นโยบายการจัดการและรักษาความปลอดภัยของข้อมูลและสารสนเทศ
(Information Security Policy)

บริษัท เอสจี แคปปิตอล จำกัด (มหาชน) (**"บริษัท"**) กำหนดนโยบายการจัดการและรักษาความปลอดภัยของข้อมูลและสารสนเทศของบริษัทให้มีความมั่นคงปลอดภัยและน่าเชื่อถือ ตลอดจนข้อมูลและสินทรัพย์สารสนเทศของบริษัทได้รับการดูแลรักษาอย่างเหมาะสม โดยคำนึงถึงความเสี่ยงจากภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศ และด้านความมั่นคงปลอดภัยจากไซเบอร์ที่อาจเกิดขึ้น กำหนดมาตรการในการรักษาความลับ ความถูกต้อง ครบถ้วน สมบูรณ์ และความพร้อมใช้ต่อการดำเนินงานอย่างเหมาะสม สอดคล้องกับข้อบังคับ กฎ ระเบียบ กฎหมายด้าน ความมั่นคงปลอดภัยสารสนเทศ จึงได้กำหนดนโยบายการจัดการและรักษาความปลอดภัยของข้อมูลและสารสนเทศ เพื่อเป็นแนวทางการดำเนินการด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศของบริษัทไว้ดังนี้

1. <u>การตรวจสอบและประเมินความเสี่ยง</u>

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องจัดให้มีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยให้ครอบคลุมถึงการระบุความเสี่ยง การประเมิน ความเสี่ยง และการควบคุมความเสี่ยงให้อยู่ในเกณฑ์ที่บริษัทยอมรับได้ รวมถึงจัดให้มีผู้รับผิดชอบในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม เพื่อให้มั่นใจว่าการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศถูกจัดการอย่างเหมาะสม

2. <u>การบริหารจัดการทรัพยากรด้านเทคโนโลยีสารสนเทศ</u>

หน่วยงานเจ้าของโครงการต้องจัดให้มีการบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับแผนกลยุทธ์บริษัท โดยให้ครอบคลุมถึงการบริหารทรัพยากรบุคคลและระบบเทคโนโลยีสารสนเทศที่เพียงพอต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ รวมถึงจัดให้มีการจัดการความเสี่ยงสำคัญในกรณีที่ไม่สามารถจัดสรรทรัพยากรได้เพียงพอต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ

3. <u>การรักษาความปลอดภัยต่อทรัพย์สินสารสนเทศ</u>

3.1 การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องกำหนดมาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับการควบคุมเข้าถึงและการใช้งานระบบสารสนเทศของบริษัทให้เหมาะสมกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง ช่องทางการเข้าถึง และจัดให้มีการป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก รวมถึงจากโปรแกรมที่ไม่พึงประสงค์ที่จะสร้างความเสียหายให้แก่ข้อมูลของบริษัท

3.2 การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

หน่วยงานเจ้าของโครงการหรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทต้องกำหนดมาตรการป้องกัน ควบคุมการใช้งาน การบำรุงรักษาด้านกายภาพของทรัพย์สินสารสนเทศ และอุปกรณ์

สารสนเทศซึ่งเป็นโครงสร้างพื้นฐานที่สนับสนุนการทำงานของระบบสารสนเทศของบริษัทให้อยู่ในสภาพที่มีความสมบูรณ์พร้อมใช้รวมถึงป้องกันการเข้าถึงทรัพย์สินสารสนเทศหรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

3.3 การจัดการข้อมูลสารสนเทศและการรักษาความลับ

1) การจำแนกประเภททรัพย์สินสารสนเทศ หน่วยงานเจ้าของโครงการหรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทต้องกำหนดแนวทางการจัดหมวดหมู่ของทรัพย์สินสารสนเทศ และจัดลำดับชั้นความลับของสารสนเทศ โดยต้องกำหนดชั้นความลับให้สอดคล้องกับกฎหมายและข้อกำหนดที่เกี่ยวข้องกับบริษัทมาร่วมพิจารณาการกำหนดชั้นความลับที่เหมาะสม รวมถึงต้องดำเนินการบริหารจัดการลำดับชั้นความลับข้อมูลตามแนวทางการดำเนินงานที่กำหนดไว้

2) การจัดทำระบบสำรองและแผนรองรับกรณีเกิดเหตุฉุกเฉิน หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทต้องจัดทำระบบสารสนเทศสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานโดยคัดเลือกระบบสารสนเทศที่สำคัญ รวมทั้งจัดทำแผนรองรับกรณีเกิดเหตุฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามการดำเนินงาน พร้อมทั้งต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสารสนเทศสำรอง การจัดทำแผนรองรับกรณีเกิดเหตุฉุกเฉินในกรณีที่ไม่สามารถ ดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ จัดให้มีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและแผนรองรับกรณีเกิดเหตุฉุกเฉินอย่างสม่ำเสมอ

3) การควบคุมการเข้ารหัสข้อมูล หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทต้องกำหนดมาตรการการเข้ารหัสลับข้อมูลและแนวทางการเลือกมาตรฐานการเข้ารหัสลับข้อมูล โดยให้มีความเหมาะสมกับความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลในแต่ละลำดับชั้นความลับที่กำหนดไว้ รวมทั้งติดตามให้มีการปฏิบัติให้เป็นไปตามนโยบายและวิธีการดังกล่าวอย่างสม่ำเสมอ

