veranda resort
PUBLIC COMPANY LIMITED

นโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

บริษัท วีรันดา รีสอร์ท จำกัด (มหาชน) และบริษัทย่อย ("บริษัท")

บริษัทตระหนักถึงความสำคัญของเทคโนโลยีสารสนเทศ ระบบเครือข่าย และปัญญาประดิษฐ์ (Artificial Intelligence : AI) ที่นำมาใช้เป็นเครื่องมือเพื่อเสริมสร้างประสิทธิภาพและประสิทธิผลการดำเนินงาน รวมทั้งการเติบโตขององค์กรอย่างยั่งยืน โดยยึดมั่นในการปกป้องข้อมูล ระบบ และการใช้ปัญญาประดิษฐ์อย่างมั่นคงปลอดภัย มีธรรมาภิบาล และมีความรับผิดชอบ

บริษัทได้จัดทำนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ ("นโยบาย") ที่สอดคล้องกับหลักกฎหมายและมาตรฐานสากลที่เกี่ยวข้อง เพื่อให้มั่นใจว่าการใช้และการบริหารจัดการเทคโนโลยีดังกล่าว มีความมั่นคง ปลอดภัย โปร่งใส เชื่อถือได้ โดยมีวัตถุประสงค์เพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ เพื่อกำหนดกรอบการควบคุม การป้องกัน และการบริหารจัดการความเสี่ยงด้านไซเบอร์อย่างเป็นระบบ

การบริหารจัดการความเสี่ยงด้านความปลอดภัยของเทคโนโลยีสารสนเทศอย่างเหมาะสมภายในองค์กร ตามแนวทางมาตรฐานสากลในการปกป้องทรัพย์สินเทคโนโลยีสารสนเทศของบริษัท จะลดความเสี่ยงของลูกค้า บุคคล และผู้มีส่วนได้เสียที่อยู่ในการดูแลรับผิดชอบของบริษัทจากภัยคุกคามต่างๆ ทั้งจากภายในและภายนอก ทั้งโดยเจตนาและไม่เจตนา และเพื่อให้เป็นไปตามกฎหมายและข้อบังคับต่างๆ ที่เกี่ยวข้อง ได้แก่

- กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และฉบับแก้ไขเพิ่มเติม
- กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (PDPA)
- กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์
- กฎหมายอื่นๆ ที่เกี่ยวข้อง และข้อบังคับจากหน่วยงานของรัฐ

นโยบายนี้มีขอบข่ายบังคับใช้กับผู้ใช้งานคอมพิวเตอร์ทุกคน ทั้งกรรมการ ผู้บริหาร และพนักงานทุกระดับของบริษัท รวมไปถึงบุคคลภายนอกที่ได้รับสิทธิ์ในการเข้าถึงระบบเทคโนโลยีสารสนเทศของบริษัท

บริษัทกำหนดโครงสร้างการกำกับดูแลให้การดำเนินงานเพื่อให้สอดคล้องกับนโยบาย ดังนี้

ผู้ที่เกี่ยวข้อง	หน้าที่และความรับผิดชอบ
กรรมการ	• กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ ไซเบอร์ และปัญญาประดิษฐ์ในภาพรวม • รับทราบรายงานความเสี่ยงด้านเทคโนโลยีสารสนเทศ ไซเบอร์ และปัญญาประดิษฐ์ที่มีนัยสำคัญ • พิจารณาอนุมัติการทบทวนนโยบาย
ผู้บริหาร/ผู้บังคับบัญชา	• ผลักดัน สนับสนุนและทบทวนการปฏิบัติงานและมาตรการต่างๆ ในขอบเขตความรับผิดชอบให้สอดคล้องกับกฎหมาย ข้อบังคับ และนโยบายบริษัท • สื่อสารนโยบายและมาตรการต่างๆ ให้กับพนักงานและบุคคลภายนอกภายใต้ขอบเขตความรับผิดชอบ • ดำเนินการให้พนักงานทุกคนในหน่วยงานได้รับการอบรมและมีความตระหนักด้านความปลอดภัยของเทคโนโลยีสารสนเทศอย่างเพียงพอที่จะรู้เท่าทันภัยในการปฏิบัติงานและการใช้งานระบบเทคโนโลยีสารสนเทศ

