นโยบายการรักษาความลับ

ฉบับที่ 2/2569 VNG-GOV-CONF-PL-02
วันที่มีผลบังคับใช้: 13 พฤษภาคม 2569

VANACHAI GROUP

นโยบายการรักษาความลับ

บริษัท วนชัย กรุ๊ป จำกัด (มหาชน) และบริษัทย่อย

บริษัท วนชัย กรุ๊ป จำกัด (มหาชน) และบริษัทย่อย ("บริษัท") ตระหนักว่าข้อมูลที่เป็นความลับ ข้อมูลทางธุรกิจ ข้อมูลส่วนบุคคล องค์ความรู้ทางเทคนิค ทรัพย์สินทางปัญญา ความลับทางการค้า ข้อมูลทางการเงิน ข้อมูลลูกค้าและคู่ค้า ข้อมูลพนักงาน เงื่อนไขทางการค้า แผนกลยุทธ์ ข้อมูลการผลิต และบันทึกดิจิทัล เป็นทรัพย์สินที่มีความสำคัญต่อความสามารถในการแข่งขัน ความไว้วางใจ การกำกับดูแลกิจการ นวัตกรรม และการสร้างคุณค่าในระยะยาว

บริษัทมุ่งมั่นในการปกป้องข้อมูลที่เป็นความลับจากการเข้าถึง การใช้ การเปิดเผย การคัดลอก การสูญหาย การแก้ไขเปลี่ยนแปลง การทำลาย การรั่วไหล หรือการนำไปใช้ในทางที่ไม่เหมาะสมโดยไม่ได้รับอนุญาต ไม่ว่าข้อมูลดังกล่าวจะอยู่ในรูปแบบเอกสาร สิ่งพิมพ์ อิเล็กทรอนิกส์ คำพูด ภาพ การประชุม หรืออยู่บนระบบคลาวด์ บริษัทตระหนักว่าการเปิดเผยข้อมูลที่เป็นความลับโดยไม่เหมาะสมอาจก่อให้เกิดผลกระทบด้านกฎหมาย การเงิน การดำเนินงาน ชื่อเสียง และความเชื่อมั่นของผู้มีส่วนได้เสีย

นโยบายฉบับนี้กำหนดหลักการ โครงสร้างการกำกับดูแล บทบาทความรับผิดชอบ และมาตรการควบคุมสำหรับการระบุ การจัดชั้นความลับ การปกป้อง การใช้ การจัดเก็บ การแบ่งปัน การเก็บรักษา และการทำลายข้อมูลที่เป็นความลับ เพื่อสนับสนุนกรอบการกำกับดูแลกิจการ การบริหารความเสี่ยง การควบคุมภายใน การคุ้มครองข้อมูลส่วนบุคคล ความปลอดภัยด้านเทคโนโลยีสารสนเทศ และการดำเนินธุรกิจอย่างรับผิดชอบของบริษัท

นโยบายฉบับนี้ได้รับการอนุมัติและประกาศใช้ เพื่อให้ผู้เกี่ยวข้องทุกฝ่ายรับทราบและนำไปปฏิบัติอย่างเคร่งครัด

1) วัตถุประสงค์

- กำหนดกรอบการดำเนินงานระดับองค์กรที่ชัดเจนสำหรับการคุ้มครองข้อมูลที่เป็นความลับ และป้องกันการเปิดเผยหรือการนำไปใช้โดยไม่ได้รับอนุญาต
- สร้างความเข้าใจให้กรรมการ ผู้บริหาร พนักงาน และบุคคลภายนอกที่เกี่ยวข้องทราบถึงหน้าที่และความรับผิดชอบในการจัดการข้อมูลที่เป็นความลับ
- ปกป้องผลประโยชน์ทางธุรกิจ ความสามารถในการแข่งขัน ชื่อเสียง ทรัพย์สินทางปัญญา ข้อมูลส่วนบุคคล ความลับทางการค้า และความไว้วางใจของผู้มีส่วนได้เสีย
- กำหนดให้การเข้าถึงและการเปิดเผยข้อมูลที่เป็นความลับดำเนินการเฉพาะเพื่อวัตถุประสงค์ทางธุรกิจที่ชอบด้วยกฎหมาย ได้รับอนุญาต และจำเป็นตามหลักการรู้เท่าที่จำเป็น
- ส่งเสริมการปฏิบัติตามกฎหมาย กฎระเบียบ สัญญา ภาระผูกพันด้านการไม่เปิดเผยข้อมูล หลักการกำกับดูแลกิจการ และนโยบายภายในที่เกี่ยวข้อง
- เสริมสร้างการควบคุมด้านการจัดชั้นข้อมูล การบริหารสิทธิการเข้าถึง การจัดเก็บอย่างปลอดภัย การสื่อสารอย่างปลอดภัย การเก็บรักษา การทำลาย การรายงานเหตุการณ์ และภาระผูกพันด้านการรักษาความลับของบุคคลภายนอก

- บูรณาการการบริหารความเสี่ยงด้านการรักษาความลับเข้าสู่กรอบการบริหารความเสี่ยงองค์กรและการดำเนินงานประจำวัน

