวบรวม การใช้ การเปิดเผย การโอนย้าย หรือการจัดเก็บข้อมูลส่วนบุคคล:** ไม่ว่าจะอยู่ในรูปแบบเอกสาร ข้อมูลอิเล็กทรอนิกส์ หรือข้อมูลดิจิทัลผ่านระบบสารสนเทศ หรือช่องทางออนไลน์และออฟไลน์ทุกประเภท
- **การบริหารจัดการข้อมูลส่วนบุคคล การสื่อสาร และการตอบสนองต่อสิทธิของเจ้าของข้อมูล:** รวมถึงการจัดการเหตุการณ์ละเมิดข้อมูล (Data Breach Management) การร้องเรียน และการดำเนินการตามข้อกำหนดของกฎหมายคุ้มครองข้อมูลส่วนบุคคล

(สอดคล้องกับ GRI 418: Customer Privacy, FTSE Russell SHR07: Data Privacy, ISO/IEC 27701, PDPA พ.ศ. 2562 และ SDG 16 – Peace, Justice and Strong Institutions)

4) คำจำกัดความและเอกสารอ้างอิง

- **ข้อมูลส่วนบุคคล** *(Personal Data):* ข้อมูลใด ๆ ที่สามารถระบุตัวตนของบุคคลได้ ไม่ว่าทางตรงหรือทางอ้อม เช่น ชื่อ-นามสกุล หมายเลขบัตรประจำตัวประชาชน ที่อยู่ เบอร์โทรศัพท์ อีเมล ข้อมูลชีวมิติ (Biometric Data) หรือข้อมูลอื่นที่สามารถเชื่อมโยงกับตัวบุคคลได้
- **เจ้าของข้อมูลส่วนบุคคล** *(Data Subject):* บุคคลธรรมดาซึ่งเป็นเจ้าของข้อมูลส่วนบุคคลที่บริษัทเก็บรวบรวม ใช้ หรือเปิดเผย ไม่ว่าจะเป็นพนักงาน ลูกค้า ผู้สมัครงาน คู่ค้า หรือบุคคลอื่นใดที่เกี่ยวข้องกับการดำเนินงานของบริษัท
- **ผู้ควบคุมข้อมูลส่วนบุคคล** *(Data Controller)***:** บุคคลหรือนิติบุคคลที่มีอำนาจและหน้าที่ในการตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
- **ผู้ประมวลผลข้อมูลส่วนบุคคล** *(Data Processor):* บุคคลหรือนิติบุคคลที่ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล
- **การเก็บรวบรวมข้อมูล** *(Data Collection):* การได้รับข้อมูลส่วนบุคคลจากเจ้าของข้อมูลโดยตรง หรือจากแหล่งข้อมูลอื่นใด ทั้งในรูปแบบเอกสารหรืออิเล็กทรอนิกส์
- **การประมวลผลข้อมูล** *(Data Processing)*: การดำเนินการใด ๆ ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล เช่น การเก็บรวบรวม จัดเก็บ ใช้ โอน ย้าย วิเคราะห์ หรือทำลายข้อมูล
- **การโอนข้อมูลข้ามพรมแดน** *(Cross-Border Data Transfer)*: การส่งหรือเปิดเผยข้อมูลส่วนบุคคลไปยังต่างประเทศ หรือให้บุคคลภายนอกที่อยู่ต่างประเทศสามารถเข้าถึงข้อมูลนั้นได้
- **การละเมิดข้อมูลส่วนบุคคล** *(Data Breach)*: เหตุการณ์ที่ก่อให้เกิดการเข้าถึง ใช้ เปิดเผย หรือสูญหายของข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต ซึ่งอาจกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูล
- **เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล** *(Data Protection Officer: DPO)*: บุคลากรที่ได้รับมอบหมายจากบริษัทให้ทำหน้าที่กำกับดูแล ให้คำปรึกษา ตรวจสอบ และรายงานการดำเนินการที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลให้เป็นไปตามกฎหมายและนโยบายของบริษัท
- **การประเมินสาระสำคัญและความเสี่ยงแบบบูรณาการของวนชัย (Vanachai Integrated Materiality and Risk Assessment: V-IMRA):** กระบวนการประเมินภายในของบริษัทที่ใช้ในการระบุ ประเมิน และจัดลำดับความสำคัญของประเด็นด้านความยั่งยืน โดยบูรณาการทั้ง

มิติผลกระทบและมิติทางการเงิน ครอบคลุมตลอดห่วงโซ่คุณค่า เพื่อสนับสนุนการบริหารความเสี่ยงองค์กร การกำหนดกลยุทธ์ และการตัดสินใจของฝ่ายบริหาร
(สอดคล้องกับเกณฑ์ FTSE Russell SHR07, GRI 418, ISO/IEC 27701, PDPA พ.ศ. 2562, OECD Guidelines, และ SDG 16 – Peace, Justice and Strong Institutions)

5) การกำกับดูแลและความรับผิดชอบ

- **คณะกรรมการบริษัท:** ทำหน้าที่อนุมัติและกำกับดูแลนโยบายการคุ้มครองข้อมูลส่วนบุคคล รวมถึงกำหนดทิศทาง กลยุทธ์ และแนวทางการดำเนินงานด้านการบริหารจัดการข้อมูลส่วนบุคคลให้สอดคล้องกับกฎหมาย พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) และมาตรฐานสากล เพื่อให้มั่นใจว่าบริษัทดำเนินการเก็บรวบรวม ใช้ เปิดเผย และเก็บรักษาข้อมูลส่วนบุคคลอย่างถูกต้อง ปลอดภัย โปร่งใส และเคารพสิทธิของผู้มีส่วนได้เสียทุกกลุ่ม
- **คณะกรรมการตรวจสอบ**: ติดตาม ตรวจสอบ และประเมินผลการดำเนินงานตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล รวมถึงตรวจสอบความเพียงพอของมาตรการควบคุมภายในด้านการจัดการข้อมูลส่วนบุคคล และรายงานผลการดำเนินงานต่อคณะกรรมการบริษัท พร้อมข้อเสนอแนะเพื่อปรับปรุงและพัฒนากระบวนการบริหารจัดการข้อมูลให้มีประสิทธิภาพมากยิ่งขึ้น
- **คณะกรรมการบริหารความเสี่ยงและกำกับดูแลกิจการ**: กำกับดูแลให้การจัดการความเสี่ยงด้านข้อมูลส่วนบุคคลเป็นส่วนหนึ่งของระบบบริหารความเสี่ยงองค์กร (ERM) และติดตามผลการดำเนินงานด้านความปลอดภัยของข้อมูลและการป้องกันเหตุละเมิดข้อมูลส่วนบุคคล (Data Breach) เพื่อให้มั่นใจว่าบริษัทสามารถป้องกัน บรรเทา และตอบสนองต่อเหตุการณ์ที่อาจกระทบต่อข้อมูลส่วนบุคคลได้อย่างเหมาะสม
- **เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล** *(Data Protection Officer- DPO):* รับผิดชอบในการดำเนินมาตรการด้านความมั่นคงปลอดภัยของข้อมูล (Information Security) และการจัดการทางเทคนิค เพื่อป้องกันการเข้าถึง การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต รวมถึงดำเนินการสำรองข้อมูล การเข้ารหัสข้อมูล (Encryption) และการตรวจสอบระบบตามแผนงานด้านความปลอดภัยไซเบอร์ของบริษัท
- **หน่วยงานเทคโนโลยีสารสนเทศ:** รับผิดชอบในการดำเนินมาตรการด้านความมั่นคงปลอดภัยของข้อมูล (Information Security) และการจัดการทางเทคนิค เพื่อป้องกันการเข้าถึง การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต รวมถึงดำเนินการสำรองข้อมูล การเข้ารหัสข้อมูล (Encryption) และการตรวจสอบระบบตามแผนงานด้านความปลอดภัยไซเบอร์ของบริษัท
- **พนักงานทุกคน:** มีหน้าที่และความรับผิดชอบในการปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัด โดยต้อง:

