

ประกาศคณะกรรมการบริษัท ราชพัฒนา เอ็นเนอร์ยี จำกัด (มหาชน)

ที่ 10/2567

เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

.....

เพื่อให้ระบบเทคโนโลยีสารสนเทศของ บริษัท ราชพัฒนา เอ็นเนอร์ยี จำกัด (มหาชน) มีความมั่นคงปลอดภัย สามารถดำเนินงานได้อย่างต่อเนื่องและมีประสิทธิภาพ มีมาตรการในการป้องกันปัญหาอันอาจเกิดขึ้นจากการถูกภาวะคุกคามต่าง ๆ และจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่พึงประสงค์ ซึ่งอาจก่อความเสียหายแก่บริษัทในภาพรวม และเป็นการป้องกันการกระทำความผิดตามกฎหมายและระเบียบอื่น ๆ ที่เกี่ยวข้อง คณะกรรมการบริษัท ราชพัฒนา เอ็นเนอร์ยี จำกัด (มหาชน) ครั้งที่ 5/2567 วันที่ 26 มิถุนายน 2567 มีมติกำหนดนโยบายการคุ้มครองข้อมูลส่วนบุคคล ของบริษัท และบริษัทย่อย และยกเลิกประกาศนโยบายรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ลงวันที่ 20 มิถุนายน 2565 ดังนี้

ข้อ 1 ในประกาศนี้

“ผู้ใช้งาน” หมายถึง ลูกจ้าง พนักงานประจำ พนักงานชั่วคราว ที่ปฏิบัติงานเกี่ยวกับระบบสารสนเทศของบริษัท และบุคคลภายนอกที่เข้ามาใช้บริการระบบสารสนเทศของบริษัท รวมถึงหน่วยงานภายนอก ที่ได้รับอนุญาตให้ใช้งานระบบสารสนเทศของบริษัท

“สิทธิของผู้ใช้งาน” หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใด เพื่อการเข้าถึง หรือเข้าใช้งานระบบสารสนเทศ และสินทรัพย์ที่เกี่ยวข้องกับระบบสารสนเทศ

“สินทรัพย์” หมายถึง ข้อมูล อุปกรณ์ฮาร์ดแวร์ ซอฟต์แวร์ต่าง ๆ และทรัพย์สินต่าง ๆ ที่มีไว้เพื่อการปฏิบัติงานทางด้านระบบสารสนเทศของบริษัท

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายถึง การอนุญาต การกำหนดสิทธิการเข้าถึงหรือการใช้งานอุปกรณ์คอมพิวเตอร์ ระบบเครือข่าย และระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ

“ความมั่นคงปลอดภัยด้านเทคโนโลยีและสารสนเทศ” หมายถึง การดำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของระบบสารสนเทศของบริษัท ทั้งนี้รวมถึงคุณสมบัติในด้านความถูกต้องแท้จริง (authenticity) ความรับผิดชอบ (accountability) การห้ามปฏิเสธความรับผิดชอบ (non-repudiation) และความน่าเชื่อถือ (reliability) ของระบบสารสนเทศของบริษัท

“เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายถึง เหตุการณ์ที่เกิดขึ้นกับระบบเครือข่าย และระบบสารสนเทศ หรือเหตุการณ์ที่สงสัยว่าจะเป็จุดอ่อน หรืออาจสร้างความเสียหายได้ในที่สุด ซึ่งอาจส่งผลให้เกิดการหยุดชะงักต่อกระบวนการ หรือขั้นตอนการปฏิบัติงานทางด้านระบบเครือข่าย และระบบสารสนเทศของบริษัท ซึ่งแสดงให้เห็นความเป็นไปได้ที่เกิดจากการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” หมายถึง เหตุบกพร่องหรือเหตุละเมิดด้านความมั่นคงปลอดภัย ซึ่งอาจทำให้ระบบสารสนเทศของบริษัท สูญเสียการปฏิบัติงาน รวมถึง

การให้บริการต่าง ๆ แต่เพียงบางส่วนหรือบางส่วนหรือทั้งหมดจากการถูกบุกรุก หรือโจมตีทางช่องโหว่ และ ความมั่นคงปลอดภัยถูกคุกคามจากภัยคุกคามในรูปแบบต่าง ๆ