2) ความสอดคล้องของนโยบายและมาตรฐานสากล

นโยบายนี้สอดคล้องกับมาตรฐาน กรอบการดำเนินงาน และแนวทางที่เกี่ยวข้อง ดังต่อไปนี้

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และกฎระเบียบลำดับรองที่เกี่ยวข้อง ในกรณีที่เกี่ยวข้องกับข้อมูลส่วนบุคคล
- พระราชบัญญัติความลับทางการค้า พ.ศ. 2545 และกฎหมายทรัพย์สินทางปัญญาที่เกี่ยวข้อง ในกรณีที่ข้อมูลทางธุรกิจ ข้อมูลทางเทคนิค หรือข้อมูลทางการค้ามีคุณสมบัติเป็นความลับทางการค้าหรือทรัพย์สินทางปัญญา
- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 พระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์ และกฎหมายอื่นที่เกี่ยวข้องกับระบบสารสนเทศ บันทึกอิเล็กทรอนิกส์ และการสื่อสารดิจิทัล
- พระราชบัญญัติหลักทรัพย์และตลาดหลักทรัพย์ แนวทางของ ก.ล.ต. และตลาดหลักทรัพย์แห่งประเทศไทย ในกรณีที่ข้อมูลที่เป็นความลับอาจเป็นข้อมูลภายในที่มีสาระสำคัญหรือข้อมูลอ่อนไหวต่อตลาดทุน
- ISO/IEC 27001 ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27002 มาตรการควบคุมความมั่นคงปลอดภัยสารสนเทศ และ ISO/IEC 27701 ระบบบริหารจัดการข้อมูลความเป็นส่วนตัว ตามความเหมาะสมกับบริบทและระดับความพร้อมของบริษัท
- หลักการของ NIST Cybersecurity Framework ด้านการกำกับดูแล การระบุ การปกป้อง การตรวจจับ การตอบสนอง และการกู้คืน ตามความเหมาะสม
- GRI Standards ได้แก่ GRI 2-23 Policy Commitments, GRI 2-24 Embedding Policy Commitments, GRI 2-27 Compliance with Laws and Regulations, GRI 3-3 Management of Material Topics และ GRI 418 Customer Privacy ตามความเกี่ยวข้อง
- FTSE Russell ESG Indicators ที่เกี่ยวข้องกับการกำกับดูแลกิจการ การบริหารความเสี่ยง ความมั่นคงปลอดภัยไซเบอร์ ความเป็นส่วนตัวของข้อมูล จริยธรรมทางธุรกิจ การควบคุมภายใน และการกำกับดูแลห่วงโซ่อุปทาน ตามความเกี่ยวข้อง
- จรรยาบรรณธุรกิจของบริษัท นโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศ ประกาศและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล นโยบายการป้องกันการใช้ข้อมูลภายในเพื่อแสวงหาผลประโยชน์ นโยบายการแจ้งเบาะแส นโยบายสิทธิมนุษยชน ข้อกำหนดด้านการจัดซื้อจัดจ้าง และระเบียบปฏิบัติภายในอื่นที่เกี่ยวข้อง

3) ขอบเขตของนโยบาย

นโยบายนี้ครอบคลุม:

- นโยบายฉบับนี้ใช้บังคับกับบริษัท บริษัทย่อย และกิจการร่วมค้าที่อยู่ภายใต้การควบคุมการดำเนินงานของบริษัท

- นโยบายฉบับนี้ใช้บังคับกับกรรมการ ผู้บริหาร พนักงาน พนักงานชั่วคราว นักศึกษาฝึกงาน ผู้รับเหมา ที่ปรึกษา บุคลากรจากภายนอกที่ได้รับมอบหมาย และบุคคลใดก็ตามที่สามารถเข้าถึงข้อมูลที่เป็นความลับของบริษัท
- นโยบายฉบับนี้ใช้บังคับกับคู่ค้า ลูกค้า ตัวแทน ผู้ให้บริการ ผู้ให้บริการคลาวด์ ผู้จำหน่ายซอฟต์แวร์ ผู้สอบบัญชี ที่ปรึกษา และพันธมิตรทางธุรกิจที่ได้รับ ประมวลผล จัดเก็บ ส่งต่อ หรือบริหารจัดการข้อมูลที่เป็นความลับของบริษัท
- นโยบายฉบับนี้ครอบคลุมข้อมูลที่เป็นความลับทุกรูปแบบ รวมถึงเอกสารกระดาษ ไฟล์อิเล็กทรอนิกส์ อีเมล ฐานข้อมูล บันทึกระบบ รูปภาพ แบบร่าง สูตรผลิตภัณฑ์ ข้อมูลทางเทคนิค แผนธุรกิจ ข้อมูลทางการเงิน เงื่อนไขทางการค้า เอกสารประกอบการประชุม การสื่อสารด้วยวาจา บันทึกบนระบบคลาวด์ และข้อมูลที่จัดเก็บอยู่ในอุปกรณ์ต่าง ๆ
- นโยบายฉบับนี้ใช้ตลอดวงจรชีวิตของข้อมูล ตั้งแต่การสร้าง การเก็บรวบรวม การจัดชั้น การเข้าถึง การใช้ การเปิดเผย การส่งต่อ การจัดเก็บ การเก็บรักษา การเก็บถาวร การส่งคืน การกำจัด และการทำลาย