- ศึกษาและทำความเข้าใจหลักการคุ้มครองข้อมูลส่วนบุคคล รวมถึงมาตรการรักษาความลับและความปลอดภัยของข้อมูลที่บริษัทกำหนด
- ปฏิบัติหน้าที่ด้วยความระมัดระวัง ไม่เปิดเผยหรือส่งต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต
- รายงานกรณีพบเห็นหรือสงสัยว่ามีการละเมิดข้อมูลส่วนบุคคลต่อหัวหน้างานหรือเจ้าหน้าที่ DPO โดยไม่ต้องกังวลต่อการถูกตอบโต้
- ร่วมมือกับหน่วยงานที่เกี่ยวข้องในการตรวจสอบและแก้ไขปัญหาอย่างโปร่งใส
- สนับสนุนวัฒนธรรมองค์กรที่ให้ความสำคัญกับความปลอดภัยและความเป็นส่วนตัวของข้อมูลในทุกระดับการทำงาน

(สอดคล้องกับเกณฑ์ FTSE Russell SHR07 – Data Privacy and Protection Oversight, GAC07 – Board Oversight and Ethical Governance, GRI 418: Customer Privacy, ISO/IEC 27701, และ SDG 16 – Peace, Justice and Strong Institutions)

6) พันธสัญญาและหลักการ

บริษัทมุ่งมั่นดำเนินธุรกิจภายใต้หลักธรรมาภิบาล โปร่งใส และรับผิดชอบต่อสังคม โดยยึดมั่นในหลักการเคารพสิทธิความเป็นส่วนตัวของบุคคล และการปกป้องข้อมูลส่วนบุคคลอย่างถูกต้องตามกฎหมายและมาตรฐานสากล เพื่อสร้างความเชื่อมั่นแก่ผู้มีส่วนได้เสียทุกฝ่าย บริษัทกำหนดพันธสัญญาและหลักการดำเนินงาน ดังต่อไปนี้

6.1 การปฏิบัติตามกฎหมายและมาตรฐานสากล (*FTSE Russell SHR07, GRI 418, PDPA พ.ศ. 2562, SDG 16.10*)

- บริษัทปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) และกฎหมาย ระเบียบ ข้อบังคับ รวมถึงหลักเกณฑ์ของหน่วยงานกำกับดูแลที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล ทั้งในระดับประเทศและระดับสากล
- บริษัทนำแนวทางและมาตรฐานสากลมาเป็นแนวปฏิบัติ เช่น FTSE Russell SHR07 – Data Privacy, GRI 418 – Customer Privacy, ISO/IEC 27701 – Privacy Information Management System (PIMS), OECD Privacy Guidelines, และ UN Global Compact Principle 1 เพื่อยกระดับการบริหารจัดการข้อมูลให้เทียบเท่ามาตรฐานสากล
- บริษัทส่งเสริมให้พนักงานและคู่ค้าทุกฝ่ายเข้าใจและปฏิบัติตามข้อกำหนดเหล่านี้อย่างเคร่งครัด โดยจัดให้มีการสื่อสารและอบรมความรู้ด้านการคุ้มครองข้อมูลส่วนบุคคลอย่างต่อเนื่อง

6.2 การปกป้องข้อมูลและลดความเสี่ยงจากการละเมิด *(FTSE Russell SHR07, ISO/IEC 27701, GRI 418-1, SDG 16.6)*

- บริษัทดำเนินการประเมินความเสี่ยงด้านข้อมูลส่วนบุคคลเป็นประจำทุกปี และบูรณาการผลการประเมินเข้าสู่ระบบบริหารความเสี่ยงองค์กร (Enterprise Risk Management – ERM) เพื่อระบุ ประเมิน และจัดการความเสี่ยงที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล
- บริษัทมีมาตรการควบคุมภายในที่รัดกุม เพื่อป้องกันการเข้าถึง การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต รวมถึงมีระบบบันทึกและตรวจสอบการเข้าถึงข้อมูล (Access Log) เพื่อให้สามารถติดตามและตรวจสอบได้อย่างโปร่งใส
- ในกรณีที่เกิดเหตุละเมิดข้อมูล (Data Breach) บริษัทจะดำเนินการแจ้งเหตุและจัดการตามขั้นตอนที่กำหนดภายในระยะเวลาที่กฎหมายกำหนด พร้อมรายงานต่อหน่วยงานกำกับดูแลและเจ้าของข้อมูลส่วนบุคคลโดยทันที เพื่อบรรเทาผลกระทบและป้องกันการเกิดซ้ำ

6.3 การเคารพสิทธิของเจ้าของข้อมูลส่วนบุคคล *(FTSE Russell SHR07, GRI 418-1, PDPA Section 30–35, SDG 16.7)*

- บริษัทเคารพสิทธิของเจ้าของข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด ได้แก่ สิทธิในการเข้าถึง แก้ไข ลบ ระงับการใช้ หรือเพิกถอนความยินยอมในการใช้ข้อมูลส่วนบุคคล
- บริษัทจัดให้มีช่องทางการติดต่อและกระบวนการรับคำร้องของเจ้าของข้อมูลอย่างชัดเจน โดยเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) เป็นผู้ประสานงานหลักในการตรวจสอบและตอบสนองคำร้องเหล่านั้น
- บริษัทส่งเสริมการดำเนินงานอย่างโปร่งใส โดยเปิดเผยนโยบายและประกาศความเป็นส่วนตัว (Privacy Notice) บนเว็บไซต์ www.vanachai.com เพื่อให้เจ้าของข้อมูลสามารถรับทราบวัตถุประสงค์ วิธีการ และสิทธิของตนได้อย่างชัดเจน

6.4 การเสริมสร้างวัฒนธรรมองค์กรด้านความปลอดภัยของข้อมูล *(FTSE Russell SHR07, ISO/IEC 27001, SDG 9.5):*