ผู้ที่เกี่ยวข้อง	หน้าที่และความรับผิดชอบ
ผู้ใช้งานทุกคน	ผู้ใช้งานทุกคนที่อยู่ภายใต้การบังคับใช้นโยบาย ต้องปฏิบัติตามนโยบาย และมาตรการต่างๆ ของบริษัท นอกจากนี้ผู้ใช้ต้องรายงานเหตุการณ์สิ่งผิดปกติ ที่พบเกี่ยวกับความปลอดภัยด้านเทคโนโลยีสารสนเทศ ให้กับแผนกเทคโนโลยีสารสนเทศรับทราบโดยทันที
เจ้าของระบบ/ข้อมูล	ทุกระบบข้อมูลสารสนเทศ หรือทรัพย์สินประเภทอื่นๆ ต้องมีบุคคลที่รับผิดชอบชัดเจน โดยเจ้าของระบบ/ข้อมูล จะต้องทำการ ดังนี้ • ประเมินความเสี่ยงและผลกระทบทางธุรกิจของระบบและข้อมูลสารสนเทศ • แบ่งระดับชั้นความปลอดภัยข้อมูล และสิทธิ์การใช้งานในระบบ ตามตำแหน่งงาน หรือหน้าที่การปฏิบัติงานสำหรับข้อมูลสารสนเทศในความรับผิดชอบ • ทบทวนประสิทธิผลของมาตรการที่จัดทำไป
ผู้ควบคุมข้อมูลส่วนบุคคล	ข้อมูลส่วนบุคคลที่ได้รับ จัดเก็บ ประมวลผล ส่งต่อ และทำลาย ต้องมีผู้ควบคุมข้อมูลที่รับผิดชอบชัดเจน โดยผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ควบคุมการบริหารจัดการข้อมูลส่วนบุคคลให้เป็นไปตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลและนโยบายนี้
หน่วยงานเทคโนโลยีสารสนเทศ	**การสนับสนุนและให้คำปรึกษา** • สนับสนุนงานปฏิบัติการระบบให้กับเจ้าของระบบ/ข้อมูล • ให้คำแนะนำทางเทคนิคกับเจ้าของระบบ/ข้อมูล ในการกำหนดความต้องการ • เลือกมาตรการการควบคุมที่เหมาะสม **การวางแผนและพัฒนาระบบ** • วางแผน ออกแบบ และพัฒนาระบบเทคโนโลยีสารสนเทศให้สอดคล้องกับกลยุทธ์องค์กร • บำรุงรักษาอุปกรณ์ Software / Hardware ให้อยู่ในสภาพพร้อมใช้งาน **การควบคุมการเข้าถึงและความปลอดภัย** • กำหนดมาตรการควบคุมการเข้าถึงระบบ (Access Control) • บริหารจัดการรหัสผ่านและสิทธิ์ผู้ใช้งานอย่างเป็นระบบ • การบริหารจัดการข้อมูลและภาวะฉุกเฉิน • จัดให้มีการสำรองข้อมูล (Backup) และทดสอบการกู้คืนข้อมูล (Recovery Test) **การรายงานและตรวจสอบ** • เฝ้าระวังภัยคุกคามทางไซเบอร์ และจัดทำแผนตอบสนองเหตุการณ์ รวมทั้งรายงานสถานะความเสี่ยงด้านเทคโนโลยีสารสนเทศต่อผู้บริหารทุกไตรมาส

ทั้งนี้ เพื่อให้การบริหารจัดการและการใช้งานระบบเทคโนโลยีสารสนเทศของบริษัทเป็นไปอย่างมีประสิทธิภาพ มีความมั่นคงปลอดภัย และเป็นไปตามมาตรฐาน รวมทั้งสามารถบริหารจัดการความเสี่ยงที่เกี่ยวข้องได้อย่างเหมาะสม และสอดคล้องกับนโยบายของบริษัท บริษัทจึงกำหนดหลักเกณฑ์ และมาตรการในการควบคุมดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ เพื่อใช้เป็นแนวทางให้ผู้ใช้งานและผู้ที่เกี่ยวข้องถือปฏิบัติ ดังต่อไปนี้

1. การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย

1.1 อุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น เครื่องแม่ข่าย (Server) อุปกรณ์เครือข่าย (Network) จะต้องถูกเก็บไว้ในศูนย์คอมพิวเตอร์หรือพื้นที่หวงห้าม ที่มีการจำกัดสิทธิการเข้าออกศูนย์คอมพิวเตอร์ให้เฉพาะเจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศเท่านั้น และบุคคลที่มีหน้าที่เกี่ยวข้องซึ่งอาจมีความจำเป็นต้องเข้าศูนย์คอมพิวเตอร์ในบางครั้ง ต้องมีการควบคุมอย่างรัดกุม เช่น กำหนดให้มีเจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศควบคุมดูแลการเข้าออกและปฏิบัติตามระเบียบขั้นตอนอย่างเคร่งครัด

1.2 บริษัทจะจัดให้มีระบบเก็บบันทึกการเข้าออกศูนย์คอมพิวเตอร์ โดยบันทึกดังกล่าวต้องมีรายละเอียดเกี่ยวกับตัวบุคคลและเวลาผ่านเข้าออก และควรมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ

2. บัญชีผู้ใช้งาน และรหัสผ่านของระบบเทคโนโลยีสารสนเทศ

2.1 บัญชีผู้ใช้งาน (User Account) และรหัสผ่าน (Password) ต้องเก็บเป็นความลับและห้ามเผยแพร่ให้กับบุคคลอื่น เพื่อความปลอดภัยของข้อมูลของบริษัท เช่น สิทธิบัตร ลิขสิทธิ์ ความลับทางการตลาด กฎหมาย ฯลฯ

2.2 การตั้งรหัสผ่านระบบงานต่างๆ ผู้ใช้งานควรกำหนดให้รหัสผ่านมีความยากต่อการคาดเดา เช่น ความยาวอย่างน้อย 8 ตัวอักษร และผสมด้วยตัวอักษร ตัวเลข อักขระพิเศษ เพื่อความปลอดภัยของบัญชี และข้อมูลผู้ใช้งาน

2.3 หากไม่ได้อยู่ที่เครื่องคอมพิวเตอร์ ผู้ใช้งานต้องทำการล็อคหน้าจอเพื่อไม่ให้บุคคลอื่นใช้งานได้ และต้องออกจากระบบ (Logoff) เมื่อไม่ได้ใช้งานระบบนั้นแล้วทันที

2.4 ผู้ใช้งานควรเปลี่ยนรหัสผ่านของทุกระบบที่ใช้งานทุก 90 วัน

2.5 ผู้ใช้งานจากภายนอก (Remote User) หรือ ผู้ใช้งานชั่วคราว (Guest) ต้องทำการร้องขอต่อแผนกเทคโนโลยีสารสนเทศเพื่อเปิดใช้งานบัญชีผู้ใช้งานชั่วคราวตามระยะเวลาที่ร้องขอ โดยรหัสผ่านจะเป็นลักษณะใช้งานได้ครั้งเดียว และต้องมีการกำกับดูแลการปฏิบัติงานของบุคคลภายนอกอย่างเคร่ง เพื่อป้องกันความเสียของระบบข้อมูล และข้อมูลอาจรั่วไหลได้

3. มาตรการการรักษาข้อมูลจากภัยคุกคามทางไซเบอร์

3.1 บริษัทจะกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลแต่ละประเภทชั้นความลับ และวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลให้สอดคล้องกับความสำคัญของข้อมูลประเภทต่างๆ

3.2 การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น การใช้ SSL การใช้ VPN เป็นต้น

3.3 บริษัทจะมีมาตรการรักษาความปลอดภัยข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของบริษัท เช่น การส่งซ่อม การตัดจำหน่ายทรัพย์สิน เป็นต้น ควรย้ายหรือทำลายข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เพื่อป้องกันข้อมูลสำคัญของบริษัทรั่วไหล

3.4 การป้องกันไวรัส และการโจมตีจากผู้ไม่หวังดี (Hacker) ที่อาจเจาะเข้าสู่ระบบข้อมูลของบริษัทโดยไม่ได้รับอนุญาต จะต้องมีมาตรการป้องกันที่มีประสิทธิภาพและปรับปรุงให้ทันสมัยอยู่เสมอสำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ของผู้ใช้งานที่เชื่อมต่อกับระบบเครือข่ายทุกเครื่อง เช่น ติดตั้งซอฟต์แวร์ป้องกันไวรัส (Antivirus) มีอุปกรณ์ไฟร์วอลล์ (Firewall) เพื่อป้องกันการโจมตีระบบข้อมูลของบริษัท ซึ่งอาจทำให้ข้อมูลของบริษัทรั่วไหลได้