4) คำจำกัดความและเอกสารอ้างอิง

- **ข้อมูลที่เป็นความลับ:** ข้อมูลที่ไม่เปิดเผยต่อสาธารณะ ซึ่งเป็นของบริษัท อยู่ภายใต้การควบคุมของบริษัท ได้รับมอบหมายให้บริษัทดูแล หรือใช้ในการดำเนินธุรกิจของบริษัท และอาจก่อให้เกิดความเสียหายหรือความเสียเปรียบแก่บริษัทหรือผู้มีส่วนได้เสียหากถูกเปิดเผยโดยไม่ได้รับอนุญาต
- **ข้อมูลที่มีข้อจำกัดสูง:** ข้อมูลที่เป็นความลับซึ่งมีความอ่อนไหวสูง และต้องได้รับการคุ้มครองอย่างเข้มงวดเป็นพิเศษ เนื่องจากมีนัยสำคัญด้านกฎหมาย กลยุทธ์ การเงิน การค้า ข้อมูลส่วนบุคคล ความลับทางการค้า หรือข้อมูลอ่อนไหวต่อตลาดทุน
- **ข้อมูลภายในองค์กร:** ข้อมูลที่จัดทำเพื่อใช้ภายในบริษัทและไม่เปิดเผยต่อสาธารณะ เว้นแต่ได้รับอนุญาตตามช่องทางที่กำหนด
- **ข้อมูลสาธารณะ:** ข้อมูลที่ได้รับอนุมัติอย่างเป็นทางการให้เปิดเผยต่อสาธารณะผ่านช่องทางที่ได้รับอนุญาต
- **ข้อมูลส่วนบุคคล:** ข้อมูลเกี่ยวกับบุคคลซึ่งสามารถระบุตัวบุคคลนั้นได้ ตามความหมายที่กำหนดไว้ในกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง
- **ความลับทางการค้า:** ข้อมูลทางธุรกิจ เทคนิค หรือการค้า ที่ไม่เป็นที่รู้จักโดยทั่วไป มีมูลค่าทางการค้าเนื่องจากเป็นความลับ และมีมาตรการที่เหมาะสมในการรักษาไว้เป็นความลับ
- **ข้อมูลภายในที่มีสาระสำคัญซึ่งยังไม่เปิดเผยต่อสาธารณะ:** ข้อมูลที่ยังไม่เปิดเผยต่อสาธารณะ และอาจมีผลอย่างสมเหตุสมผลต่อราคาหลักทรัพย์ การตัดสินใจของผู้ลงทุน มูลค่าธุรกิจ หรือการตัดสินใจของผู้มีส่วนได้เสีย และต้องได้รับการจัดการตามนโยบายการใช้ข้อมูลภายในของบริษัท
- **เจ้าของข้อมูล:** หน่วยงาน สายงาน หรือบุคคลที่ได้รับมอบอำนาจให้กำหนดระดับชั้นข้อมูล สิทธิการเข้าถึง การใช้งาน ระยะเวลาการเก็บรักษา และวิธีการทำลายข้อมูล
- **ผู้ดูแลข้อมูล:** บุคคลหรือหน่วยงานที่รับผิดชอบในการดูแล จัดเก็บ รักษาความปลอดภัย หรือดำเนินงานระบบที่เก็บข้อมูลที่เป็นความลับ

- **หลักการรู้เท่าที่จำเป็น:** การจำกัดการเข้าถึงข้อมูลที่เป็นความลับเฉพาะบุคคลที่จำเป็นต้องใช้ข้อมูลดังกล่าวเพื่อปฏิบัติหน้าที่ที่ได้รับอนุญาต หรือเพื่อวัตถุประสงค์ทางธุรกิจที่ชอบด้วยกฎหมาย
- **ข้อตกลงการไม่เปิดเผยข้อมูล (NDA):** ข้อตกลงเป็นลายลักษณ์อักษรที่กำหนดให้บุคคลหรือองค์กรต้องคุ้มครองข้อมูลที่เป็นความลับ และจำกัดการใช้และการเปิดเผยข้อมูลดังกล่าว
- **การรั่วไหลของข้อมูล:** การเปิดเผย การส่งต่อ การสูญหาย หรือการเปิดให้บุคคลที่ไม่ได้รับอนุญาตเข้าถึงข้อมูลที่เป็นความลับ ไม่ว่าจะเกิดจากความจงใจ ความผิดพลาด หรือความประมาทเลินเล่อ
- **กรอบการประเมินสาระสำคัญและความเสี่ยงแบบบูรณาการของกลุ่มบริษัทวนชัย (V-IMRA):** กระบวนการภายในของบริษัทในการระบุและจัดลำดับความสำคัญของประเด็นด้านความยั่งยืน การกำกับดูแล และความเสี่ยงทางธุรกิจ โดยบูรณาการมุมมองสาระสำคัญด้านผลกระทบและสาระสำคัญทางการเงิน เพื่อสนับสนุนการบริหารความเสี่ยงองค์กร การวางแผนกลยุทธ์ และการตัดสินใจ

5) การกำกับดูแลและความรับผิดชอบ

- **คณะกรรมการบริษัท:** อนุมัตินโยบายฉบับนี้ และกำกับดูแลการกำกับกิจการ การบริหารความเสี่ยง การควบคุมภายใน และการดำเนินงานอย่างมีจริยธรรมที่เกี่ยวข้องกับการรักษาความลับและการคุ้มครองข้อมูล
- **คณะกรรมการบริหารความเสี่ยงและกำกับดูแลกิจการ:** กำกับดูแลความเสี่ยงที่เกี่ยวข้องกับการรักษาความลับ รวมถึงการรั่วไหลของข้อมูล การเปิดเผยข้อมูลที่ไม่เหมาะสม ความขัดแย้งทางผลประโยชน์ การนำข้อมูลไปใช้ในทางที่ไม่เหมาะสม ความเสี่ยงด้านข้อมูลจากบุคคลภายนอก และการบูรณาการเข้าสู่กรอบการบริหารความเสี่ยงองค์กร
- **คณะกรรมการตรวจสอบ:** ทบทวนความเพียงพอและประสิทธิผลของการควบคุมภายใน ผลการตรวจสอบ และมาตรการแก้ไขที่เกี่ยวข้องกับการรักษาความลับ การควบคุมการเข้าถึง และการคุ้มครองข้อมูล
- **กรรมการผู้จัดการและฝ่ายบริหาร:** จัดให้มีทรัพยากร ระบบ ระเบียบปฏิบัติ การอบรม และกลไกการบังคับใช้ที่เหมาะสม เพื่อให้การดำเนินงานตามนโยบายฉบับนี้มีประสิทธิผล
- **ฝ่ายกฎหมาย ฝ่ายกำกับดูแล และเลขานุการบริษัท:** ให้คำแนะนำเกี่ยวกับภาระผูกพันทางกฎหมาย ข้อกำหนดการรักษาความลับในสัญญา ข้อตกลงไม่เปิดเผยข้อมูล การเปิดเผยข้อมูลตามกฎระเบียบ และข้อมูลที่อ่อนไหวต่อตลาดทุน
- **ฝ่ายเทคโนโลยีสารสนเทศ:** ดำเนินการและดูแลมาตรการควบคุมทางเทคนิคเพื่อคุ้มครองข้อมูลที่เป็นความลับ รวมถึงการควบคุมการเข้าถึง การพิสูจน์ตัวตน การเข้ารหัส การบันทึกการใช้งาน การสำรองข้อมูล ความปลอดภัยคลาวด์ การติดตาม และการตอบสนองต่อเหตุการณ์
- **ฝ่ายทรัพยากรบุคคล:** บูรณาการข้อกำหนดด้านการรักษาความลับเข้ากับวงจรชีวิตพนักงาน การปฐมนิเทศ สัญญาจ้าง การอบรม การโยกย้าย การสิ้นสุดการจ้างงาน และการดำเนินการทางวินัย
- **หัวหน้าหน่วยงานและเจ้าของข้อมูล:** กำหนดชั้นข้อมูล อนุมัติสิทธิการเข้าถึง ควบคุมการใช้ข้อมูลที่เป็นความลับ และทบทวนสิทธิการเข้าถึงของบุคลากรภายใต้ความรับผิดชอบอย่างสม่ำเสมอ
- **พนักงานและผู้ใช้งานทุกคน:** ต้องรักษาความลับ ใช้ข้อมูลเพื่อวัตถุประสงค์ที่ได้รับอนุญาต ปฏิบัติตามหลักการรู้เท่าที่จำเป็น และรายงานเหตุการณ์หรือข้อสงสัยเกี่ยวกับการรั่วไหลของข้อมูลโดยทันที