- บริษัทมุ่งสร้างวัฒนธรรมองค์กรที่ให้ความสำคัญกับความปลอดภัยของข้อมูล โดยจัดให้มีการฝึกอบรมพนักงานทุกระดับเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล การรักษาความลับ และการใช้เทคโนโลยีสารสนเทศอย่างปลอดภัย
- บริษัทกำหนดให้การรักษาความมั่นคงปลอดภัยของข้อมูลเป็นหนึ่งในตัวชี้วัดประสิทธิภาพการทำงาน (KPI) ของหน่วยงานที่เกี่ยวข้อง เพื่อให้มั่นใจว่าการปกป้องข้อมูลเป็นภารกิจร่วมของทุกคนในองค์กร

7) การบริหารความเสี่ยง ผลกระทบ และการพึ่งพา

ความเสี่ยง ผลกระทบ และการพึ่งพาที่เกี่ยวข้องกับประเด็นตามนโยบายฉบับนี้ ได้รับการระบุ วิเคราะห์ และจัดลำดับความสำคัญผ่านกระบวนการประเมินสาระสำคัญและความเสี่ยงแบบบูรณาการของบริษัท (Vanachai Integrated Materiality and Risk Assessment: V-IMRA) ซึ่ง

เป็นกรอบการประเมินภายในที่ครอบคลุมทั้งมิติผลกระทบ (Impact Materiality) และมิติทางการเงิน (Financial Materiality) ตลอดห่วงโซ่คุณค่า

- **ผลลัพธ์จาก V-IMRA** ถูกนำไปบูรณาการเข้าสู่ระบบบริหารความเสี่ยงองค์กร (Enterprise Risk Management: ERM) เพื่อสนับสนุนการกำหนดนโยบาย การตัดสินใจเชิงกลยุทธ์ การกำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และการสร้างคุณค่าอย่างยั่งยืนในระยะยาว
- **การระบุและประเมินความเสี่ยง (Risk Identification and Assessment):** ดำเนินการระบุและประเมินความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคลอย่างเป็นระบบ ครอบคลุมทุกกระบวนการที่เกี่ยวข้องกับการเก็บรวบรวม การใช้ การเปิดเผย การโอนย้าย และการจัดเก็บข้อมูลส่วนบุคคล ทั้งในรูปแบบเอกสารและระบบดิจิทัล โดยเฉพาะในขั้นตอนที่มีความอ่อนไหว เช่น การจัดการข้อมูลลูกค้า พนักงาน คู่ค้า และผู้สมัครงาน เพื่อระบุโอกาสในการเกิดเหตุละเมิดข้อมูล (Data Breach) หรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
  โดยบริษัทประเมินระดับความเสี่ยง (Risk Level) ตามความร้ายแรงของผลกระทบและความถี่ในการเกิด เพื่อจัดลำดับความสำคัญและกำหนดมาตรการควบคุมป้องกันที่เหมาะสม โดยบูรณาการเข้ากับระบบบริหารความเสี่ยงองค์กร (Enterprise Risk Management – ERM) เพื่อให้สามารถติดตามและบริหารความเสี่ยงได้อย่างต่อเนื่อง
- **การประเมินผลกระทบ (Impact Assessment):** บริษัทดำเนินการประเมินผลกระทบที่อาจเกิดขึ้นจากการละเมิดข้อมูลส่วนบุคคล หรือการจัดการข้อมูลที่ไม่เป็นไปตามกฎหมายในมิติต่าง ๆ ได้แก่
  - **ด้านกฎหมายและการเงิน:** ความเสียหายจากการถูกฟ้องร้อง ค่าปรับ หรือการชดใช้ค่าเสียหายอันเกิดจากการละเมิดข้อมูลส่วนบุคคล
  - **ด้านชื่อเสียงและความเชื่อมั่น:** การสูญเสียความไว้วางใจจากลูกค้า ผู้ถือหุ้น คู่ค้า และหน่วยงานกำกับดูแล ซึ่งอาจส่งผลกระทบต่อภาพลักษณ์ขององค์กรในระยะยาว
  - **ด้านการดำเนินงาน:** การหยุดชะงักของระบบเทคโนโลยีสารสนเทศ การสูญหายของข้อมูลสำคัญ หรือการขัดข้องของระบบที่ส่งผลกระทบต่อประสิทธิภาพทางธุรกิจ
  - **ด้านสังคมและผู้มีส่วนได้เสีย:** การละเมิดสิทธิในความเป็นส่วนตัวของบุคคลที่อาจสร้างผลกระทบทางจิตใจหรือสังคม รวมถึงการบั่นทอนความเชื่อมั่นต่อการดำเนินธุรกิจอย่างรับผิดชอบของบริษัท

  ผลการประเมินเหล่านี้จะถูกนำมาใช้เพื่อปรับปรุงระบบควบคุมภายใน มาตรการป้องกัน และแผนตอบสนองต่อเหตุการณ์ด้านข้อมูลส่วนบุคคล เพื่อให้มั่นใจว่าบริษัทสามารถบริหารความเสี่ยงได้อย่างมีประสิทธิภาพและโปร่งใส
- **การพึ่งพาและความเชื่อมโยงกับระบบอื่น** (Dependency Management): บริษัทตระหนักว่าการบริหารจัดการข้อมูลส่วนบุคคลมีความเกี่ยวข้องกับระบบการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy) และนโยบายการรักษาความลับของข้อมูล

(Confidentiality Policy) โดยตรง จึงได้บูรณาการนโยบายทั้งหมดให้เชื่อมโยงกัน เพื่อสร้างระบบการป้องกันแบบครบวงจร ตั้งแต่การออกแบบระบบเทคโนโลยี การควบคุมการเข้าถึงข้อมูล ไปจนถึงการทำลายข้อมูลเมื่อสิ้นสุดวัตถุประสงค์ของการใช้งาน
นอกจากนี้ บริษัทยังพึ่งพาความร่วมมือจากคู่ค้าและพันธมิตรทางธุรกิจในการบริหารความเสี่ยงด้านข้อมูล โดยกำหนดให้คู่ค้าทุกรายปฏิบัติตามมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลและมีระบบความปลอดภัยของข้อมูลที่เทียบเท่ากับบริษัท
(สอดคล้องกับเกณฑ์ FTSE Russell SHR07 – Data Privacy and Protection, GAC07 – Governance Oversight, GRI 418-1, ISO/IEC 27701, และ SDG 16 – Peace, Justice and Strong Institutions)

8) เป้าหมายและตัวชี้วัด

กำหนดเป้าหมายและตัวชี้วัดหลัก (Key Performance Indicators: KPIs) เพื่อใช้ติดตามและประเมินผลการดำเนินงานด้านการคุ้มครองข้อมูลส่วนบุคคลให้มีความต่อเนื่อง โปร่งใส และตรวจสอบได้ โดยเน้นทั้งมิติของการ ป้องกัน (Prevention) การ ตรวจพบ (Detection) และการ ตอบสนองต่อเหตุการณ์ (Response) เพื่อให้มั่นใจว่าข้อมูลส่วนบุคคลของผู้มีส่วนได้เสียทุกกลุ่มได้รับการคุ้มครองอย่างเหมาะสมและปลอดภัย

