นโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

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

บริษัทฯ และบริษัทย่อยได้จัดทำนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยมีวัตถุประสงค์เพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ เพื่อเป็นข้อกำหนดในการใช้งานคอมพิวเตอร์ภายในบริษัทฯ และบริษัทย่อย และเพื่อสร้างวัฒนธรรมที่ยอมรับเชื่อใจและซื่อสัตย์เพื่อป้องกันพนักงาน ลูกค้า บริษัทฯ และบริษัทย่อย ในการกระทำที่คุกคาม ผิดกฎหมาย หรือสร้างความเสียหายจากบุคคล หรือกลุ่มบุคคลใดๆ ไม่ว่าจะตั้งใจหรือไม่ตั้งใจ ให้แก่บริษัทฯ และบริษัทย่อย

1. วัตถุประสงค์

เพื่อจัดระเบียบการใช้งานรหัสผ่านระบบงานต่างๆ ของแผนกเทคโนโลยีสารสนเทศ ภายในองค์กรโดยคำนึงถึงความปลอดภัยของข้อมูลให้มีประสิทธิภาพและมีมาตรฐานในระดับเดียวกัน และให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ที่มีผลบังคับใช้ และกฎหมายประกอบอื่นๆ ที่เกี่ยวข้อง

2. ขอบข่าย

นโยบายฯ นี้ มีขอบข่ายบังคับใช้กับผู้ใช้งานคอมพิวเตอร์ทุกคน ที่เป็นกรรมการ ผู้บริหาร และพนักงานทุกระดับของบริษัทฯ และบริษัทย่อย

3. หน้าที่และความรับผิดชอบในสายงานเทคโนโลยีสารสนเทศ

3.1 Cluster IT Manager หรือผู้จัดการภาคแผนกเทคโนโลยีสารสนเทศ มีหน้าที่ บริหารและควบคุมระบบเทคโนโลยีสารสนเทศภายในบริษัทฯ และบริษัทย่อยทั้งหมด

3.2 IT Manager หรือผู้จัดการแผนกเทคโนโลยีสารสนเทศ มีหน้าที่ วิเคราะห์ วางแผน และพัฒนาหรือออกแบบระบบเทคโนโลยีสารสนเทศทั้งหมด รวมถึงกำหนดนโยบายและจัดทำงบประมาณประจำปีภายในบริษัทฯ และบริษัทย่อย

3.3 Assistant IT Manager หรือผู้ช่วยผู้จัดการแผนกเทคโนโลยีสารสนเทศ มีหน้าที่ รับผิดชอบในส่วนงานที่ได้รับมอบหมาย เพื่อนำมาปรับปรุงแก้ไขและพัฒนาเทคโนโลยีสารสนเทศทั้งหมด และรายงานถึงผู้จัดการฝ่ายเทคโนโลยีสารสนเทศโดยตรง

3.4 IT Supervisor หรือหัวหน้างานแผนกเทคโนโลยีสารสนเทศ มีหน้าที่ วิเคราะห์การแก้ไขปัญหาเบื้องต้น ตรวจเช็คความเรียบร้อยของระบบให้อยู่ในสภาพพร้อมใช้งานอยู่ตลอดเวลา

3.5 IT Officer/IT Admin หรือเจ้าหน้าที่ดูแลแผนกเทคโนโลยีสารสนเทศ มีหน้าที่ดูแลรับผิดชอบ จัดการ แก้ไข ซ่อมแซม บำรุงรักษาเครื่องใช้อุปกรณ์คอมพิวเตอร์ ตลอดจน Software และ Hardware ของบริษัทฯ และบริษัทย่อยให้อยู่ในสภาพที่ดี และพร้อมใช้งานอยู่เสมอ

4. การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย

4.1 อุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น เครื่องแม่ข่าย อุปกรณ์เครือข่าย จะต้องถูกเก็บไว้ในศูนย์คอมพิวเตอร์หรือพื้นที่หวงห้าม ที่มีการจำกัดสิทธิการเข้าออกศูนย์คอมพิวเตอร์ให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้อง เช่น ผู้จัดการแผนกเทคโนโลยีสารสนเทศ (IT Manager) ผู้ช่วยผู้จัดการแผนกเทคโนโลยีสารสนเทศ (Assistant IT Manager) เป็นต้น บุคคลที่ไม่มีหน้าที่เกี่ยวข้องซึ่งอาจมีความจำเป็นต้องเข้าออกศูนย์คอมพิวเตอร์ในบางครั้ง ต้องมีการควบคุมอย่างรัดกุม เช่น กำหนดให้มีเจ้าหน้าที่ควบคุมดูแลการเข้าออกและปฏิบัติตามระเบียบขั้นตอนอย่างเคร่งครัด