- **คู่ค้า ผู้รับเหมา ที่ปรึกษา และพันธมิตรทางธุรกิจ:** ต้องปฏิบัติตามข้อกำหนดด้านการรักษาความลับตามสัญญา นโยบาย และข้อกำหนดของบริษัทเมื่อได้รับหรือเข้าถึงข้อมูลที่เป็นความลับของบริษัท

6) พันธสัญญาและหลักการ

6.1 การปฏิบัติตามกฎหมายและการดำเนินงานอย่างมีจริยธรรม

- ปฏิบัติตามกฎหมาย กฎระเบียบ ภาระผูกพันตามสัญญา ภาระผูกพันด้านการไม่เปิดเผยข้อมูล และนโยบายภายในที่เกี่ยวข้องกับข้อมูลที่เป็นความลับ ข้อมูลส่วนบุคคล ความลับทางการค้า ทรัพย์สินทางปัญญา และข้อมูลอ่อนไหวต่อตลาดทุน
- ใช้ข้อมูลที่เป็นความลับเฉพาะเพื่อวัตถุประสงค์ทางธุรกิจที่ชอบด้วยกฎหมาย และสอดคล้องกับความซื่อสัตย์สุจริต ความโปร่งใส และความรับผิดชอบทางวิชาชีพ

6.2 การจัดชั้นข้อมูลและการเข้าถึงตามหลักการรู้เท่าที่จำเป็น

- จัดชั้นข้อมูลตามระดับความอ่อนไหว ความสำคัญต่อธุรกิจ ข้อกำหนดทางกฎหมาย และผลกระทบที่อาจเกิดขึ้นจากการเปิดเผยโดยไม่ได้รับอนุญาต
- จำกัดการเข้าถึงข้อมูลที่เป็นความลับตามหลักการรู้เท่าที่จำเป็นและหลักสิทธิขั้นต่ำที่จำเป็น พร้อมการอนุมัติและการทบทวนอย่างเหมาะสม

6.3 การควบคุมการคุ้มครอง การใช้ และการเปิดเผยข้อมูล

- ปกป้องข้อมูลที่เป็นความลับจากการเข้าถึง การคัดลอก การแก้ไข การส่งต่อ การเปิดเผย การทำลาย การสูญหาย หรือการนำไปใช้ในทางที่ไม่เหมาะสมโดยไม่ได้รับอนุญาต
- เปิดเผยข้อมูลที่เป็นความลับเฉพาะแก่บุคคลหรือองค์กรที่ได้รับอนุญาต และเฉพาะเมื่อจำเป็นเพื่อวัตถุประสงค์ทางธุรกิจที่ได้รับอนุมัติหรือข้อกำหนดทางกฎหมาย

6.4 การจัดเก็บ การส่งต่อ และการสื่อสารอย่างปลอดภัย

- จัดเก็บข้อมูลที่เป็นความลับไว้ในระบบที่ได้รับอนุมัติ สถานที่จัดเก็บทางกายภาพที่ปลอดภัย หรือคลังข้อมูลดิจิทัลที่มีการควบคุมการเข้าถึงอย่างเหมาะสม
- ใช้ช่องทางการสื่อสารที่ปลอดภัย การเข้ารหัส หรือมาตรการคุ้มครองอื่นเมื่อส่งต่อข้อมูลที่มีข้อจำกัดสูงหรือข้อมูลอ่อนไหว

6.5 การคุ้มครองข้อมูลส่วนบุคคลและความเป็นส่วนตัว

- จัดการข้อมูลส่วนบุคคลให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล ประกาศความเป็นส่วนตัว และระเบียบปฏิบัติด้านการคุ้มครองข้อมูลของบริษัท
- เก็บรวบรวม ใช้ เปิดเผย เก็บรักษา และลบข้อมูลส่วนบุคคลเท่าที่จำเป็นสำหรับวัตถุประสงค์ที่ชอบด้วยกฎหมายและระบุไว้อย่างชัดเจน

6.6 ความลับทางการค้า ทรัพย์สินทางปัญญา และองค์ความรู้ทางธุรกิจ

- คุ้มครองข้อมูลการพัฒนาผลิตภัณฑ์ สูตรผลิตภัณฑ์ องค์ความรู้ทางเทคนิค กระบวนการผลิต ข้อมูลเชิงลึกลูกค้า กลยุทธ์ทางการค้า ข้อมูลวิจัยและนวัตกรรม ในฐานะทรัพย์สินที่เป็นความลับของบริษัท
- ป้องกันการเปิดเผยหรือการใช้ความลับทางการค้าและทรัพย์สินทางปัญญาของบริษัท ลูกค้า คู่ค้า หรือพันธมิตรทางธุรกิจโดยไม่ได้รับอนุญาต