เป้าหมายระยะสั้น *(Short-Term Goals – ภายใน 1 ปี)*

- พนักงาน 100% ผ่านการอบรมเรื่องการคุ้มครองข้อมูลส่วนบุคคล (PDPA Awareness Training) และการรักษาความปลอดภัยทางไซเบอร์อย่างน้อยปีละหนึ่งครั้ง
- ทุกหน่วยงานต้องดำเนินการประเมินความเสี่ยงด้านข้อมูลส่วนบุคคลประจำปี และจัดทำแผนบริหารความเสี่ยง (Personal Data Risk Management Plan)
- มีการแต่งตั้งและประกาศรายชื่อ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer – DPO) อย่างเป็นทางการ พร้อมระบุบทบาทและความรับผิดชอบที่ชัดเจน
- จัดให้มีช่องทางการร้องเรียนและรายงานเหตุละเมิดข้อมูลส่วนบุคคลที่เข้าถึงง่าย ปลอดภัย และคุ้มครองข้อมูลของผู้ร้องเรียน

เป้าหมายระยะกลาง *(Medium-term Targets: 3–5 ปี)*

- พัฒนาและรับรองระบบบริหารจัดการข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐาน ISO/IEC 27701: Privacy Information Management System (PIMS)
- ดำเนินการตรวจประเมิน (Audit) การจัดการข้อมูลส่วนบุคคลภายในองค์กรอย่างน้อยปีละหนึ่งครั้ง เพื่อให้มั่นใจว่ามีการปฏิบัติตามกฎหมาย PDPA และมาตรการภายใน
- คู่ค้าและพันธมิตรทางธุรกิจ 100% ต้องผ่านการรับรองการปฏิบัติตามข้อกำหนดด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Privacy Compliance Assessment)

- ยกระดับการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ (IT Security System) โดยลดอัตราการเกิดเหตุผิดปกติ (Incident Rate) อย่างน้อย 30% ภายใน 3 ปี

เป้าหมายระยะยาว *(Long-term Targets: 5 ปีขึ้นไป)*

- ไม่มีเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่ได้รับการยืนยันว่าเกิดขึ้นภายในองค์กร ("Zero Confirmed Data Breach Cases")
- บริษัทได้รับการยอมรับในระดับอุตสาหกรรมว่าเป็นองค์กรที่มีระบบบริหารจัดการข้อมูลส่วนบุคคลที่เข้มแข็งและโปร่งใส (Data Privacy Excellence Organization)
- สร้างวัฒนธรรมองค์กรที่ให้ความสำคัญกับความปลอดภัยของข้อมูลและสิทธิในความเป็นส่วนตัวให้เป็นส่วนหนึ่งของค่านิยมหลักของบริษัท (Core Values Integration)

ตัวชี้วัดหลัก (Key Performance Indicators – KPIs)

หมวด	**ตัวชี้วัด** (Indicators)	**ความถี่ในการติดตาม**	**หน่วยงานรับผิดชอบ**
การป้องกัน (Prevention)	ร้อยละของพนักงานที่ผ่านการอบรมด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA & Cybersecurity Training)	รายปี	ฝ่ายทรัพยากรบุคคล / ฝ่ายเทคโนโลยีสารสนเทศ
การตรวจพบ (Detection)	จำนวนเหตุการณ์การละเมิดข้อมูล (Data Breach Incidents) ที่ได้รับการตรวจพบและรายงานต่อ DPO	รายไตรมาส	เจ้าหน้าที่ DPO / ฝ่าย IT Security
การตอบสนอง (Response)	ระยะเวลาเฉลี่ยในการดำเนินการตอบสนองและแจ้งเหตุละเมิดข้อมูลต่อเจ้าของข้อมูลและหน่วยงานกำกับดูแล (Incident Response Time	รายปี	เจ้าหน้าที่ DPO / คณะกรรมการบริหารความเสี่ยง
การปฏิบัติตาม (Compliance Monitoring)	ร้อยละของหน่วยงานที่ผ่านการตรวจประเมินการปฏิบัติตาม PDPA และนโยบายคุ้มครองข้อมูลส่วนบุคคล	รายปี	ฝ่ายตรวจสอบภายใน / ฝ่ายกฎหมาย
การมีส่วนร่วมของคู่ค้า (Partner Engagement)	ร้อยละของคู่ค้าที่ผ่านการประเมินด้าน Data Privacy Compliance	รายปี	ฝ่ายจัดซื้อ / ฝ่ายพัฒนาองค์กร
ความโปร่งใสในการเปิดเผยข้อมูล (Disclosure Transparency)	การเปิดเผยข้อมูลด้านการคุ้มครองข้อมูลส่วนบุคคลในรายงานความยั่งยืน (Sustainability Report – GRI 418)	รายปี	คณะกรรมการความยั่งยืน / คณะทำงานด้านการพัฒนาเพื่อความยั่งยืน

การเชื่อมโยงกับการประเมินผลผู้บริหารและองค์กร (Performance Integration)

- การเชื่อมโยงกับการประเมินผลผู้บริหารและองค์กร (Performance Integration)
- ตัวชี้วัดด้านการคุ้มครองข้อมูลส่วนบุคคลจะถูกรวมเข้ากับ ตัวชี้วัดผลการปฏิบัติงานของผู้บริหารระดับสูง (Executive KPIs) และการประเมินผลการดำเนินงานขององค์กร เพื่อสร้างความรับผิดชอบร่วมกันในการบริหารจัดการข้อมูลส่วนบุคคลอย่างโปร่งใส มีประสิทธิภาพ และสอดคล้องกับกลยุทธ์ด้านความยั่งยืนของบริษัท

(สอดคล้องกับเกณฑ์ FTSE Russell SHR07 – Data Privacy and Protection, GRI 418 – Customer Privacy, ISO/IEC 27701, PDPA พ.ศ. 2562, และ SDG 16.10 – Access to Information)