4.2 บริษัทฯ และบริษัทย่อยจะจัดให้มีระบบเก็บบันทึกการเข้าออกศูนย์คอมพิวเตอร์ โดยบันทึกดังกล่าวต้องมีรายละเอียดเกี่ยวกับตัวบุคคล และเวลาผ่านเข้าออก และควรมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ

5. รหัสผ่าน

5.1 รหัสผ่าน (password) หมายถึง สายอักขระหรือคำที่เป็นความลับ ที่ใช้สำหรับยืนยันตัวตน พิสูจน์ความเป็นเจ้าของหรือเข้าถึงแหล่งข้อมูล รหัสผ่านต้องเก็บเป็นความลับและห้ามเผยแพร่ให้บุคคลอื่นเพื่อให้คนอื่นเข้าถึงได้ เนื่องมาจากความปลอดภัยของข้อมูล เช่น สิทธิบัตร ลิขสิทธิ์ ความลับทางการตลาด กฎหมาย ฯลฯ

5.2 หากผู้ใช้งานที่ใช้รหัสผ่านระบบงานต่างๆ ไม่เข้าใจหรือไม่มั่นใจวิธีการใช้งานในทุกกรณี ให้ติดต่อแผนกเทคโนโลยีสารสนเทศเท่านั้น

5.3 ในการใช้งานระบบงานต่างๆ ในครั้งแรก หลังจากที่มีการร้องขอทำการเปลี่ยนรหัสผ่าน หรือหากไม่มั่นใจว่าผู้ใช้งานรายอื่นทราบรหัสผ่าน ผู้ใช้งานมีหน้าที่เปลี่ยนรหัสผ่านทันทีเพื่อความปลอดภัยของข้อมูล

5.4 การตั้งรหัสผ่านระบบงานต่างๆ ผู้ใช้งานต้องปฏิบัติตามข้อกำหนดดังนี้

5.4.1 ควรกำหนดให้รหัสผ่านมีความยาวขั้นต่ำอย่างน้อย 6 ตัวอักษร

5.4.2 รหัสผ่านควรประกอบด้วย อักขระต่างๆ ดังนี้

5.4.2.1 มีตัวอักษรตัวใหญ่ ได้แก่ A, B, C,...Z

5.4.2.2 มีตัวอักษรตัวเล็ก ได้แก่ a, b, c,...z

5.4.2.3 มีตัวเลขอารบิค ได้แก่ 0, 1, 2,...9

5.4.2.4 มีอักขระพิเศษ ได้แก่ !, @, #, $, &, *, \, _, -

5.4.3 ในการเปลี่ยนรหัสผ่านแต่ละครั้ง ไม่ควรกำหนดรหัสผ่านใหม่ให้ซ้ำของเดิมย้อนหลังอย่างน้อย 3 รหัสผ่านย้อนหลัง

5.4.4 ไม่ควรกำหนดรหัสผ่านอย่างเป็นแบบแผน เช่น "abcdef" "aaaaaa" "123456" เป็นต้น

5.4.5 ไม่ควรกำหนดรหัสผ่านเป็นคำศัพท์ที่อยู่ในพจนานุกรม

5.5 ผู้ใช้งานต้องไม่จดหรือแปะรหัสผ่านบริเวณที่ไม่ปลอดภัย เช่น Post-It บนหน้าจอคอมพิวเตอร์ เป็นต้น

5.6 หากไม่ได้อยู่ที่เครื่องคอมพิวเตอร์ผู้ใช้งานต้องทำการล็อคหน้าจอเพื่อไม่ให้บุคคลอื่นใช้งานได้และผู้ใช้งานมีหน้าที่ออกจากระบบ (Logoff) เมื่อไม่ได้ใช้งานระบบนั้นๆ แล้ว

5.7 หากผู้ใช้งานเข้ารหัสผ่าน ผิดต่อเนื่องเกิน 5 ครั้ง ระบบจะทำการ Lock User ทันที ผู้ใช้งานจะต้องทำการร้องขอเพื่อปลด Lock ระบบ

5.8 รหัสผ่านของระบบงานต่างๆ (System-Level Passwords) รหัสผ่านของผู้ใช้งานระบบงานต่างๆ (User-Level Passwords) ต้องทำการเปลี่ยนรหัสผ่านทุกๆ 90 วัน

5.9 ผู้ใช้งานจากภายนอก (Remote User) หรือ ผู้ใช้งานชั่วคราว (Guest) ต้องทำการร้องขอต่อแผนกเทคโนโลยีสารสนเทศ เพื่อเปิดใช้งาน โดยรหัสผ่านจะเป็นลักษณะใช้งานได้ครั้งเดียว