6.7 ข้อมูลภายในและการสื่อสารภายนอก

- จัดการข้อมูลภายในที่มีสาระสำคัญซึ่งยังไม่เปิดเผยต่อสาธารณะให้สอดคล้องกับนโยบายการป้องกันการใช้ข้อมูลภายในเพื่อแสวงหาผลประโยชน์ของบริษัท
- กำหนดให้การสื่อสารภายนอก การให้ข่าวแก่สื่อ การสื่อสารกับนักลงทุน รายงานสาธารณะ และการเปิดเผยข้อมูลตามกฎระเบียบ ดำเนินการโดยบุคคลที่ได้รับอนุญาตผ่านช่องทางที่ได้รับอนุมัติเท่านั้น

6.8 การรักษาความลับของบุคคลภายนอก

- กำหนดให้มีข้อกำหนดการรักษาความลับ ข้อตกลงไม่เปิดเผยข้อมูล ข้อตกลงการคุ้มครองข้อมูล หรือมาตรการคุ้มครองที่เทียบเท่าอย่างเหมาะสมก่อนแบ่งปันข้อมูลที่เป็นความลับกับบุคคลภายนอก
- กำหนดให้บุคคลภายนอกที่ได้รับข้อมูลที่เป็นความลับใช้ข้อมูลดังกล่าวเฉพาะตามวัตถุประสงค์ที่ตกลงไว้ และต้องใช้มาตรการรักษาความปลอดภัยที่เหมาะสม

6.9 การเก็บรักษา การส่งคืน และการทำลายอย่างปลอดภัย

- เก็บรักษาข้อมูลที่เป็นความลับเท่าที่จำเป็นตามกฎหมาย สัญญา หรือความจำเป็นทางธุรกิจ
- ส่งคืน ลบ ทำลาย หรือจัดเก็บถาวรข้อมูลที่เป็นความลับอย่างปลอดภัยเมื่อไม่จำเป็นต้องใช้ต่อไป หรือเมื่อสิ้นสุดความสัมพันธ์ด้านการจ้างงาน สัญญา หรือธุรกิจ

6.10 การรายงานเหตุการณ์และความรับผิดชอบ

- รายงานกรณีที่สงสัยหรือเกิดการสูญหาย การรั่วไหล การเปิดเผยโดยไม่ได้รับอนุญาต หรือการนำข้อมูลที่เป็นความลับไปใช้ในทางที่ไม่เหมาะสมโดยทันทีผ่านช่องทางที่บริษัทกำหนด
- ดำเนินมาตรการแก้ไข มาตรการทางวินัย และการดำเนินการทางกฎหมายตามความเหมาะสมเมื่อเกิดการละเมิดการรักษาความลับ

7) การบริหารความเสี่ยง ผลกระทบ และการพึ่งพา

- ความเสี่ยง ผลกระทบ และการพึ่งพาที่เกี่ยวข้องกับประเด็นภายใต้นโยบายฉบับนี้จะได้รับการระบุ วิเคราะห์ และจัดลำดับความสำคัญผ่านกระบวนการกรอบการประเมินสาระสำคัญและความเสี่ยงแบบบูรณาการของกลุ่มบริษัทวนชัย (V-IMRA) ซึ่งพิจารณาทั้งสาระสำคัญด้านผลกระทบและสาระสำคัญทางการเงินตลอดห่วงโซ่คุณค่า
- ผลการประเมินจาก V-IMRA จะถูกบูรณาการเข้าสู่ระบบการบริหารความเสี่ยงองค์กร (ERM) เพื่อสนับสนุนการกำหนดนโยบาย การตัดสินใจเชิงกลยุทธ์ การควบคุมภายใน ระดับความเสี่ยงที่ยอมรับได้ เจ้าของความเสี่ยง และการสร้างคุณค่าในระยะยาว
- ความเสี่ยงด้านการรักษาความลับที่สำคัญ ได้แก่ การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต การรั่วไหลของข้อมูล การเข้าถึงที่ไม่เหมาะสม การบุกรุกทางไซเบอร์ การใช้ข้อมูลโดยบุคคลภายในในทางที่ไม่เหมาะสม การสูญหายของเอกสารหรืออุปกรณ์ การเปิดเผยข้อมูลโดยบุคคลภายนอก การสื่อสารสาธารณะที่ไม่เหมาะสม การเปลี่ยนแปลงบุคลากร การหลอกลวงทางสังคม การตั้งค่าระบบคลาวด์ไม่เหมาะสม และการใช้เครื่องมือดิจิทัลที่ไม่ได้รับอนุมัติ

- บริษัทจะประเมินความเสี่ยงด้านการรักษาความลับโดยพิจารณาความอ่อนไหวของข้อมูล ภาระผูกพันทางกฎหมาย ความสำคัญต่อธุรกิจ ผลกระทบต่อผู้มีส่วนได้เสีย ความสูญเสียทางการเงินที่อาจเกิดขึ้น ความเสียหายต่อชื่อเสียง และความเป็นไปได้ของการเกิดเหตุการณ์
- มาตรการตอบสนองต่อความเสี่ยงประกอบด้วยการจัดชั้นข้อมูล การควบคุมการเข้าถึง ข้อตกลงไม่เปิดเผยข้อมูล การสื่อสารอย่างปลอดภัย การเข้ารหัส การปฏิบัติตามหลักโต๊ะทำงานสะอาดและหน้าจอปลอดข้อมูล การสร้างความตระหนักของผู้ใช้งาน การทำลายอย่างปลอดภัย การติดตาม การตอบสนองต่อเหตุการณ์ และการดำเนินมาตรการแก้ไข
- เหตุการณ์ด้านการรักษาความลับและจุดอ่อนของการควบคุมที่มีสาระสำคัญต้องได้รับการรายงานต่อฝ่ายบริหารและหน่วยงานกำกับดูแลที่เกี่ยวข้อง พร้อมติดตามจนกว่ามาตรการแก้ไขจะดำเนินการแล้วเสร็จ