3.5 ห้ามนำข้อมูลสำคัญของบริษัทเข้าสู่ระบบ Chatbot หรือ AI ซึ่งระบบอาจจะมีการขอข้อมูล จดจำข้อมูล และนำไปเผยแพร่ต่อผู้ใช้รายอื่น ซึ่งอาจทำให้ข้อมูลสำคัญของบริษัทรั่วไหลได้

4. **การใช้บริการระบบเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอก** (IT Outsourcing)

เพื่อเป็นการป้องกันการเข้าถึงระบบข้อมูลสารสนเทศของผู้ให้บริการภายนอก (IT Outsourcing) และมีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัย และระดับการให้บริการตามที่ตกลงกันไว้ในข้อตกลงการให้บริการ โดยมีแนวทางปฏิบัติ ดังนี้

4.1 จัดทำข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับข้อมูลของบริษัทสำหรับผู้ให้บริการภายนอกที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ โดยสอดคล้องกับข้อกำหนดเกี่ยวกับการรักษาความลับข้อมูลของบริษัท โดยเลือกผู้ให้บริการที่สามารถตรวจสอบประวัติ ข้อมูลต่างๆ ของผู้ให้บริการภายนอกได้ เช่น ผู้ให้บริการที่มีใบรบรองมาตรฐานสากล (ISO)

4.2 กรณีที่ขอบเขตการปฏิบัติงานของผู้ให้บริการภายนอกที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ (IT Outsourcing) มีส่วนเกี่ยวข้องกับการเก็บรวบรวม ใช้ เปิดเผย ข้อมูลส่วนบุคคลที่อยู่ในความครอบครองหรือควบคุมของบริษัท จะต้องเป็นไปตามนโยบายคุ้มครองข้อมูลส่วนบุคคล (PDPA) ของบริษัท

4.3 ต้องกำหนดให้มีการติดตาม ทบทวน และตรวจประเมินการให้บริการของผู้ให้บริการภายนอก (IT Outsourcing) อย่างสม่ำเสมอ รวมถึงจัดให้มีการอัปเดตข้อตกลงเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญในข้อตกลงหรือระบบที่เกี่ยวข้อง โดยจะต้องทำการประเมินความเสี่ยงด้านความมั่นคงและรายงานต่อผู้ที่เกี่ยวข้องก่อนดำเนินการ

5. **การสำรองข้อมูลและระบบคอมพิวเตอร์** (Backup)

5.1 บริษัทต้องสำรองข้อมูลสำคัญทางธุรกิจ รวมถึงโปรแกรมระบบปฏิบัติการ (Operating System) โปรแกรมระบบงานคอมพิวเตอร์ (Application System) และชุดคำสั่งที่ใช้ทำงานให้ครบถ้วน ให้สามารถพร้อมใช้งานได้อย่างต่อเนื่อง โดยต้องจัดเก็บสื่อบันทึกข้อมูลสำรอง พร้อมทั้งสำเนาขั้นตอนหรือวิธีปฏิบัติต่างๆ ไว้นอกสถานที่ เพื่อความปลอดภัยในกรณีที่สถานที่ปฏิบัติงานได้รับความเสียหาย โดยสถานที่ดังกล่าวต้องจัดให้มีระบบควบคุมการเข้าออกและระบบป้องกันความเสียหายดังกล่าว

5.2 ในกรณีที่จำเป็นต้องจัดเก็บข้อมูลเป็นระยะเวลานาน บริษัทต้องคำนึงถึงวิธีการนำข้อมูลกลับมาใช้งานในอนาคต เช่น หากจัดเก็บข้อมูลในสื่อบันทึกประเภทใด ก็ต้องมีการเก็บอุปกรณ์และซอฟท์แวร์ที่เกี่ยวข้องสำหรับใช้อ่านสื่อบันทึกประเภทนั้นไว้ด้วยเช่นกัน