6. มาตรการการรักษาข้อมูล

6.1 บริษัทฯ และบริษัทย่อยจะกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลแต่ละประเภทชั้นความลับ และวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลให้สอดคล้องกับความสำคัญของข้อมูลประเภทต่างๆ

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

6.3 บริษัทฯ และบริษัทย่อยจะมีมาตรการรักษาความปลอดภัยข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของบริษัทฯ และบริษัทย่อยเช่น ส่งซ่อม หรือทำลายข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

6.5 การป้องกันไวรัส จะต้องมีมาตรการป้องกันไวรัสที่มีประสิทธิภาพและปรับปรุงให้ทันสมัยอยู่เสมอสำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ของผู้ใช้งานที่เชื่อมต่อกับระบบเครือข่ายทุกเครื่อง เช่น ติดตั้งซอฟต์แวร์ป้องกันไวรัส

7. การสำรองข้อมูลและระบบคอมพิวเตอร์ (Backup)

7.1 บริษัทฯ และบริษัทย่อยต้องสำรองข้อมูลสำคัญทางธุรกิจ รวมถึงโปรแกรมระบบปฏิบัติการ (Operating System) โปรแกรมระบบงานคอมพิวเตอร์ (Application System) และชุดคำสั่งที่ใช้ทำงานให้ครบถ้วน ให้สามารถพร้อมใช้งานได้อย่างต่อเนื่อง โดยต้องจัดเก็บสื่อบันทึกข้อมูลสำรอง พร้อมทั้งสำเนาขั้นตอนหรือวิธีปฏิบัติต่างๆ ไว้นอกสถานที่ เพื่อความปลอดภัยในกรณีที่สถานที่ปฏิบัติงานได้รับความเสียหาย โดยสถานที่ดังกล่าวต้องจัดให้มีระบบควบคุมการเข้าออกและระบบป้องกันความเสียหายดังกล่าว

7.2 ในกรณีที่จำเป็นต้องจัดเก็บข้อมูลเป็นระยะเวลานาน บริษัทฯ ต้องคำนึงถึงวิธีการนำข้อมูลกลับมาใช้งานในอนาคต เช่น ถ้าจัดเก็บข้อมูลในสื่อบันทึกประเภทใด ก็ต้องมีการเก็บอุปกรณ์และซอฟท์แวร์ที่เกี่ยวข้องสำหรับใช้อ่านสื่อบันทึกประเภทนั้นไว้ด้วยเช่นกัน

7.3 ต้องทดสอบข้อมูลสำรองอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าข้อมูล รวมทั้งโปรแกรมระบบต่างๆ ที่ได้สำรองไว้ มีความถูกต้องครบถ้วนและใช้งานได้

7.4 ต้องมีแผนฉุกเฉินเพื่อให้สามารถกู้ระบบคอมพิวเตอร์หรือจัดหาระบบคอมพิวเตอร์มาทดแทนได้โดยเร็วเพื่อให้เกิดความเสียหายน้อยที่สุด โดยต้องทดสอบการปฏิบัติตามแผนฉุกเฉินอย่างน้อยปีละ 1 ครั้ง ในลักษณะการจำลองสถานการณ์จริง เพื่อให้มั่นใจได้ว่าสามารถนำไปใช้ได้จริงในทางปฏิบัติ และต้องมีการบันทึกผลการทดสอบไว้ด้วย

โดยแผนฉุกเฉินต้องมีรายละเอียด ดังนี้

7.4.1 จัดลำดับความสำคัญของระบบงาน ความสัมพันธ์ของแต่ละระบบงาน และระยะเวลาในการกู้แต่ละระบบงาน

7.4.2 กำหนดสถานการณ์หรือลำดับความรุนแรงของปัญหา

7.4.3 ขั้นตอนการแก้ไขปัญหาโดยละเอียดในแต่ละสถานการณ์

7.4.4 กำหนดเจ้าหน้าที่รับผิดชอบ และผู้มีอำนาจในการตัดสินใจ รวมทั้งต้องมีรายชื่อและเบอร์โทรศัพท์ของบุคคลที่เกี่ยวข้องทั้งหมด

7.4.5 รายละเอียดของอุปกรณ์ที่จำเป็นต้องใช้ในกรณีฉุกเฉินของแต่ละระบบงาน เช่น รุ่นของเครื่องคอมพิวเตอร์ คุณลักษณะ ของเครื่องคอมพิวเตอร์ (Specification) ขั้นต่ำ ค่า Configuration และอุปกรณ์เครือข่าย เป็นต้น

7.4.6 ในกรณีที่บริษัทฯ และบริษัทย่อย มีศูนย์คอมพิวเตอร์สำรอง ก็ต้องระบุรายละเอียดเกี่ยวกับศูนย์คอมพิวเตอร์สำรองให้ชัดเจน เช่น สถานที่ตั้ง แผนที่ เป็นต้น