8) เป้าหมายและตัวชี้วัด

- ร้อยละของพนักงานและผู้ใช้งานที่เกี่ยวข้องที่ผ่านการอบรมด้านการรักษาความลับ การคุ้มครองข้อมูลส่วนบุคคล และการสร้างความตระหนักด้านความปลอดภัยสารสนเทศ
- ร้อยละของแหล่งจัดเก็บข้อมูลที่เป็นความลับและมีความสำคัญที่มีเจ้าของข้อมูลที่ได้รับมอบหมายและมีการควบคุมการเข้าถึงที่ได้รับอนุมัติ
- ร้อยละของสิทธิการเข้าถึงของผู้ใช้งานในระบบที่มีข้อมูลอ่อนไหว ซึ่งได้รับการทบทวนอย่างน้อยปีละครั้ง หรือเมื่อมีการเปลี่ยนแปลงบทบาท โอนย้าย ลาออก หรือสิ้นสุดสัญญา
- ร้อยละของสัญญาที่เกี่ยวข้องกับคู่ค้า ผู้รับเหมา ที่ปรึกษา และพันธมิตรทางธุรกิจ ซึ่งมีข้อกำหนดการรักษาความลับหรือการไม่เปิดเผยข้อมูล
- จำนวนและระดับความรุนแรงของการละเมิดการรักษาความลับ เหตุการณ์ข้อมูลรั่วไหล เหตุการณ์เข้าถึงโดยไม่ได้รับอนุญาต และเหตุการณ์ข้อมูลส่วนบุคคล
- ระยะเวลาเฉลี่ยในการรับทราบ ควบคุม ตรวจสอบ และปิดเหตุการณ์ที่เกี่ยวข้องกับการรักษาความลับ
- ร้อยละของบุคคลภายนอกที่มีความสำคัญที่ได้รับการประเมินด้านการรักษาความลับ การคุ้มครองข้อมูลส่วนบุคคล และการควบคุมความปลอดภัยสารสนเทศ ตามความเกี่ยวข้อง
- จำนวนมาตรการแก้ไขจากการตรวจสอบ เหตุการณ์ หรือการทบทวน ที่ดำเนินการแล้วเสร็จภายในระยะเวลาที่กำหนด
- การรายงานผลการดำเนินงานด้านการรักษาความลับ ความเสี่ยงสำคัญ และมาตรการปรับปรุงต่อหน่วยงานกำกับดูแลที่เกี่ยวข้องเป็นประจำทุกปี

9) ห่วงโซ่อุปทานและความรับผิดชอบของพันธมิตร

- กำหนดให้คู่ค้า ผู้รับเหมา ที่ปรึกษา ผู้ให้คำปรึกษา ผู้ให้บริการคลาวด์ ผู้จำหน่ายซอฟต์แวร์ และพันธมิตรทางธุรกิจต้องคุ้มครองข้อมูลที่เป็นความลับที่ได้รับจากบริษัท
- ระบุข้อกำหนดด้านการรักษาความลับ การไม่เปิดเผยข้อมูล การคุ้มครองข้อมูล การควบคุมการเข้าถึง การแจ้งเหตุการณ์ สิทธิในการตรวจสอบ การจ้างช่วง และการส่งคืนหรือทำลายข้อมูลในสัญญาและเอกสารจัดซื้อจัดจ้างที่เกี่ยวข้อง

- ดำเนินการตรวจสอบสถานะด้านการรักษาความลับและความปลอดภัยสารสนเทศของบุคคลภายนอกที่มีความสำคัญ ตามระดับความอ่อนไหวของข้อมูลและความสำคัญของบริการ
- จำกัดการเข้าถึงข้อมูลที่เป็นความลับของบุคคลภายนอกเฉพาะวัตถุประสงค์ที่ได้รับอนุมัติ มีการจัดทำเอกสาร กำหนดระยะเวลา และเป็นไปตามหลักการรู้เท่าที่จำเป็น พร้อมยกเลิกสิทธิทันทีเมื่อไม่จำเป็นต้องเข้าถึงอีกต่อไป
- กำหนดให้บุคคลภายนอกรับรองว่าพนักงาน ผู้รับเหมาช่วง และตัวแทนของตนที่เข้าถึงข้อมูลที่เป็นความลับของบริษัทอยู่ภายใต้ภาระผูกพันด้านการรักษาความลับที่เทียบเท่า
- กำหนดให้ข้อมูลที่เป็นความลับต้องถูกส่งคืน ลบ หรือทำลายอย่างปลอดภัยเมื่อสัญญาสิ้นสุด การให้บริการสิ้นสุดลง หรือเมื่อบริษัทร้องขอ ทั้งนี้อยู่ภายใต้ข้อกำหนดด้านการเก็บรักษาตามกฎหมายและสัญญา

10) การบูรณาการกับกลยุทธ์องค์กร

นโยบายฉบับนี้สนับสนุนวัตถุประสงค์ด้านการกำกับดูแลกิจการ การบริหารความเสี่ยง การเปลี่ยนผ่านดิจิทัล นวัตกรรม ความไว้วางใจของลูกค้า ความร่วมมือกับคู่ค้า การรายงานด้านความยั่งยืน และความต่อเนื่องทางธุรกิจของบริษัท

