นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

เพื่อให้ระบบเทคโนโลยีสารสนเทศของ บริษัท สหโคเจน (ชลบุรี) จำกัด (มหาชน) และบริษัทย่อย มีความมั่นคงปลอดภัย สามารถดำเนินงานได้อย่างต่อเนื่องและมีประสิทธิภาพ มีมาตรการในการป้องกันปัญหาอันอาจเกิดขึ้นจากการถูกภาวะคุกคามต่าง ๆ และจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่พึงประสงค์ ซึ่งอาจก่อความเสียหายแก่บริษัทในภาพรวม และเป็นการป้องกันการกระทำความผิดตามกฎหมายและระเบียบอื่น ๆ ที่เกี่ยวข้อง จึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ให้ทราบและถือปฏิบัติ ไว้ดังนี้

ข้อ 1 ในประกาศนี้

“ผู้ใช้งาน” หมายถึง ลูกจ้าง พนักงานประจำ พนักงานชั่วคราว ที่ปฏิบัติงานเกี่ยวกับระบบสารสนเทศของบริษัท และบุคคลภายนอกที่เข้ามาใช้บริการระบบสารสนเทศของบริษัท รวมถึงหน่วยงานภายนอก ที่ได้รับอนุญาตให้ใช้งานระบบสารสนเทศของบริษัท

“สิทธิของผู้ใช้งาน” หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใด เพื่อการเข้าถึง หรือเข้าใช้งานระบบสารสนเทศ และสินทรัพย์ที่เกี่ยวกับระบบสารสนเทศ

“สินทรัพย์” หมายถึง ข้อมูล อุปกรณ์ฮาร์ดแวร์ ซอฟต์แวร์ต่างๆ และทรัพย์สินต่างๆ ที่มีไว้เพื่อการปฏิงานทางด้านระบบสารสนเทศของบริษัท

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายถึง การอนุญาต การกำหนดสิทธิการเข้าถึงหรือการใช้งานอุปกรณ์คอมพิวเตอร์ ระบบเครือข่าย และระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ

“ความมั่นคงปลอดภัยด้านเทคโนโลยีและสารสนเทศ” หมายถึง การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของระบบสารสนเทศของบริษัท ทั้งนี้รวมถึงคุณสมบัติในด้านความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability) ของระบบสารสนเทศของบริษัท

“เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายถึง เหตุการณ์ที่เกิดขึ้นกับระบบเครือข่าย และระบบสารสนเทศ หรือเหตุการณ์ที่สงสัยว่าจะเป็นจุดอ่อน หรืออาจสร้างความเสียหายได้ในที่สุด ซึ่งอาจส่งผลให้เกิดการหยุดชะงักต่อกระบวนการ หรือขั้นตอนการปฏิบัติงานทางด้านระบบเครือข่าย และระบบสารสนเทศ ของบริษัท ซึ่งแสดงให้เห็นความเป็นไปได้ที่เกิดจากการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” หมายถึงเหตุบกพร่องหรือเหตุละเมิดด้านความมั่นคงปลอดภัย ซึ่งอาจทำให้ระบบสารสนเทศของบริษัท สูญเสียการปฏิบัติงาน รวมถึงการให้บริการต่างๆ แต่เพียงบางส่วนหรือบางส่วนหรือทั้งหมดจากการถูกบุกรุก หรือโจมตีทางช่องโหว่ และความมั่นคงปลอดภัยถูกคุกคามจากภัยคุกคามในรูปแบบต่างๆ

“อุปกรณ์คอมพิวเตอร์” หมายถึง อุปกรณ์ หรือชุดอุปกรณ์ของคอมพิวเตอร์ โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดและแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ ทำหน้าที่ประมวลผลข้อมูลอัตโนมัติ

“ระบบสารสนเทศ” หมายถึง ข้อมูลของบริษัทที่นำเอาเทคโนโลยีของระบบคอมพิวเตอร์และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศของบริษัท และสามารถนำสารสนเทศนั้นมาใช้ในการวางแผน การบริหาร การพัฒนา การควบคุม สนับสนุนในภารกิจของบริษัท รวมทั้งนโยบายหรือแนวปฏิบัติในการใช้อุปกรณ์เหล่านี้

“ผู้ดูแลระบบ” หมายถึง เจ้าหน้าที่ได้รับมอบหมายจากผู้จัดการส่วนเทคโนโลยีสารสนเทศ ให้มีหน้าที่รับผิดชอบในการเป็นผู้ดูแล บริหารจัดการ และรักษาสินทรัพย์ ระบบเครือข่ายคอมพิวเตอร์ และสารสนเทศต่างๆ ของบริษัท

“หน่วยงานภายนอก” หมายถึง หน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึง และการใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของบริษัท โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับข้อมูล

ข้อ 2 ให้จัดทำแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เพื่อควบคุมการเข้าถึงและควบคุมการใช้อุปกรณ์คอมพิวเตอร์ ระบบปฏิบัติการระบบเครือข่าย ระบบสารสนเทศของบริษัท โดยผู้ใช้งานที่มีการปฏิบัติงานเกี่ยวกับระบบสารสนเทศของบริษัท ต้องได้รับการพิสูจน์ตัวตนการเข้าใช้งานก่อนทุกครั้ง และผู้ใช้งานต้องได้รับการพิจารณาอนุมัติตามขั้นตอนที่ระบุ

ไว้อย่างเคร่งครัด และต้องมีการจำกัดสิทธิการเข้าถึงระบบของผู้ใช้งานให้อยู่ในระดับที่เหมาะสมต่อความจำเป็นในการทำงานตามอำนาจหน้าที่ เพื่อให้เกิดความเชื่อมั่นและป้องกันความเสียหายอันเกิดจากการกระทำที่ไม่ถูกต้อง และได้รับสิทธิในการเข้าถึงระบบตามอำนาจหน้าที่ความรับผิดชอบเท่านั้น โดยให้เป็นไปตามแนวปฏิบัติในการรักษามั่นคงปลอดภัยด้านสารสนเทศของบริษัทท้ายประกาศนี้

