

ประกาศ TTT ที่ 038-2567

เรื่อง นโยบายและมาตรการรักษาความปลอดภัยของระบบสารสนเทศ

1. วัตถุประสงค์

บริษัท ทีทีที คอร์ปอเรชั่น จำกัด (“บริษัท”) ได้กำหนดนโยบายและระเบียบการใช้เทคโนโลยีสารสนเทศตามหลักการกำกับดูแลกิจการที่ดี รวมถึงการจัดให้มีมาตรการป้องกันความปลอดภัยของระบบคอมพิวเตอร์และข้อมูลสารสนเทศ เพื่อเป็นการควบคุมข้อมูลภายในของบริษัท และเพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมทั้งได้รับทราบเกี่ยวกับหน้าที่และความรับผิดชอบ และแนวทางปฏิบัติในการควบคุมความเสี่ยงด้านต่าง ๆ

บริษัทได้ตระหนักถึงความปลอดภัยของระบบเทคโนโลยีสารสนเทศ จึงได้มีการวางแผนจัดทำนโยบายและมาตรการรักษาความปลอดภัยของระบบสารสนเทศฉบับนี้ขึ้น เพื่อเป็นกรอบแนวทางปฏิบัติของพนักงานในองค์กร เพื่อให้พนักงานตระหนักถึงความปลอดภัยของเทคโนโลยีสารสนเทศ และการรักษาความปลอดภัยของระบบข้อมูลสารสนเทศของบริษัท และเป็นมาตรการป้องกันความเสี่ยงต่อการเกิดปัญหา เพื่อให้การดำเนินการใด ๆ ด้านเทคโนโลยีสารสนเทศของบริษัทมีความมั่นคงปลอดภัยและน่าเชื่อถือ ตลอดจนข้อมูลและสินทรัพย์สารสนเทศของบริษัทได้รับการดูแลรักษาอย่างเหมาะสม โดยคำนึงถึงความเสี่ยงจากภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศและด้านความมั่นคงปลอดภัยทางไซเบอร์ที่อาจเกิดขึ้น มาตรการในการรักษาความลับ ความถูกต้อง ครบถ้วน สมบูรณ์ และความพร้อมใช้ต่อการดำเนินงานอย่างเหมาะสม รวมถึงสอดคล้องกับข้อบังคับ กฎ ระเบียบ กฎหมายด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

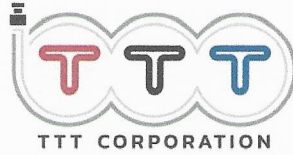
2. การรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

(1) การตรวจสอบและประเมินความเสี่ยง

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องจัดให้มีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยให้ครอบคลุมถึงการระบุความเสี่ยง การประเมินความเสี่ยง และการควบคุมความเสี่ยงให้อยู่ในเกณฑ์ที่บริษัทยอมรับได้ รวมถึงจัดให้มีผู้รับผิดชอบในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม เพื่อให้มั่นใจว่าการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศถูกจัดการอย่างเหมาะสม

(2) การบริหารจัดการทรัพยากรด้านเทคโนโลยีสารสนเทศ

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องจัดให้มีการบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับแผนกลยุทธ์ของบริษัท โดยให้ครอบคลุมถึงการบริหารทรัพยากรบุคคลและระบบ

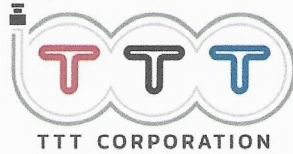


เทคโนโลยีสารสนเทศที่เพียงพอต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ รวมถึงจัดให้มีการจัดการความเสี่ยงสำคัญในกรณีที่ไม่สามารถจัดสรรทรัพยากรได้เพียงพอต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ

(3) การรักษาความปลอดภัยต่อทรัพย์สินสารสนเทศ

1) การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ

- (ก) หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องกำหนดมาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับการควบคุมเข้าถึงและการทำงานของระบบสารสนเทศของบริษัท ให้เหมาะสมกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูลรวมทั้งระดับขั้นการเข้าถึง เวลาที่ได้เข้าถึงและช่องทางการเข้าถึง และจัดให้มีการป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก รวมถึงจากโปรแกรมที่ไม่พึงประสงค์ที่จะสร้างความเสียหายให้แก่ข้อมูลของบริษัท
- (ข) การใช้งานคอมพิวเตอร์และเทคโนโลยีสารสนเทศของบริษัท จะต้องเป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (และที่ได้ออกแก้ไขเพิ่มเติม) รวมถึงกฎหมายอื่นที่เกี่ยวข้อง
- (ค) บริษัทจะจำกัดการเข้าถึงข้อมูลภายในโดยให้เฉพาะผู้บริหารที่เข้าถึงข้อมูลดังกล่าวได้ หรือผู้ที่มิหน้าที่โดยตรงในการบริหารงานต่าง ๆ ที่เกี่ยวข้องเท่านั้น ทั้งนี้ ให้รวมถึงการเปิดเผยข้อมูลที่จำเป็นต่อพนักงานของบริษัท โดยบริษัทจะแจ้งให้พนักงานทราบว่าข้อมูลดังกล่าวเป็นความลับ และไม่สามารถเปิดเผยให้แก่บุคคลภายนอกได้
- (ง) บริษัทจะจัดระบบรักษาความปลอดภัยเพื่อป้องกันการเข้าถึงข้อมูล และเอกสารที่เป็นความลับอย่างเคร่งครัด
- (จ) พนักงานที่ได้รับอนุญาตให้เข้าถึงข้อมูลที่เป็นความลับ จะต้องใช้ระบบเทคโนโลยีสารสนเทศให้ถูกต้องตามสิทธิที่ได้รับอนุญาต และจะต้องไม่ยินยอมให้ผู้อื่นใช้ หรือเข้าถึงรหัสผ่านสำหรับใช้งานระบบเทคโนโลยีสารสนเทศนั้น
- (ฉ) ห้ามบุคคลใดใช้งานระบบเทคโนโลยีสารสนเทศเพื่อเข้าถึง หรือส่งข้อมูลส่วนตัว หรือข้อมูลที่มีเนื้อหาขัดต่อศีลธรรมอันดีเกี่ยวกับการพนัน การละเมิดสิทธิผู้อื่น หรือกระทบต่อความมั่นคงของประเทศชาติ
- (ช) หากมีการสื่อสารผ่านสังคมออนไลน์ จะต้องดำเนินการอย่างเหมาะสม ถูกต้องตามความเป็นจริง โดยคำนึงถึงความเป็นธรรมต่อผู้มีส่วนเกี่ยวข้องทุกฝ่าย ไม่ก่อให้เกิดความเสียหายต่อบริษัท และจะไม่สื่อสารข้อมูลส่วนตัวในฐานะพนักงานของบริษัท ทั้งนี้ การดำเนินการใด ๆ ในฐานะตัวแทน



ของบริษัทผ่านสื่อสังคมออนไลน์ จะดำเนินการได้ต่อเมื่อได้รับอนุมัติจากบุคคลหรือฝ่ายที่รับผิดชอบในเรื่องที่เกี่ยวข้องนั้น ๆ รวมถึงได้ดำเนินการตามอำนาจและขั้นตอนการอนุมัติของบริษัทแล้วเท่านั้น

2) การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

- (ก) หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องกำหนดมาตรการป้องกันควบคุมการใช้งาน และการบำรุงรักษาด้านกายภาพของทรัพย์สินสารสนเทศและอุปกรณ์สารสนเทศซึ่งเป็นโครงสร้างพื้นฐานที่สนับสนุนการทำงานของระบบสารสนเทศของบริษัท ให้อยู่ในสภาพที่มีความสมบูรณ์พร้อมใช้ รวมถึงป้องกันการเข้าถึงทรัพย์สินสารสนเทศหรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต
- (ข) ห้ามบุคคลใดทำการเปลี่ยนแปลง ทำซ้ำ ลบทิ้ง หรือทำลายข้อมูลของบริษัท รวมทั้งห้ามมิให้เปิดเผยข้อมูลที่มีอยู่ในระบบสารสนเทศของบริษัท โดยไม่ได้รับอนุญาต

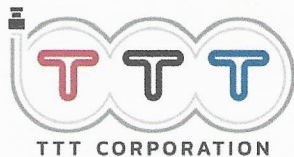
3) การจัดการข้อมูลสารสนเทศและการรักษาความลับ

- (ก) การจำแนกประเภททรัพย์สินสารสนเทศ

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องกำหนดแนวทางการจัดหมวดหมู่ของทรัพย์สินสารสนเทศ และจัดลำดับชั้นความลับของสารสนเทศ โดยต้องกำหนดชั้นความลับให้สอดคล้องกับกฎหมายและข้อกำหนดที่เกี่ยวข้องกับบริษัท รวมถึงต้องดำเนินการบริหารจัดการลำดับชั้นความลับข้อมูลตามแนวทางการดำเนินงานที่กำหนดไว้