9) ห่วงโซ่อุปทาน และความรับผิดชอบของพันธมิตร

- **การคัดเลือกและประเมินคู่ค้า** *(FTSE Russell SHR07, GRI 418-1, ISO/IEC 27701, SDG 16.6)*: บริษัทดำเนินการคัดเลือกและประเมินคู่ค้าทางธุรกิจที่เกี่ยวข้องกับการจัดเก็บประมวลผล หรือเข้าถึงข้อมูลส่วนบุคคล โดยใช้หลักเกณฑ์ด้านจริยธรรม ความปลอดภัย และความสอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นปัจจัยสำคัญในการพิจารณา โดยเฉพาะผู้ให้บริการระบบเทคโนโลยีสารสนเทศ ผู้ให้บริการคลาวด์ และหน่วยงานภายนอกที่มีการเข้าถึงข้อมูลส่วนบุคคล โดยก่อนการว่าจ้างบริษัทจะดำเนินการตรวจสอบสถานะ (Due Diligence) ของคู่ค้าในด้าน Data Privacy Compliance และกำหนดให้ลงนามใน ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement – DPA) เพื่อยืนยันความรับผิดชอบและมาตรการปกป้องข้อมูลที่ชัดเจน
- **การปฏิบัติตามจรรยาบรรณคู่ค้า** *(FTSE Russell SHR07, GRI 102-16, SDG 8.7 และ SDG 12.6)*: บริษัทกำหนดให้คู่ค้าทุกฝ่ายต้องปฏิบัติตาม จรรยาบรรณคู่ค้า (Supplier Code of Conduct) และ นโยบายการคุ้มครองข้อมูลส่วนบุคคล ของบริษัท ซึ่งครอบคลุมหลักการสำคัญ ได้แก่
  - การปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลและมาตรฐานความปลอดภัยของข้อมูล
  - การเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลเฉพาะเท่าที่จำเป็นและตามวัตถุประสงค์ที่ได้รับความยินยอมจากเจ้าของข้อมูล
  - การใช้มาตรการด้านเทคโนโลยี เช่น การเข้ารหัส (Encryption) การควบคุมสิทธิ์การเข้าถึง (Access Control) และการตรวจสอบการใช้งาน (Audit Trail)
  - การแจ้งให้บริษัททราบทันทีเมื่อเกิดเหตุละเมิดข้อมูลส่วนบุคคล เพื่อให้สามารถดำเนินการตามขั้นตอนตอบสนองเหตุการณ์ได้อย่างทันท่วงที

  บริษัทมีสิทธิ์ในการตรวจสอบ (Audit) หรือขอข้อมูลจากคู่ค้าเพื่อยืนยันการปฏิบัติตามข้อกำหนด หากพบว่ามีการละเมิดหรือไม่ปฏิบัติตามมาตรฐาน บริษัทอาจระงับการให้บริการหรือยุติความสัมพันธ์ทางธุรกิจโดยทันที

- **การฝึกอบรมและการเสริมสร้างศักยภาพ** *(FTSE Russell SHR07, GRI 205-2, SDG 17 – Partnerships for the Goals):* บริษัทส่งเสริมให้คู่ค้าและพันธมิตรทางธุรกิจมีความรู้และความเข้าใจเกี่ยวกับแนวทางการคุ้มครองข้อมูลส่วนบุคคล ผ่านการอบรม การสื่อสารข้อมูลข่าวสาร หรือการจัดประชุมแลกเปลี่ยนความรู้ เพื่อให้คู่ค้ามีความพร้อมในการจัดการข้อมูลอย่างปลอดภัยตามมาตรฐานเดียวกับบริษัท รวมถึงสนับสนุนการนำเทคโนโลยีใหม่ ๆ มาใช้เพื่อเพิ่มประสิทธิภาพในการรักษาความปลอดภัยของข้อมูลในห่วงโซ่อุปทาน
- **การตรวจสอบและการติดตามผล** *(TSE Russell SHR07, GRI 418-1, SDG 16.10)***:** บริษัทดำเนินการตรวจสอบและติดตามผลการปฏิบัติตามข้อกำหนดด้านการคุ้มครองข้อมูลส่วนบุคคลของคู่ค้าอย่างต่อเนื่อง โดยอาจดำเนินการตรวจเยี่ยมสถานประกอบการ (On-site Audit) การประเมินเอกสาร หรือการตรวจสอบระบบเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจว่ามีการปฏิบัติตามมาตรการปกป้องข้อมูลที่กำหนด ผลการตรวจสอบจะถูกรายงานต่อคณะกรรมการบริหารความเสี่ยงและคณะกรรมการตรวจสอบ เพื่อพิจารณาแนวทางปรับปรุงและพัฒนา
- **การส่งเสริมเครือข่ายธุรกิจที่มีความรับผิดชอบ** *(FTSE Russell SHR07, GRI 102-43, SDG 17 – Partnerships for the Goals):* บริษัทมุ่งสร้างเครือข่ายพันธมิตรทางธุรกิจที่ให้ความสำคัญกับความปลอดภัยของข้อมูลและการเคารพสิทธิในความเป็นส่วนตัว โดยสนับสนุนให้คู่ค้าและพันธมิตรทางธุรกิจเข้าร่วมประกาศเจตนารมณ์ (Privacy and Data Ethics Commitment) เพื่อยกระดับมาตรฐานความโปร่งใสของอุตสาหกรรม และร่วมมือกับหน่วยงานภาครัฐ สมาคมการค้า และองค์กรสากลในการแลกเปลี่ยนแนวปฏิบัติที่ดี (Best Practices) ด้านการคุ้มครองข้อมูลส่วนบุคคล

10) การบูรณาการกับกลยุทธ์องค์กร

บริษัทได้บูรณาการนโยบายการคุ้มครองข้อมูลส่วนบุคคลเข้ากับกลยุทธ์การดำเนินงานขององค์กร ภายใต้กรอบ “Forest | Future | Together – for a Sustainable Living” ซึ่งเป็นวิสัยทัศน์หลักของบริษัทในการสร้างสมดุลระหว่างการเติบโตทางธุรกิจ ความรับผิดชอบต่อสิ่งแวดล้อม และการเคารพสิทธิมนุษยชนของผู้มีส่วนได้เสียทุกกลุ่ม โดยนโยบายนี้ถือเป็นกลไกสำคัญในการเสริมสร้างความเชื่อมั่น ความโปร่งใส และธรรมาภิบาลในยุคดิจิทัล

- **FOREST – ธรรมาภิบาลและความรับผิดชอบต่อสิ่งแวดล้อม:** บริษัทดำเนินการบริหารจัดการข้อมูลส่วนบุคคลโดยยึดหลักความโปร่งใส ความปลอดภัย และความรับผิดชอบเช่นเดียวกับแนวทางการใช้ทรัพยากรอย่างยั่งยืนในห่วงโซ่อุปทาน โดยเน้นการลดผลกระทบจากการใช้เทคโนโลยีและระบบสารสนเทศที่เกี่ยวข้องกับข้อมูลส่วนบุคคล เพื่อให้มั่นใจว่าการดำเนินธุรกิจด้านดิจิทัลและข้อมูลสอดคล้องกับแนวทางการบริหารสิ่งแวดล้อมและธรรมาภิบาลขององค์กร