“อุปกรณ์คอมพิวเตอร์” หมายถึง อุปกรณ์ หรือชุดอุปกรณ์ของคอมพิวเตอร์ โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ ทำหน้าที่ประมวลผลข้อมูลอัตโนมัติ

“ระบบสารสนเทศ” หมายถึง ข้อมูลของบริษัทที่นำเอาเทคโนโลยีของระบบคอมพิวเตอร์และระบบ เครือข่ายมาช่วยในการสร้างสารสนเทศของบริษัท และสามารถนำสารสนเทศนั้นมาใช้ในการวางแผน การบริหาร การพัฒนา การควบคุม สนับสนุนในภารกิจของบริษัท รวมทั้งนโยบายหรือแนวปฏิบัติในการใช้ อุปกรณ์เหล่านี้

“ผู้ดูแลระบบ” หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้จัดการส่วนธุรการและเทคโนโลยี สารสนเทศให้มีหน้าที่รับผิดชอบในการเป็นผู้ดูแลบริหารจัดการและรักษาสินทรัพย์ ระบบเครือข่าย คอมพิวเตอร์ และสารสนเทศต่างๆ ของบริษัท

“หน่วยงานภายนอก” หมายถึง หน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึง และการใช้ งานข้อมูลหรือทรัพย์สินต่าง ๆ ของบริษัท โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้อง รับผิดชอบในการรักษาความลับข้อมูล

ข้อ 2 ให้มีนโยบายการควบคุมการเข้าถึงและควบคุมการใช้อุปกรณ์คอมพิวเตอร์ ระบบปฏิบัติการ ระบบเครือข่าย ระบบสารสนเทศของบริษัท โดยผู้ใช้งานที่มีการปฏิบัติงานเกี่ยวกับระบบสารสนเทศของบริษัท ต้องได้รับการพิสูจน์ตัวตนการเข้าใช้งานก่อนทุกครั้ง และผู้ใช้งานต้องได้รับการพิจารณาอนุมัติตามขั้นตอนที่ ระบุไว้อย่างเคร่งครัดและต้องมีการจำกัดสิทธิการเข้าถึงระบบของผู้ใช้งานให้อยู่ในระดับที่เหมาะสมต่อความ จำเป็นในการทำงานตามอำนาจหน้าที่ เพื่อให้เกิดความเชื่อมั่นและป้องกันความเสียหายอันเกิดจากการกระทำ ที่ไม่ถูกต้อง และได้รับสิทธิในการเข้าถึงระบบตามอำนาจหน้าที่ความรับผิดชอบเท่านั้น โดยให้เป็นไปตามแนว ปฏิบัติในการรักษามั่นคงปลอดภัยด้านสารสนเทศของบริษัทท้ายประกาศนี้

ข้อ 3 ผู้ดูแลระบบต้องจัดให้มีการควบคุมการเข้าถึงระบบสารสนเทศของบริษัท โดยกำหนดให้ ผู้ใช้งานต้องได้รับการพิสูจน์ตัวตนของผู้ใช้งานก่อนทุกครั้ง และผู้ใช้งานต้องได้รับพิจารณาอนุญาตให้ใช้งาน ระบบสารสนเทศเท่าที่จำเป็นครอบคลุมในทุกขั้นตอน ตั้งแต่การกำหนดวิธีการลงทะเบียนผู้ใช้งาน การ บริหารจัดการรหัสผ่านผู้ใช้งาน การบริหารจัดการสิทธิการใช้งานระบบสารสนเทศ ให้มีความมั่นคงปลอดภัย และกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึงระบบสารสนเทศ ประเภทข้อมูล ลำดับความสำคัญ และ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน

ข้อ 4 ผู้ดูแลระบบต้องบริหารจัดการอุปกรณ์คอมพิวเตอร์ของบริษัททั้งหมด บริหารจัดการการเข้าถึง และเข้าใช้อุปกรณ์คอมพิวเตอร์ ควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์ ป้องกันอุปกรณ์คอมพิวเตอร์ที่ไม่มี ผู้ปฏิบัติงาน ดูแลกำหนดมาตรการทำลายสื่อบันทึกข้อมูล และข้อมูลอิเล็กทรอนิกส์ กำหนดมาตรการควบคุม การเข้า - ออกห้องควบคุมระบบคอมพิวเตอร์แม่ข่าย บริหารจัดการการเข้าถึงเครือข่าย ควบคุมป้องกันไม่ให้ บุคคลที่ไม่มีอำนาจที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึงระบบเครือข่ายที่จะทำให้เกิดความเสียหายต่อข้อมูล และระบบสารสนเทศของบริษัทได้ โดยมีการกำหนดกระบวนการควบคุมการเข้าใช้งานเครือข่ายที่แตกต่างกัน

ของกลุ่มเครือข่ายต่าง ๆ ตามการแบ่งแยกเครือข่าย บริหารจัดการการเข้าถึงระบบสารสนเทศ กำหนด มาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาตให้เข้าถึงระบบสารสนเทศ และป้องกันการบุกรุกผ่านระบบเครือข่าย จากโปรแกรมชุดคำสั่งที่ไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบสารสนเทศ ให้หยุดชะงัก และสามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศของบริษัทได้

ข้อ 5 ผู้ใช้งานต้องตระหนักเรื่องความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและต้องปฏิบัติตาม แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของบริษัทท้ายประกาศนี้อย่างเคร่งครัด โดยต้อง ทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้สิทธิ์ฯ หรือเข้าถึงระบบสารสนเทศของบริษัท และต้องเข้าใจถึงสิทธิ การเข้าถึงระบบของผู้ใช้งานต่อความจำเป็นในการทำงานตามอำนาจหน้าที่ความรับผิดชอบสำหรับผู้ใช้งานเอง เท่านั้น

ข้อ 6 ให้มีนโยบายระบบสำรองข้อมูลสารสนเทศและแผนเตรียมความพร้อมกรณีฉุกเฉิน เพื่อให้ ผู้ดูแลระบบ สามารถดำเนินการสำรองข้อมูลได้อย่างถูกต้องและสามารถกู้คืนระบบสารสนเทศได้ตาม ระยะเวลาที่กำหนด รวมทั้งจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับ ระบบสารสนเทศ เพื่อให้ระบบสารสนเทศของบริษัทบริการได้อย่างต่อเนื่อง รวมทั้งปรับปรุงแก้ไขให้ทันสมัย อยู่เสมอ โดยให้เป็นไปตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัท ท้ายประกาศนี้

ข้อ 7 ให้มีนโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ อย่างน้อย ปีละ 1 ครั้ง เพื่อป้องกันและลดระดับความเสี่ยงที่อาจเกิดขึ้นกับระบบสารสนเทศของบริษัท โดยให้เป็นไป ตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทท้ายประกาศนี้

ข้อ 8 ให้ผู้จัดการส่วนเทคโนโลยีสารสนเทศ มีหน้าที่ดูแล บริหารจัดการ และรักษาสิทธิ์ระบบ เครือข่ายคอมพิวเตอร์ และระบบสารสนเทศต่าง ๆ ของบริษัท พร้อมทั้งแต่งตั้งผู้ดูแลระบบให้มีหน้าที่ รับผิดชอบในการเป็นผู้ดูแล บริหารจัดการ และรักษาสิทธิ์ ระบบเครือข่ายคอมพิวเตอร์ และระบบ สารสนเทศต่าง ๆ ของบริษัท ให้สอดคล้องตามนโยบายนี้

ข้อ 9 นโยบายในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทท้ายประกาศนี้ ให้มีการทบทวนปรับปรุง ให้มีความทันสมัยอยู่เสมอ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อระบบสารสนเทศมีการเปลี่ยนแปลงที่สำคัญ

ข้อ 10 กรณีระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่บริษัท หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเอียด หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการ รักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ทั้งนี้ ให้ผู้จัดการส่วนธุรการและเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ประกาศ ณ วันที่ 26 เดือน มิถุนายน พ.ศ. 2567

สุจริต ปัจฉิมนันท์

(นายสุจริต ปัจฉิมนันท์)

ประธานกรรมการบริษัท