7.4.7 ต้องปรับปรุงแผนฉุกเฉินให้เป็นปัจจุบันอยู่เสมอ และเก็บแผนฉุกเฉินไว้นอกสถานที่

8. การให้บริการเครือข่ายคอมพิวเตอร์

แผนกเทคโนโลยีสารสนเทศ จะทำการให้บริการรหัสผ่านระบบงานต่างๆ สำหรับผู้ใช้งานแต่ละรายโดยยึดหลักนโยบายการให้บริการต่างๆ ของแผนกเทคโนโลยีสารสนเทศในฉบับนี้ ทั้งนี้พนักงานใหม่ของบริษัทฯ และบริษัทย่อย จะได้รับรหัสผ่านต่างๆ ตามสิทธิและนโยบายพนักงานใหม่ที่จำเป็นต้องใช้รหัสผ่านหรือนอกเหนือจากที่ระบุในนโยบายระบบงานต่างๆ จะต้องร้องขอผ่านใบคำร้อง (Request form) พร้อมระบุความจำเป็น เหตุผลการใช้งาน และได้รับอนุมัติจากผู้บริหารระดับสูงสุดในสายงาน จึงจะมีสิทธิ์รับรหัสผ่านนั้นได้

9. **นโยบายการให้บริการและคำร้องขอ**

9.1 พนักงานหรือหน่วยงาน ที่จำเป็นต้องเปลี่ยนรหัสผ่านระบบงานต่างๆ ไม่ว่าจะเป็นสาเหตุจากการลืมรหัส การโยกย้ายหรือเปลี่ยนแปลงผู้ใช้งาน การยกเลิกหรือลาออกของผู้ใช้งาน และนอกเหนือจากที่ระบุในนโยบายฉบับนี้ จะต้องร้องขอผ่านใบคำร้อง (Request form) พร้อมระบุความจำเป็น เหตุผลการใช้งาน และได้รับอนุมัติจากผู้บริหารระดับสูงสุดในสายงาน จึงจะมีสิทธิ์ในการเปลี่ยนแปลงหรือลบรหัสผ่านนั้นได้

9.2 การร้องขอในทุกเรื่องไม่ว่าจะเป็น การขอใหม่ การแก้ปัญหาหรือดูแลรักษาในทุกระบบของแผนกเทคโนโลยีสารสนเทศ สามารถทำได้ตามข้อตกลงด้านล่างนี้เท่านั้น นอกเหนือจากวิธีดังกล่าวแผนกเทคโนโลยีสารสนเทศ ไม่รับประกันการร้องขอหรือปัญหาจะได้รับการดำเนินการหรือรับรู้และแก้ไขในเวลาที่สมควร การร้องขอสามารถทำได้โดยวิธีดังต่อไปนี้

9.2.1 ใบร้องขอ (Request form) ซึ่งจะมีการเผยแพร่ในข้อมูลส่วนกลางหรือสามารถขอได้จากแผนก เทคโนโลยีสารสนเทศ

9.2.2 ส่งจดหมายอีเล็กทรอนิกส์ (E-mail) พร้อมแนบใบร้องขอมายังแผนกเทคโนโลยีสารสนเทศ

9.3 คำขอมีอยู่ 2 ประเภท คือ

9.3.1 การร้องขอ (Request) หมายถึง การขอใหม่ การปรับปรุง โดยจะมีผลกระทบต่อระบบหรือเปลี่ยนแปลงระบบหรือมีค่าใช้จ่าย

9.3.2 ปัญหา (Incident) สามารถแจ้งได้โดยตรงจากผู้ใช้งานทุกคน

10. **การบังคับ**

ผู้ใช้งานระบบคอมพิวเตอร์ทุกคน ต้องปฏิบัติตามนโยบายระบบงานสายเทคโนโลยีฉบับนี้อย่างเคร่งครัด หากตรวจสอบพบว่าผู้ใช้งานระบบงานต่างๆ กระทำผิดข้อใดข้อหนึ่งตามนโยบายฉบับนี้ บริษัทฯ และบริษัทย่อยจะลงโทษขั้นสูงสุดตามระเบียบของบริษัทฯ และบริษัทย่อยทันที และหากการกระทำนั้นทำให้บริษัทฯ และบริษัทย่อยได้รับความเสียหาย หรือเสียชื่อเสียง บริษัทฯ และบริษัทย่อย จะดำเนินคดีตามกฎหมาย

นโยบายนี้มีผลบังคับใช้ตั้งแต่วันที่ 27 กันยายน 2561

อนุมัติโดย .....

(นายชัย จรุงธนาภิบาล)

ประธานคณะกรรมการ