- **FUTURE – นวัตกรรมและการพัฒนาระบบบริหารจัดการข้อมูลอย่างยั่งยืน**: บริษัทพัฒนาระบบบริหารจัดการข้อมูลส่วนบุคคลให้สอดคล้องกับเทคโนโลยีสมัยใหม่ เช่น ระบบคลาวด์ (Cloud System) การเข้ารหัสข้อมูล (Data Encryption) และการใช้ AI เพื่อช่วยตรวจสอบความปลอดภัยของข้อมูล ทั้งนี้เพื่อเสริมสร้างประสิทธิภาพในการบริหารข้อมูล ลดความเสี่ยงจากภัยไซเบอร์ และตอบสนองต่อกฎหมายและมาตรฐานสากลที่เกี่ยวข้อง เช่น PDPA พ.ศ. 2562, ISO/IEC 27701, และ FTSE Russell SHR07
  นอกจากนี้ บริษัทยังส่งเสริมการสร้างนวัตกรรมด้าน "Data Ethics" เพื่อให้พนักงานและพันธมิตรมีความเข้าใจในการใช้ข้อมูลอย่างมีจริยธรรม เคารพสิทธิในความเป็นส่วนตัว และใช้ข้อมูลเพื่อประโยชน์ทางธุรกิจอย่างโปร่งใส
- **TOGETHER-ความร่วมมือกับผู้มีส่วนได้เสียเพื่อยกระดับมาตรฐานข้อมูลส่วนบุคคล**: บริษัทให้ความสำคัญกับความร่วมมือระหว่างพนักงาน คู่ค้า ลูกค้า หน่วยงานภาครัฐและชุมชน โดยร่วมกันพัฒนากลไกการบริหารจัดการข้อมูลส่วนบุคคลที่มีความปลอดภัย ครอบคลุม และตรวจสอบได้
  บริษัทจัดให้มีการอบรม การสื่อสาร และกิจกรรมสร้างความตระหนักรู้ด้านการคุ้มครองข้อมูลส่วนบุคคลอย่างต่อเนื่อง เพื่อให้ผู้มีส่วนได้เสียทุกกลุ่มมีส่วนร่วมในการส่งเสริมวัฒนธรรมองค์กรด้าน "Data Privacy and Cybersecurity Responsibility" ร่วมกันขับเคลื่อนให้การใช้ข้อมูลในห่วงโซ่อุปทานเป็นไปอย่างมีจริยธรรม โปร่งใส และรับผิดชอบ

นโยบายการคุ้มครองข้อมูลส่วนบุคคลนี้ยังได้รับการบูรณาการเข้ากับ

- **กลยุทธ์ด้านความยั่งยืนขององค์กร** (Corporate Sustainability Strategy): เพื่อให้แน่ใจว่าการบริหารจัดการข้อมูลสอดคล้องกับเป้าหมายด้านธรรมาภิบาล (Governance) และความรับผิดชอบต่อสังคม (Social Responsibility)
- ระบบบริหารความเสี่ยงองค์กร (Enterprise Risk Management – ERM): โดยบูรณาการการบริหารความเสี่ยงด้านข้อมูลส่วนบุคคลเข้ากับการบริหารความเสี่ยงด้านเทคโนโลยีและไซเบอร์ เพื่อให้สามารถติดตาม ตรวจสอบ และตอบสนองได้อย่างมีประสิทธิภาพ
- การประเมินผลด้าน ESG: บริษัทนำผลการดำเนินงานด้านการคุ้มครองข้อมูลส่วนบุคคลมาเป็นส่วนหนึ่งของตัวชี้วัดด้านธรรมาภิบาล (G – Governance) ภายใต้กรอบการประเมินของ FTSE Russell และ GRI Standards เพื่อแสดงถึงความมุ่งมั่นในการดำเนินธุรกิจอย่างโปร่งใสและเคารพสิทธิมนุษยชนในยุคดิจิทัล

(สอดคล้องกับ FTSE Russell SHR07 – Data Privacy, GRI 418 – Customer Privacy, ISO/IEC 27701, PDPA พ.ศ. 2562, UNGC Principle 1, และ SDG 9, SDG 16, SDG 17)

11) การดำเนินงานและเครื่องมือ

- **ระบบบริหารจัดการข้อมูลส่วนบุคคล** *(Data Privacy Management System – DPMS)*: บริษัทได้จัดตั้งระบบบริหารจัดการข้อมูลส่วนบุคคล เพื่อใช้เป็นกรอบในการดำเนินงานตามหลัก PDPA พ.ศ. 2562 และมาตรฐาน ISO/IEC 27701 โดยระบบนี้ครอบคลุมการดำเนินการตั้งแต่การเก็บรวบรวม การใช้ การเปิดเผย การโอนย้าย และการทำลายข้อมูลส่วนบุคคล พร้อมกำหนดขั้นตอนการควบคุมสิทธิ์การเข้าถึง (Access Control) การตรวจสอบ (Audit Trail) และการอนุมัติ (Authorization) เพื่อให้สามารถตรวจสอบย้อนกลับได้ทุกขั้นตอน
- **การบริหารจัดการความยินยอม** (Consent Management System): บริษัทพัฒนาและใช้ระบบจัดการความยินยอมของเจ้าของข้อมูลส่วนบุคคล เพื่อให้มั่นใจว่าทุกการเก็บรวบรวมและการใช้ข้อมูลได้รับความยินยอมอย่างชัดเจน โปร่งใส และตรวจสอบได้ โดยระบบดังกล่าวจะบันทึกหลักฐานการให้ความยินยอม (Consent Record) และเปิดโอกาสให้เจ้าของข้อมูลสามารถถอนความยินยอมได้ทุกเมื่อผ่านช่องทางที่กำหนด
- **การรักษาความมั่นคงปลอดภัยของข้อมูล** (Information Security Tools): บริษัทดำเนินการควบคุมและคุ้มครองข้อมูลส่วนบุคคลผ่านระบบความปลอดภัยของเทคโนโลยีสารสนเทศตามมาตรฐาน ISO/IEC 27001 – Information Security Management System (ISMS) โดยใช้เครื่องมือหลัก เช่น
  - ระบบเข้ารหัสข้อมูล (Data Encryption): เพื่อป้องกันการเข้าถึงและการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต
  - ระบบตรวจจับและป้องกันการบุกรุก (Intrusion Detection & Prevention System – IDPS): เพื่อเฝ้าระวังและป้องกันภัยคุกคามทางไซเบอร์
  - ระบบสำรองและกู้คืนข้อมูล (Backup and Recovery System): เพื่อให้มั่นใจว่าสามารถกู้คืนข้อมูลได้ในกรณีเกิดเหตุไม่คาดคิด
  - ระบบจัดการสิทธิ์ผู้ใช้งาน (Identity & Access Management – IAM): เพื่อควบคุมการเข้าถึงข้อมูลตามระดับสิทธิ์และบทบาทหน้าที่ของพนักงาน
- **แผนรับมือเหตุละเมิดข้อมูลส่วนบุคคล** (Data Breach Response Plan): บริษัทได้จัดทำแผนตอบสนองต่อเหตุละเมิดข้อมูล (Data Breach Response Plan) เพื่อให้สามารถจัดการเหตุการณ์ได้อย่างรวดเร็วและมีประสิทธิภาพ โดยครอบคลุมขั้นตอนสำคัญ ได้แก่
  - การตรวจพบและประเมินเหตุการณ์เบื้องต้น
  - การควบคุมและจำกัดขอบเขตความเสียหาย
  - การรายงานต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) และหน่วยงานกำกับดูแลภายในระยะเวลาที่กฎหมายกำหนด
  - การแจ้งเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ
  - การวิเคราะห์สาเหตุและจัดทำรายงานสรุปเพื่อป้องกันการเกิดซ้ำ

