นโยบายด้านเทคโนโลยีสารสนเทศ
บริษัท สยามสตีลอินเตอร์เนชั่นแนล จำกัด(มหาชน)

เพื่อให้มั่นใจว่าการดำเนินการใดๆ ด้านเทคโนโลยีสารสนเทศของบริษัท สยามสตีลอินเตอร์เนชั่นแนล จำกัด(มหาชน) และบริษัทในเครือ มีความมั่นคงปลอดภัยและน่าเชื่อถือ ข้อมูลและสินทรัพย์สารสนเทศของบริษัทฯ ได้รับการดูแลรักษาอย่างเป็นระบบและเหมาะสม โดยคำนึงถึงความเสี่ยงจากภัยคุกคามด้านความมั่นคงไซเบอร์ที่อาจเกิดขึ้น และการใช้งานระบบสารสนเทศที่มีมาตรการรักษาความลับ ความถูกต้อง สมบูรณ์ และมีความพร้อมในการใช้งาน สอดคล้องกับข้อบังคับ กฎ ระเบียบ กฎหมายด้านความปลอดภัยสารสนเทศ บริษัทฯ จึงกำหนดนโยบายด้านเทคโนโลยีสารสนเทศ ดังนี้

นโยบายด้านเทคโนโลยีสารสนเทศ

บริษัทฯ จะ

- ดำเนินธุรกิจภายใต้หลักการกำกับดูแลกิจการที่ดี การดำเนินการด้านเทคโนโลยีของบริษัทฯ จะเป็นไปตามกฎหมายและกฎระเบียบที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ
- จะให้มีระบบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน
- จัดให้มีการควบคุมการเข้าถึงข้อมูลและระบบต่างๆ อย่างเหมาะสม และมีมาตรฐานความปลอดภัยที่เพียงพอ
- จัดให้มีแผนดำเนินการและมาตรการในการป้องกันและบรรเทาผลกระทบด้านความมั่นคงปลอดภัยทางไซเบอร์ โดยศึกษาถึงผลกระทบจากการประเมินความเสี่ยงแบบรอบด้าน
- ส่งเสริมให้ผู้บริหารและพนักงานมีความรู้ความเข้าใจในการใช้งานและกฎระเบียบต่างๆ ที่เกี่ยวกับเทคโนโลยีสารสนเทศ
- จัดให้มีการตรวจสอบการใช้งานระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ

แนวทางปฏิบัติ

1. การตรวจสอบและการประเมินความเสี่ยง

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศ จะต้องจัดให้มีการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและการควบคุมความเสี่ยงให้อยู่ในเกณฑ์ที่บริษัทฯ ยอมรับได้ เพื่อให้มั่นใจว่า การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทฯ ถูกจัดการอย่างเหมาะสม

2. การรักษาความปลอดภัยต่อทรัพย์สินสารสนเทศ

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศ ต้องกำหนดมาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ เพื่อควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของบริษัทฯ ให้เหมาะสมกับประเภทข้อมูล ลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ระดับชั้นการเข้าถึง เวลาและช่องทางที่เข้าถึงได้ รวมทั้งจัดให้มีการป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก และจากโปรแกรมที่ไม่พึงประสงค์ที่จะสร้างความเสียหายให้แก่ข้อมูลบริษัทฯ ดังต่อไปนี้

2.1 การจำแนกประเภททรัพย์สินสารสนเทศ ต้องกำหนดแนวทางการจัดการหมวดหมู่ของสินทรัพย์สารสนเทศ และจัดลำดับชั้นความลับให้สอดคล้องกับกฎหมายและข้อกำหนดที่เกี่ยวข้องกับบริษัทฯ

2.2 การจัดทำระบบสำรองและแผนรองรับกรณีเกิดเหตุฉุกเฉิน ต้องจัดทำระบบสารสนเทศสำรองที่เหมาะสมและอยู่ในสภาพพร้อมใช้งาน รวมทั้งจัดทำแผนรองรับกรณีเกิดเหตุฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง พร้อมทั้งต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลระบบสารสนเทศ และให้มีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และแผนรองรับกรณีเกิดเหตุฉุกเฉินอย่างสม่ำเสมอ

2.3 การควบคุมการเข้าถึงรหัสข้อมูล กำหนดให้มีแนวทางการเข้ารหัสลับข้อมูลให้มีความเหมาะสมกับความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลในแต่ละลำดับชั้นความลับที่กำหนดไว้ รวมทั้งติดตามให้มีการปฏิบัติให้เป็นไปตามนโยบายและวิธีการดังกล่าวเสมอ

2.4 การควบคุมดูแลบุคลากรผู้ปฏิบัติงาน หน่วยงานผู้ได้รับมอบหมายให้ดูแลระบบเทคโนโลยีสารสนเทศ ต้องดำเนินการดังนี้