- **FOREST**: คุ้มครองข้อมูลด้านการจัดหาแหล่งวัตถุดิบ การตรวจสอบย้อนกลับ สวนป่า การผลิต สิ่งแวดล้อม และข้อมูลด้านความยั่งยืนที่สนับสนุนการบริหารจัดการทรัพยากรธรรมชาติและผลิตภัณฑ์ไม้ทดแทนธรรมชาติอย่างรับผิดชอบ
- **FUTURE**: คุ้มครองข้อมูลด้านนวัตกรรม การวิจัยและพัฒนา การออกแบบผลิตภัณฑ์ ระบบดิจิทัล กลยุทธ์ทางการค้า และข้อมูลเชิงธุรกิจ เพื่อเสริมสร้างความสามารถในการแข่งขันระยะยาว
- **TOGETHER**: เสริมสร้างความไว้วางใจของผู้มีส่วนได้เสียด้วยการคุ้มครองข้อมูลของพนักงาน ลูกค้า คู่ค้า ชุมชน นักลงทุน และพันธมิตรทางธุรกิจ ผ่านการกำกับดูแลข้อมูลอย่างรับผิดชอบและโปร่งใส

บูรณาการประเด็นการรักษาความลับเข้ากับกระบวนการจัดซื้อจัดจ้าง การบริหารสัญญา การบริหารวงจรชีวิตพนักงาน การบริหารโครงการ การพัฒนาผลิตภัณฑ์ การเปลี่ยนผ่านดิจิทัล การสื่อสารภายนอก และกระบวนการเปิดเผยข้อมูล

11) การดำเนินงานและเครื่องมือการบริหารจัดการ

11.1 การจัดชั้นและการระบุระดับข้อมูล

- กำหนดระดับชั้นข้อมูลที่สามารถนำไปใช้ได้จริง เช่น ข้อมูลสาธารณะ ข้อมูลภายใน ข้อมูลลับ และข้อมูลที่มีข้อจำกัดสูง พร้อมข้อกำหนดการจัดการที่เหมาะสมสำหรับแต่ละระดับ
- ระบุระดับความอ่อนไหวและข้อกำหนดการจัดการบนเอกสารลับ ไฟล์อิเล็กทรอนิกส์ งานนำเสนอ และอีเมลตามความเหมาะสม

11.2 การควบคุมการเข้าถึงและการอนุมัติสิทธิ

- ใช้กระบวนการอนุมัติ การกำหนดสิทธิตามบทบาท หลักสิทธิขั้นต่ำที่จำเป็น การพิสูจน์ตัวตน บันทึกการเข้าถึง และการทบทวนสิทธิเป็นระยะสำหรับข้อมูลที่เป็นความลับและระบบที่มีข้อมูลอ่อนไหว
- ยกเลิกสิทธิการเข้าถึงโดยทันทีเมื่อพนักงานโอนย้าย ลาออก สิ้นสุดการจ้างงาน หรือไม่จำเป็นต้องเข้าถึงข้อมูลดังกล่าวเพื่อปฏิบัติหน้าที่อีกต่อไป

11.3 เครื่องมือด้านสัญญาและกฎหมาย

- ใช้ข้อกำหนดการรักษาความลับ ข้อตกลงไม่เปิดเผยข้อมูล ข้อตกลงการประมวลผลข้อมูล และข้อกำหนดด้านทรัพย์สินทางปัญญาตามความเหมาะสมสำหรับพนักงาน คู่ค้า ผู้รับเหมา ที่ปรึกษา และพันธมิตรทางธุรกิจ
- ทบทวนภาระผูกพันตามสัญญาก่อนแบ่งปันข้อมูลที่เป็นความลับกับบุคคลภายนอก

11.4 แนวปฏิบัติการทำงานอย่างปลอดภัย

- ใช้แนวปฏิบัติโต๊ะทำงานสะอาดและหน้าจอปลอดข้อมูล การพิมพ์เอกสารอย่างปลอดภัย การควบคุมเอกสารประกอบการประชุม การแบ่งปันไฟล์อย่างปลอดภัย ช่องทางการสื่อสารที่ได้รับอนุมัติ และการใช้อุปกรณ์พกพาอย่างระมัดระวัง
- หลีกเลี่ยงการหารือเรื่องที่เป็นความลับในพื้นที่สาธารณะ หรือการแบ่งปันข้อมูลที่เป็นความลับผ่านอีเมลส่วนบุคคล พื้นที่จัดเก็บคลาวด์ส่วนบุคคล แอปพลิเคชันรับส่งข้อความ หรือสื่อสังคมออนไลน์ที่ไม่ได้รับอนุมัติ

11.5 การอบรมและการสร้างความตระหนัก

- จัดให้มีการปฐมนิเทศและการอบรมเป็นระยะเกี่ยวกับภาระผูกพันด้านการรักษาความลับ การคุ้มครองข้อมูลส่วนบุคคล ข้อมูลภายใน การตระหนักรู้ฟิชชิง การจัดการเอกสาร การเปิดเผยข้อมูลแก่บุคคลภายนอก และการรายงานเหตุการณ์
- สื่อสารตัวอย่างพฤติกรรมต้องห้ามและพฤติกรรมที่คาดหวังอย่างชัดเจน เพื่อเสริมสร้างวัฒนธรรมการรักษาความลับของบริษัท

11.6 การตอบสนองต่อเหตุการณ์และการแก้ไข

- รักษาช่องทางการรายงานสำหรับกรณีที่สงสัยหรือเกิดการละเมิดการรักษาความลับจริง รวมถึงการรายงานต่อฝ่ายบริหาร ช่องทางแจ้งเบาะแส IT Service Center หรือช่องทางอื่นที่บริษัทกำหนด
- ตรวจสอบเหตุการณ์ ควบคุมความเสี่ยง กู้คืนข้อมูลเมื่อเป็นไปได้ แจ้งผู้เกี่ยวข้องตามข้อกำหนด และดำเนินมาตรการแก้ไขและป้องกัน