- **การอบรมและพัฒนาศักยภาพบุคลากร** (Training and Awareness Program)**:** บริษัทจัดให้มีการอบรมและสื่อสารความรู้ให้แก่พนักงานทุกระดับเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและความปลอดภัยของข้อมูลอย่างต่อเนื่อง ทั้งในรูปแบบการอบรมภายใน (In-house Training) การอบรมออนไลน์ (E-Learning) และการประชุมเชิงปฏิบัติการ (Workshop) เพื่อเสริมสร้างความตระหนักรู้ ความเข้าใจในบทบาทหน้าที่ และการปฏิบัติตามนโยบายนี้อย่างถูกต้อง
- **เครื่องมือสนับสนุนการกำกับดูแลและ**ตรวจสอบ (Monitoring & Audit Tools): บริษัทพัฒนาเครื่องมือและระบบติดตามผลการดำเนินงานด้านข้อมูลส่วนบุคคล เช่น Privacy Dashboard และ Compliance Monitoring System เพื่อให้หน่วยงานที่เกี่ยวข้องสามารถติดตามสถานะการปฏิบัติตามนโยบาย วิเคราะห์แนวโน้มความเสี่ยง และรายงานผลต่อคณะกรรมการบริหารความเสี่ยงและคณะกรรมการตรวจสอบเป็นระยะ
- **การประสานงานกับคู่ค้าและพันธมิตร** (Partner Coordination Mechanism): บริษัทจัดให้มีช่องทางการประสานงานกับคู่ค้าและพันธมิตรทางธุรกิจที่มีการประมวลผลข้อมูลส่วนบุคคลเพื่อแลกเปลี่ยนข้อมูลด้านความปลอดภัย การแจ้งเตือนเหตุการณ์ผิดปกติ และแนวทางป้องกันการละเมิดข้อมูล โดยกำหนดให้การจัดทำหรือว่าจ้างบริการที่เกี่ยวข้องกับข้อมูลส่วนบุคคลต้องได้รับการตรวจสอบจาก DPO และฝ่ายกฎหมายก่อนทุกครั้ง

(สอดคล้องกับเกณฑ์ FTSE Russell SHR07 – Data Privacy, GRI 418 – Customer Privacy, ISO/IEC 27701, ISO/IEC 27001, และ SDG 9, SDG 16 – Peace, Justice and Strong Institutions)

12) การติดตาม รายงาน และความโปร่งใส

- **การติดตามผลการดำเนินงาน** *(Monitoring)*:
  - บริษัทดำเนินการติดตามผลการปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลในทุกหน่วยงาน ผ่านกระบวนการตรวจสอบภายใน (Internal Audit) และการประเมินความสอดคล้อง (Compliance Review) อย่างน้อยปีละหนึ่งครั้ง เพื่อประเมินความพร้อม ความเสี่ยง และประสิทธิผลของมาตรการที่มีอยู่
  - เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer – DPO) รับผิดชอบในการตรวจสอบ ติดตาม และรายงานสถานะการดำเนินงานด้านข้อมูลส่วนบุคคลต่อคณะกรรมการบริหารความเสี่ยงและคณะกรรมการตรวจสอบ
  - บริษัทใช้เครื่องมือดิจิทัล เช่น Privacy Dashboard และ Incident Reporting System เพื่อเฝ้าระวัง ตรวจสอบ และเก็บบันทึกเหตุการณ์การเข้าถึงหรือการละเมิดข้อมูลส่วนบุคคลอย่างโปร่งใสและเป็นระบบ

- **การรายงานผลการดำเนินงาน** *(Reporting)*:
  - บริษัทกำหนดให้มีการจัดทำรายงานผลการดำเนินงานด้านการคุ้มครองข้อมูลส่วนบุคคลเป็นประจำทุกปี โดยรวมอยู่ในรายงานความยั่งยืน (Sustainability Report) ภายใต้มาตรฐาน GRI 418 – Customer Privacy และกรอบการประเมินของ FTSE Russell SHR07 – Data Privacy
  - ในกรณีที่เกิดเหตุละเมิดข้อมูลส่วนบุคคล (Data Breach) บริษัทจะรายงานต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (PDPC) และเจ้าของข้อมูลส่วนบุคคลภายในระยะเวลาที่กฎหมายกำหนด พร้อมเปิดเผยแนวทางแก้ไขและมาตรการป้องกันการเกิดซ้ำอย่างโปร่งใส
  - ผลการดำเนินงานด้านข้อมูลส่วนบุคคลและความมั่นคงทางไซเบอร์จะถูกรายงานต่อคณะกรรมการตรวจสอบ และนำเสนอต่อคณะกรรมการบริษัทอย่างน้อยปีละหนึ่งครั้ง เพื่อประกอบการตัดสินใจเชิงนโยบายและกำหนดทิศทางการพัฒนาในอนาคต
- **ความโปร่งใสและการสื่อสารต่อผู้มีส่วนได้เสีย** *(Transparency and Disclosure)*:
  - บริษัทมุ่งดำเนินการด้วยความโปร่งใส โดยเปิดเผยนโยบายและแนวทางการคุ้มครองข้อมูลส่วนบุคคล รวมถึง "ประกาศความเป็นส่วนตัว (Privacy Notice)" ผ่านเว็บไซต์ทางการของบริษัท www.vanachai.com เพื่อให้ผู้มีส่วนได้เสียสามารถเข้าถึงและทำความเข้าใจได้อย่างชัดเจน
  - บริษัทจัดให้มีช่องทางการร้องเรียน การสอบถาม และการขอใช้สิทธิของเจ้าของข้อมูลผ่านระบบออนไลน์และหน่วยงานที่เกี่ยวข้อง โดยทุกข้อร้องเรียนจะได้รับการตรวจสอบและดำเนินการอย่างเป็นธรรม ภายใต้การกำกับดูแลของเจ้าหน้าที่ DPO
  - บริษัทให้คำมั่นว่าจะไม่ปกปิดข้อมูลที่เกี่ยวข้องกับการละเมิดข้อมูลส่วนบุคคล และจะเปิดเผยข้อเท็จจริงอย่างตรงไปตรงมา พร้อมดำเนินการแก้ไขอย่างรับผิดชอบ เพื่อรักษาความเชื่อมั่นของผู้ถือหุ้น ลูกค้า คู่ค้า พนักงาน และชุมชน
- **การประเมินผลและการปรับปรุงอย่างต่อเนื่อง** *(Continuous Improvement and Review)*:
  - ผลจากการติดตามและการรายงานจะถูกนำมาวิเคราะห์เพื่อปรับปรุงกระบวนการบริหารจัดการข้อมูลส่วนบุคคลให้ดียิ่งขึ้น โดยเน้นการเรียนรู้จากเหตุการณ์จริงและการพัฒนาเทคโนโลยีใหม่ ๆ
  - บริษัทจัดให้มีการทบทวนประสิทธิผลของระบบคุ้มครองข้อมูลส่วนบุคคลอย่างน้อยปีละหนึ่งครั้ง เพื่อให้สอดคล้องกับการเปลี่ยนแปลงของกฎหมาย ความเสี่ยง และแนวโน้มด้านความปลอดภัยทางไซเบอร์