5.3 ต้องทดสอบข้อมูลสำรองอย่างน้อยปีละ 2 ครั้ง เพื่อให้มั่นใจได้ว่าข้อมูล รวมทั้งโปรแกรมระบบต่างๆ ที่ได้สำรองไว้มีความถูกต้องครบถ้วนและใช้งานได้

5.4 ต้องมีแผนฉุกเฉินเพื่อให้สามารถกู้ระบบคอมพิวเตอร์หรือจัดหาระบบคอมพิวเตอร์มาทดแทนได้โดยเร็ว เพื่อให้เกิดความเสียหายน้อยที่สุด โดยต้องทดสอบการปฏิบัติตามแผนฉุกเฉินอย่างน้อยปีละ 1 ครั้ง ในลักษณะการจำลองสถานการณ์จริง เพื่อให้มั่นใจได้ว่าสามารถนำไปใช้ได้จริงในทางปฏิบัติ และต้องมีการบันทึกผลการทดสอบไว้ด้วย

6. **การใช้งานระบบเทคโนโลยีสารสนเทศ**

แผนกเทคโนโลยีสารสนเทศจะกำหนดบัญชีผู้ใช้งานของระบบเทคโนโลยีสารสนเทศ โดยพนักงานของบริษัทจะได้รับบัญชีผู้ใช้งานตามสิทธิการใช้งานระบบต่างๆตามที่ได้รับมอบหมายจากหัวหน้างาน หรือหากมีการเปลี่ยนแปลงสิทธิการใช้งาน ไม่ว่าจะเป็นการโยกย้าย การเปลี่ยนแปลงผู้ใช้งาน การยกเลิกหรือลาออกของผู้ใช้งาน จะต้องได้รับการอนุมัติจากหัวหน้าระดับสูงสุดในสายงานเป็นลายลักษณ์อักษร

ทั้งนี้ การใช้งานระบบเทคโนโลยีสารสนเทศของบริษัทจะต้องไม่ขัดต่อหลักกฎหมาย พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล และกฎหมายอื่นๆ ที่เกี่ยวข้องโดยเด็ดขาด เช่น การนำข้อมูลเท็จ ภาพลามกอนาจาร หรือก่อให้เกิดความเสียหายต่อความมั่นคงของประเทศเข้าสู่ระบบคอมพิวเตอร์ การเข้าถึงระบบคอมพิวเตอร์ของบุคคล หรือองค์กรอื่นโดยไม่ได้รับอนุญาต การเผยแพร่ข้อความหมิ่นประมาทต่อบุคคลอื่น

การนำภาพบุคคลอื่นมาตัดต่อ ดัดแปลงซึ่งก่อให้เกิดความเสียหาย การเผยแพร่ข้อมูลของบุคคลอื่นโดยไม่ได้รับอนุญาต เป็นต้น ซึ่งอาจส่งผลให้บริษัทเสื่อมเสียชื่อเสียงได้ โดยให้จัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ไม่น้อยกว่า 90 วัน นับตั้งแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์

7. การกำกับดูแลและทบทวนนโยบาย

กำหนดให้มีการทบทวนนโยบาย และแนวปฏิบัติอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าหลักการของนโยบายนี้สอดคล้องกับบริบทของบริษัท หรือเมื่อมีการเปลี่ยนแปลงด้านกฎหมายเทคโนโลยี หรือภัยคุกคามที่เกี่ยวข้อง

8. การบังคับใช้

ผู้ใช้งานระบบคอมพิวเตอร์ทุกคน ต้องปฏิบัติตามนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศฉบับนี้อย่างเคร่งครัด หากตรวจสอบพบว่าผู้ใช้งานระบบงานต่างๆ กระทำผิดข้อใดข้อหนึ่งตามนโยบายฉบับนี้ บริษัทจะลงโทษตามระเบียบของบริษัททันที และหากการกระทำนั้นทำให้บริษัทได้รับความเสียหาย หรือเสียชื่อเสียง บริษัทจะดำเนินคดีตามกฎหมาย

นโยบายนี้มีผลบังคับใช้ตั้งแต่วันที่ 26 กุมภาพันธ์ 2569

ลงชื่อ .....

(นายชัย จรุงธนาภิบาล)

ประธานกรรมการ