11.7 การเก็บรักษาบันทึกและการทำลายอย่างปลอดภัย

- จัดให้มีตารางการเก็บรักษาข้อมูลที่เป็นความลับตามข้อกำหนดทางกฎหมาย สัญญา และความจำเป็นทางธุรกิจ
- กำจัดข้อมูลที่เป็นความลับด้วยวิธีการที่ได้รับอนุมัติและปลอดภัย เช่น การทำลายเอกสารด้วยเครื่องทำลายเอกสาร การลบข้อมูลอย่างปลอดภัย การล้างข้อมูลจากสื่อบันทึก หรือการทำลายโดยมีใบรับรองตามความเหมาะสม

12) การติดตามผล รายงาน และความโปร่งใส

- ติดตามการปฏิบัติตามข้อกำหนดด้านการรักษาความลับผ่านการทบทวนสิทธิการเข้าถึง การตรวจสอบภายใน บันทึกเหตุการณ์ การทบทวนสัญญา การประเมินคู่ค้า การอบรมที่เสร็จสมบูรณ์ และการรายงานต่อฝ่ายบริหาร
- รายงานความเสี่ยงด้านการรักษาความลับที่มีสาระสำคัญ เหตุการณ์สำคัญ ผลการตรวจสอบ และมาตรการแก้ไขต่อฝ่ายบริหารและหน่วยงานกำกับดูแลที่เกี่ยวข้อง
- จัดเก็บบันทึกการอนุมัติสิทธิการเข้าถึง ข้อตกลงไม่เปิดเผยข้อมูล ข้อกำหนดการรักษาความลับ การเปิดเผยข้อมูลแก่บุคคลภายนอก รายงานเหตุการณ์ ผลการสอบสวน การอบรมที่เสร็จสมบูรณ์ และมาตรการแก้ไข
- กำหนดให้การเปิดเผยข้อมูลต่อสาธารณะผ่านรายงานประจำปี รายงานความยั่งยืน เว็บไซต์ ข่าว ประชาสัมพันธ์ การสื่อสารกับนักลงทุน และช่องทางอื่น ได้รับการทบทวนและอนุมัติโดยบุคคลที่มีอำนาจก่อนเผยแพร่
- เปิดเผยเฉพาะข้อมูลระดับภาพรวมที่เหมาะสมเกี่ยวกับการกำกับดูแลและการบริหารความเสี่ยงด้านการรักษาความลับ โดยไม่เปิดเผยข้อมูลที่เป็นความลับหรือก่อให้เกิดความเสี่ยงเพิ่มเติมด้านความปลอดภัยหรือการค้า

13) การทบทวนและการพัฒนาอย่างต่อเนื่อง

- นโยบายฉบับนี้ต้องได้รับการทบทวนอย่างน้อยทุกสองปี หรือเร็วกว่านั้นหากมีการเปลี่ยนแปลงกฎหมาย กฎระเบียบ การดำเนินธุรกิจ ระบบสารสนเทศ ความคาดหวังของผู้มีส่วนได้เสีย ระดับความเสี่ยง ผลการตรวจสอบ หรือเหตุการณ์ด้านการรักษาความลับที่มีสาระสำคัญ
- บริษัทจะพัฒนามาตรการควบคุมด้านการรักษาความลับอย่างต่อเนื่องให้สอดคล้องกับแนวปฏิบัติทางธุรกิจที่เปลี่ยนแปลง การเปลี่ยนผ่านดิจิทัล ข้อกำหนดทางกฎหมาย ภัยคุกคามทางไซเบอร์ และบทเรียนจากเหตุการณ์
- ผู้รับผิดชอบนโยบายร่วมกับหน่วยงานที่เกี่ยวข้องต้องจัดทำผลการทบทวนนโยบายและข้อเสนอแนะเพื่อการปรับปรุง เพื่อเสนอให้ฝ่ายบริหารและหน่วยงานกำกับดูแลพิจารณา
- การอบรม การทบทวนสิทธิการเข้าถึง การตรวจสอบภายใน การประเมินคู่ค้า การวิเคราะห์เหตุการณ์ และข้อเสนอแนะจากพนักงาน ต้องนำมาใช้เพื่อเสริมสร้างวัฒนธรรมการรักษาความลับและการกำกับดูแลข้อมูลของบริษัท

14) ประวัติการทบทวนและปรับปรุงนโยบายการรักษาความลับ

ฉบับที่	วันที่	เจ้าของนโยบาย	อนุมัติโดย	การเปลี่ยนแปลง / หมายเหตุสำคัญ
1.0	11 พฤศจิกายน 2567	คณะทำงานด้านการพัฒนาเพื่อความยั่งยืน	คณะกรรมการบริษัท	จัดทำนโยบายการรักษาความลับฉบับแรก โดยมุ่งเน้นการคุ้มครองข้อมูลที่เป็นความลับ ภาระผูกพันด้านการไม่เปิดเผยข้อมูล การสร้างความตระหนักของพนักงาน การจัดการข้อมูล และการใช้ข้อมูลของบริษัทอย่างรับผิดชอบ
2.0	13 พฤษภาคม 2569	คณะกรรมการบริหารความเสี่ยงและกำกับดูแลกิจการ	คณะกรรมการบริษัท	ปรับปรุงและขยายเนื้อหาให้อยู่ในโครงสร้างนโยบายองค์กรภายใต้รหัส VNG-GOV-CONF-PL-02 เสริมความชัดเจนด้านการกำกับดูแล การจัดชั้นข้อมูล การเข้าถึงตามหลักการรู้เท่าที่จำเป็น การคุ้มครองความลับทางการค้าและข้อมูลส่วนบุคคล ภาระผูกพันด้านการรักษาความลับของบุคคลภายนอก การรายงานเหตุการณ์ KPI การติดตามรายงาน และการบูรณาการกับ ERM และนโยบายภายในที่เกี่ยวข้อง

นโยบายฉบับนี้ได้รับการอนุมัติและประกาศใช้เพื่อให้ผู้เกี่ยวข้องทุกฝ่ายรับทราบและนำไปปฏิบัติ