(สอดคล้องกับเกณฑ์ FTSE Russell SHR07 – Data Privacy and Protection, GRI 418 – Customer Privacy, ISO/IEC 27701, PDPA พ.ศ. 2562, และ SDG 16 – Peace, Justice and Strong Institutions)

13) การทบทวนและพัฒนาอย่างต่อเนื่อง

- **การทบทวนตามรอบระยะเวลา** *(Periodic Review)*:
  - บริษัทกำหนดให้มีการทบทวนนโยบายการคุ้มครองข้อมูลส่วนบุคคลอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงของกฎหมาย ข้อบังคับ หรือมาตรฐานที่เกี่ยวข้อง เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) มาตรฐาน ISO/IEC 27701 หรือเกณฑ์ FTSE Russell SHR07
  - การทบทวนจะดำเนินการโดย เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) ร่วมกับ คณะกรรมการบริหารความเสี่ยงและกำกับดูแลกิจการ เพื่อประเมินความเหมาะสมและประสิทธิผลของนโยบาย รวมถึงเสนอแนวทางปรับปรุงต่อคณะกรรมการบริษัทเพื่ออนุมัติ
- **การปรับปรุงและพัฒนาระบบการดำเนินงาน** (Continuous Improvement Mechanism):
  - บริษัทมุ่งมั่นในการพัฒนาและปรับปรุงระบบบริหารจัดการข้อมูลส่วนบุคคล (Data Privacy Management System – DPMS) ให้ทันต่อความเสี่ยงและภัยคุกคามทางไซเบอร์ โดยบูรณาการผลจากการตรวจสอบภายใน (Internal Audit) และการประเมินความเสี่ยง (Risk Assessment) เข้ากับการวางแผนปรับปรุงมาตรการด้านเทคโนโลยีและการควบคุมภายใน
  - บริษัทนำข้อเสนอแนะจากผู้มีส่วนได้เสีย คู่ค้า และหน่วยงานกำกับดูแลมาวิเคราะห์เพื่อพัฒนานโยบายและกระบวนการทำงานอย่างต่อเนื่อง เพื่อให้เกิดการเรียนรู้และการปรับตัวขององค์กรในด้านการคุ้มครองข้อมูลส่วนบุคคล
  - บริษัทสนับสนุนให้พนักงานและหน่วยงานที่เกี่ยวข้องร่วมเสนอแนวคิดหรือแนวทางนวัตกรรมในการปกป้องข้อมูลส่วนบุคคล เพื่อสร้างวัฒนธรรมองค์กรแห่งการเรียนรู้และการพัฒนาอย่างยั่งยืน
- **การติดตามแนวโน้มและมาตรฐานใหม่** (Emerging Standards and Technology Tracking):
  - บริษัทติดตามแนวโน้มทางเทคโนโลยีและกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล ทั้งในระดับประเทศและระดับสากล เช่น แนวทางของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (PDPC) และมาตรฐานขององค์กรมาตรฐานสากล (ISO) เพื่อปรับปรุงนโยบายและมาตรการให้ทันสมัยอยู่เสมอ
  - บริษัทพิจารณานำเครื่องมือหรือระบบใหม่ ๆ เช่น ระบบประเมินความเสี่ยงอัตโนมัติ (Automated Risk Assessment) หรือเทคโนโลยีการเข้ารหัสขั้นสูง (Advanced Encryption) มาใช้ เพื่อเพิ่มประสิทธิภาพในการบริหารความปลอดภัยของข้อมูล
- **การมีส่วนร่วมของผู้มีส่วนได้เสีย** (Stakeholder Engagement for Improvement):
  - บริษัทเปิดโอกาสให้ผู้มีส่วนได้เสีย ทั้งภายในและภายนอกองค์กร มีส่วนร่วมในการให้ข้อเสนอแนะเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ผ่านช่องทางการติดต่อสื่อสารและ

แบบสอบถามออนไลน์ เพื่อใช้เป็นข้อมูลในการปรับปรุงกระบวนการทำงานและยกระดับมาตรฐานความปลอดภัยของข้อมูลอย่างต่อเนื่อง

บริษัทมุ่งมั่นที่จะรักษามาตรฐานสูงสุดในการบริหารจัดการข้อมูลส่วนบุคคล โดยมองว่าการคุ้มครองข้อมูลไม่ใช่เพียงข้อกำหนดทางกฎหมาย แต่เป็นส่วนสำคัญของวัฒนธรรมองค์กรด้านธรรมาภิบาล ความโปร่งใส และความยั่งยืน

(สอดคล้องกับเกณฑ์ FTSE Russell SHR07 – Data Privacy and Protection, GRI 418 – Customer Privacy, ISO/IEC 27701, PDPA พ.ศ. 2562, และ SDG 16 – Peace, Justice and Strong Institutions)

14) ประวัติการทบทวนและปรับปรุงนโยบายการคุ้มครองข้อมูลส่วนบุคคล

ฉบับที่	วันที่	เจ้าของนโยบาย	อนุมัติโดย	การเปลี่ยนแปลง / หมายเหตุสำคัญ
1.0	11 พฤศจิกายน 2568	คณะกรรมการบริหารความเสี่ยงและกำกับดูแลกิจการ / คณะกรรมการความยั่งยืน / เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล	คณะกรรมการบริษัท	จัดทำและประกาศใช้นโยบายการคุ้มครองข้อมูลส่วนบุคคลฉบับแรก โดย บูรณาการ (Integration) จาก นโยบายการรักษาความลับของข้อมูล และ นโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ เพื่อสร้างกรอบการบริหารจัดการข้อมูลส่วนบุคคลที่ครอบคลุมทั้งด้านกฎหมาย ความมั่นคงปลอดภัย และสิทธิของเจ้าของข้อมูลให้เป็นเอกภาพเดียวกัน พร้อมปรับปรุงให้สอดคล้องกับ PDPA, มาตรฐาน ISO/IEC 27701, และเกณฑ์ FTSE Russell SHR07 เพื่อสนับสนุนกลยุทธ์การเปลี่ยนผ่านสู่ดิจิทัลขององค์กรอย่างมีประสิทธิภาพ

นโยบายฉบับนี้ได้รับการอนุมัติและประกาศใช้เพื่อให้ผู้เกี่ยวข้องทุกฝ่ายรับทราบและนำไปปฏิบัติ