ข้อ 3 ผู้ดูแลระบบต้องจัดให้มีการควบคุมการเข้าถึงระบบสารสนเทศของบริษัท โดยกำหนดให้ผู้ใช้งานต้องได้รับการพิสูจน์ตัวตนของผู้ใช้งานก่อนทุกครั้ง และผู้ใช้งานต้องได้รับพิจารณาอนุญาตให้ใช้งานระบบสารสนเทศเท่าที่จำเป็น ครอบคลุมในทุกขั้นตอน ตั้งแต่การกำหนดวิธีการลงทะเบียนผู้ใช้งาน การบริหารจัดการรหัสผ่านผู้ใช้งาน การบริหารจัดการสิทธิการใช้งานระบบสารสนเทศ ให้มีความมั่นคงปลอดภัย และกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึงระบบสารสนเทศ ประเภทข้อมูล ลำดับความสำคัญ และการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน

ข้อ 4 ผู้ดูแลระบบต้องบริหารจัดการอุปกรณ์คอมพิวเตอร์ของบริษัททั้งหมด บริหารจัดการการเข้าถึงและเข้าใช้อุปกรณ์คอมพิวเตอร์ ควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์ ป้องกันอุปกรณ์คอมพิวเตอร์ที่ไม่มีผู้ปฏิบัติงาน ดูแลกำหนดมาตรการทำลายสื่อบันทึกข้อมูล และข้อมูลอิเล็กทรอนิกส์ กำหนดมาตรการควบคุมการเข้า – ออกห้องควบคุมระบบคอมพิวเตอร์แม่ข่าย บริหารจัดการการเข้าถึงเครือข่าย ควบคุมป้องกันไม่ให้บุคคลที่ไม่มีอำนาจที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึงระบบเครือข่ายที่จะทำให้เกิดความเสียหายต่อข้อมูลและระบบสารสนเทศของบริษัทได้ โดยมีการกำหนดกระบวนการควบคุมการเข้าใช้งานเครือข่ายที่แตกต่างกันของกลุ่มเครือข่ายต่าง ๆ ตามการแบ่งแยกเครือข่าย บริหารจัดการการเข้าถึงระบบสารสนเทศ กำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาตให้เข้าถึงระบบสารสนเทศ และป้องกันการบุกรุกผ่านระบบเครือข่ายจากโปรแกรมชุดคำสั่งที่ไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบสารสนเทศให้หยุดชะงัก และสามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศของบริษัทได้

ข้อ 5 ผู้ใช้งานต้องตระหนักเรื่องความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและต้องปฏิบัติตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของบริษัทท้ายประกาศนี้อย่างเคร่งครัด โดยต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้สินทรัพย์ หรือเข้าถึงระบบสารสนเทศของบริษัท และต้องเข้าใจถึงสิทธิการเข้าถึงระบบของผู้ใช้งานต่อความจำเป็นในการทำงานตามอำนาจหน้าที่ความรับผิดชอบสำหรับผู้ใช้งานเองเท่านั้น

ข้อ 6 ให้มีคู่มือการสำรองข้อมูลสารสนเทศและแผนรองรับสถานการณ์ฉุกเฉินด้านไอที เพื่อให้ผู้ดูแลระบบ สามารถดำเนินการสำรองข้อมูลได้อย่างถูกต้องและสามารถกู้คืนระบบสารสนเทศได้ตามระยะเวลาที่กำหนด รวมทั้งจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบสารสนเทศ เพื่อให้ระบบสารสนเทศของบริษัทบริการได้อย่างต่อเนื่อง รวมทั้งปรับปรุงแก้ไขให้ทันสมัยอยู่เสมอ โดยให้เป็นไปตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทท้ายประกาศนี้

ข้อ 7 ให้มีการตรวจสอบคู่มือที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง เพื่อป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศของบริษัท โดยให้เป็นไปตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทท้ายประกาศนี้

ข้อ 8 ให้ผู้จัดการส่วนเทคโนโลยีสารสนเทศ มีหน้าที่ดูแล บริหารจัดการ และรักษาสินทรัพย์ระบบเครือข่ายคอมพิวเตอร์ และระบบสารสนเทศต่าง ๆ ของบริษัท พร้อมทั้งแต่งตั้งผู้ดูแลระบบให้มีหน้าที่รับผิดชอบในการเป็นผู้ดูแล บริหารจัดการ และรักษาสินทรัพย์ ระบบเครือข่ายคอมพิวเตอร์ และระบบสารสนเทศต่าง ๆ ของบริษัท ให้สอดคล้องตามนโยบายนี้

ข้อ 9 นโยบายในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทท้ายประกาศนี้ ให้มีการทบทวนปรับปรุงให้มีความทันสมัยอยู่เสมอ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อระบบสารสนเทศมีการเปลี่ยนแปลงที่สำคัญ

ข้อ 10 กรณีระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่บริษัท หรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ทั้งนี้ ให้ผู้จัดการส่วนเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อ 11 ทั้งนี้ ให้มีผลตั้งแต่วันที่ 20 มิถุนายน 2565 เป็นต้นไป และให้ยกเลิกประกาศนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ลงวันที่ 31 ตุลาคม 2562 โดยให้ใช้ประกาศฉบับนี้แทน

ประกาศ ณ วันที่ 20 มิถุนายน พ.ศ. 2565

(นายสุจริต ปัจฉิมนันท์)
ประธานกรรมการ