3.4 การจัดการระบบเครือข่ายคอมพิวเตอร์และการรับส่งข้อมูลสารสนเทศ

1) การรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทต้องควบคุมกำกับให้มีการบริหารจัดการการควบคุมเครือข่ายคอมพิวเตอร์ให้มีความมั่นคง ปลอดภัย และควบคุมให้มีการกำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัย ระดับของการให้บริการ และความต้องการด้านการบริหารจัดการของการให้บริการเครือข่ายในข้อตกลงหรือสัญญาการให้บริการด้านเครือข่ายต่าง ๆ ทั้งที่เป็นการให้บริการจากภายในหรือภายนอก รวมถึงจัดให้มีการแบ่งแยกระบบเครือข่ายคอมพิวเตอร์ตามความเหมาะสม โดยต้องพิจารณาถึงความต้องการเข้าถึงระบบเครือข่าย ผลกระทบทางด้านความมั่นคงปลอดภัยสารสนเทศ และระดับความสำคัญของข้อมูลที่อยู่บนเครือข่ายนั้น

2) การควบคุมการรับส่งข้อมูลสารสนเทศ

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัทต้องจัดให้มีการควบคุมข้อมูลที่มีการแลกเปลี่ยนระหว่างหน่วยงานภายในบริษัทรวมทั้งบริษัทในกลุ่มบริษัท และระหว่างบริษัทกับหน่วยงานภายนอกโดยให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

(1) ควบคุมกำกับให้มีข้อกำหนดสำหรับการปฏิบัติงาน ในการแลกเปลี่ยนข้อมูลสารสนเทศให้เหมาะสมสำหรับประเภทของการสื่อสารที่ใช้และประเภทของข้อมูลลำดับชั้นความลับของข้อมูล รวมถึงควบคุมให้มีข้อตกลงในการแลกเปลี่ยนข้อมูลสารสนเทศทั้งที่เป็นการแลกเปลี่ยนระหว่างหน่วยงานภายในบริษัท รวมทั้งบริษัทในกลุ่มบริษัทและระหว่างบริษัทกับหน่วยงานภายนอกอย่างเป็นลายลักษณ์อักษร

(2) ต้องกำหนดมาตรการในการควบคุมการรับส่งข้อความทางอิเล็กทรอนิกส์ (Electronic Messaging) เช่น จดหมายอิเล็กทรอนิกส์ (E-Mail) หรือ EDI (Electronic Data Interchange) หรือ Instant Messaging เป็นต้น โดยข้อความทางอิเล็กทรอนิกส์ที่สำคัญจะต้องได้รับการป้องกันอย่างเหมาะสมจากการพยายามเข้าถึง การแก้ไข การรบกวนทำให้ระบบหยุดให้บริการจากผู้ไม่มีสิทธิ

(3) ผู้บริหารระดับฝ่ายต้องจัดให้บุคลากรและหน่วยงานภายนอกที่ปฏิบัติงานให้บริษัทมีการทำสัญญารักษาความลับหรือไม่เปิดเผยข้อมูลของบริษัทอย่างเป็นลายลักษณ์อักษร

(4) กำหนดนโยบายสำหรับการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพา (Notebook, Tablet, Smartphone และอุปกรณ์สื่อสารเคลื่อนที่อื่น ๆ) ที่มีการนำมาใช้งาน เพื่อบริการจัดการความเสี่ยงด้านการนำข้อมูลไปใช้ในสภาพแวดล้อมที่ไม่ได้รับการป้องกัน

(5) ผู้ที่จำเป็นต้องปฏิบัติงานจากภายนอกสำนักงาน ต้องปฏิบัติตามระเบียบและวิธีการเรื่องการควบคุมการเข้าถึง และการลงทะเบียนการใช้งานระบบสารสนเทศ เพื่อให้มีการพิสูจน์ตัวตนและควบคุมการทำงานจากภายนอก โดยแบ่งระหว่างระบบที่เชื่อมต่ออินเทอร์เน็ตกับระบบอินทราเน็ตภายในที่ใช้งานในสำนักงาน

ทั้งนี้บริษัทได้มีการทบทวนและสอบทานนโยบายรักษาความปลอดภัยระบบสารสนเทศ ให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล จึงขอให้พนักงานทุกท่าน ปฏิบัติตามนโยบายการจัดการและรักษาความปลอดภัยของข้อมูลและสารสนเทศที่ประกาศใช้ อย่างเคร่งครัด หากพนักงานท่านใดละเลยและไม่ปฏิบัติตาม จะมีการลงโทษจากทางบริษัทขั้นสูงสุด และอาจต้องรับโทษตามที่กฎหมายกำหนดไว้

นโยบายการจัดการและรักษาความปลอดภัยของข้อมูลและสารสนเทศ ฉบับนี้คณะกรรมการบริษัทได้พิจารณาทบทวนในการประชุมคณะกรรมการบริษัท ครั้งที่ 8/2568 เมื่อวันที่ 11 พฤศจิกายน 2568 และจะพิจารณาทบทวนเป็นประจำทุกปี

(นายพิพิธ พิชัยศรทัต)
ประธานกรรมการบริษัท
บริษัท เอสจี แคปปิตอล จำกัด (มหาชน)