(ก) การควบคุมการใช้งานของผู้ใช้งาน

- ต้องกำหนดให้ผู้ใช้งานเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศโดยการใส่รหัสผ่าน และเมื่อเสร็จสิ้นการใช้งานให้ออกจากระบบโดยทันที รวมถึงมีการล็อคหน้าจอเครื่องคอมพิวเตอร์หรืออุปกรณ์สำคัญเมื่อไม่ใช้งานหรือออกห่างจากเครื่องคอมพิวเตอร์ตามเวลาที่กำหนดอย่างเหมาะสม
- กำหนดให้มีมาตรการควบคุมความมั่นคงปลอดภัยของอุปกรณ์สื่อสารประเภทพกพา โดยพิจารณาความเสี่ยงที่มีการนำอุปกรณ์เข้ามาเชื่อมต่อกับเครือข่ายคอมพิวเตอร์ของบริษัทฯ รวมถึงกำหนดมาตรการควบคุมสำหรับการนำอุปกรณ์ออกไปใช้งานภายนอกบริษัทฯ
- การควบคุมการติดตั้งซอฟต์แวร์บนระบบงาน ต้องจัดทำขั้นตอนปฏิบัติงานและมาตรการควบคุมการติดตั้งซอฟต์แวร์บนระบบ เพื่อจำกัดการติดตั้งซอฟต์แวร์โดยผู้ใช้งานและป้องกันการติดตั้งซอฟต์แวร์ที่ไม่ได้รับอนุญาตให้ใช้งาน และกำหนดรายการซอฟต์แวร์มาตรฐาน ที่อนุญาตให้ติดตั้งบนเครื่องคอมพิวเตอร์ของบริษัทฯ อย่างเป็นลายลักษณ์อักษร และปรับปรุงให้เป็นปัจจุบันเสมอ รวมทั้งสื่อสารให้ผู้ใช้งานภายในบริษัทฯ รับทราบและปฏิบัติตาม
- ควบคุมดูแลมิให้ผู้ใช้งานข้อมูลสารสนเทศ และหรือข้อมูลทางอิเล็กทรอนิกส์อื่นๆ ในทางที่ไม่เหมาะสม ผิดศีลธรรมและอาจทำให้ระบบสารสนเทศและข้อมูลของบริษัทฯ ได้รับความเสียหาย
- ระบบเทคโนโลยีสารสนเทศที่ได้รับการพัฒนาขึ้นภายในบริษัทฯ ถือเป็นทรัพย์สินของบริษัทฯ ห้ามนำไปทำซ้ำ หรือดัดแปลงแก้ไข หรือกระทำการใดๆ เพื่อประโยชน์ส่วนตัวของผู้ใช้งานหรือผู้อื่น โดยไม่ได้รับอนุญาตจากบริษัทฯ

(ข) การควบคุมดูแลผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ (IT Outsourcing) จัดทำข้อกำหนดและกรอบการปฏิบัติงานของผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ มีความมั่นคงปลอดภัย

2.5 การควบคุมการรับส่งข้อมูลสารสนเทศ ต้องกำหนดให้มีการควบคุมข้อมูลที่มีการแลกเปลี่ยนระหว่างหน่วยงานภายในบริษัทฯ รวมทั้งบริษัทฯ ในกลุ่ม และระหว่างบริษัทฯ กับหน่วยงานภายนอก โดยให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

(ก) ต้องกำหนดขั้นตอนการควบคุมการรับส่งข้อความทางอิเล็กทรอนิกส์ (Electronic Messaging) เช่น จดหมายอิเล็กทรอนิกส์ (E-Mail) โดยข้อความทางอิเล็กทรอนิกส์ที่สำคัญจะต้องได้รับการป้องกันอย่างเหมาะสมจากการพยายามเข้าถึง การแก้ไข การรบกวนจากผู้ไม่มีสิทธิ

(ข) ต้องกำหนดให้บุคลากรและหน่วยงานภายนอกที่ปฏิบัติงานให้บริษัทฯ มีการทำสัญญารักษาความลับหรือไม่เปิดเผยข้อมูลของบริษัทฯ อย่างเป็นลายลักษณ์อักษร

2.6 การป้องกันภัยคุกคามต่อระบบสารสนเทศ ต้องกำหนดมาตรการสำหรับตรวจจับ ป้องกัน และการกู้คืนระบบเพื่อป้องกันทรัพย์สินจากซอฟต์แวร์ที่ไม่ประสงค์ดี รวมทั้งต้องมีการสร้างความตระหนักให้ผู้ใช้งานอย่างเหมาะสม

3. **การรายงาน**

หน่วยงานที่ได้รับมอบหมายดูแลระบบเทคโนโลยีสารสนเทศ ต้องรายงานการปฏิบัติงานตามนโยบายด้านเทคโนโลยีสารสนเทศในกรณีที่มีเหตุการณ์ซึ่งอาจส่งผลกระทบต่อการปฏิบัติตามนโยบาย รวมถึงระเบียบและข้อกำหนดอย่างมีนัยสำคัญ เช่น ระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตราย อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนนโยบายด้านเทคโนโลยีสารสนเทศ รวมถึงระเบียบและข้อกำหนดที่บริษัทฯ กำหนดไว้

ประกาศ ณ วันที่ 10 ตุลาคม 2567

(สุรพล คุณานันทกุล)

กรรมการผู้อำนวยการ