- (ข) การจัดทำระบบสำรองและแผนรองรับกรณีเกิดเหตุฉุกเฉิน

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องจัดทำระบบสารสนเทศสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานโดยคัดเลือกระบบสารสนเทศที่สำคัญ รวมทั้งจัดทำแผนรองรับกรณีเกิดเหตุฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามการดำเนินงาน พร้อมทั้งต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสารสนเทศสำรอง และการจัดทำแผนรองรับกรณีเกิดเหตุฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ และให้มีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และแผนรองรับกรณีเกิดเหตุฉุกเฉินอย่างสม่ำเสมอ



(ค) การควบคุมการเข้ารหัสข้อมูล

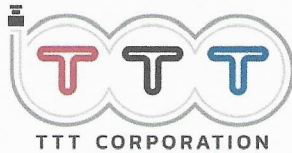
หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องกำหนดมาตรการการเข้ารหัสลับข้อมูลและแนวทางการเลือกมาตรฐานการเข้ารหัสลับข้อมูล โดยให้มีความเหมาะสมกับความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลในแต่ละลำดับชั้นความลับที่กำหนดไว้ รวมทั้งติดตามให้มีการปฏิบัติให้เป็นไปตามนโยบายและวิธีการดังกล่าวอย่างสม่ำเสมอ

4) การควบคุมดูแลบุคลากรผู้ปฏิบัติงาน

(ก) การควบคุมการใช้งานของผู้ใช้งาน

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องจัดให้มีการควบคุมการใช้งานทรัพยากรสารสนเทศและระบบสารสนเทศ ดังนี้

- กำหนดมาตรการป้องกันทรัพยากรสารสนเทศประเภทอุปกรณ์ระหว่างที่ไม่มีผู้ใช้งาน หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องกำหนดให้ผู้ใช้งานเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศโดยการใส่รหัสผ่าน และให้ออกจากระบบสารสนเทศ ระบบงานคอมพิวเตอร์ที่ใช้งาน และเครื่องคอมพิวเตอร์ โดยทันทีเมื่อไม่มีความจำเป็นต้องใช้งาน หรือเมื่อเสร็จสิ้นการปฏิบัติงาน รวมถึงให้มีการล็อกหน้าจอเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือเมื่อออกห่างจากเครื่องคอมพิวเตอร์ตามเวลาที่กำหนดอย่างเหมาะสม
- กำหนดการใช้งานอุปกรณ์เคลื่อนที่และการปฏิบัติงานจากเครือข่ายภายนอกบริษัท หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องกำหนดให้มีมาตรการที่เหมาะสมควบคุมความมั่นคงปลอดภัยของอุปกรณ์สื่อสารประเภทพกพา โดยพิจารณาจากความเสี่ยงที่มีการนำอุปกรณ์เข้ามาเชื่อมต่อกับเครือข่ายคอมพิวเตอร์ของบริษัท รวมถึงกำหนดมาตรการควบคุมสำหรับการนำอุปกรณ์ออกไปใช้งานภายนอกบริษัท
- กำหนดการควบคุมการติดตั้งซอฟต์แวร์บนระบบงาน หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องจัดทำขั้นตอนปฏิบัติงานและมาตรการควบคุมการติดตั้งซอฟต์แวร์บนระบบที่ให้บริการจริง เพื่อจำกัดการติดตั้งซอฟต์แวร์โดยผู้ใช้งานและป้องกันการติดตั้งซอฟต์แวร์ที่ไม่ได้รับอนุญาตให้ใช้งาน และกำหนดรายการซอฟต์แวร์มาตรฐาน (Software Standard) ที่อนุญาตให้ติดตั้งบนเครื่องคอมพิวเตอร์ของบริษัท อย่างเป็นลายลักษณ์อักษร และปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในบริษัท รับทราบและปฏิบัติตาม



(๒) การควบคุมดูแลผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ (IT Outsourcing)

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องจัดทำข้อกำหนดและกรอบการปฏิบัติงานของผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ มีความมั่นคงปลอดภัย โดยข้อกำหนดและกรอบการปฏิบัติงานต้องครอบคลุมกรณีที่ผู้รับดำเนินการมีการให้ผู้บริการภายนอกรายอื่น (Sub-Contract) รับช่วงจัดการงานด้านเทคโนโลยีสารสนเทศ

5) การจัดการระบบเครือข่ายคอมพิวเตอร์และการรับส่งข้อมูลสารสนเทศ

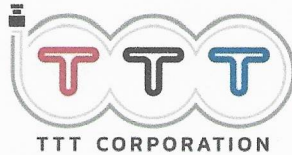
(ก) การรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องควบคุม กำกับให้มีการบริหารจัดการการควบคุมเครือข่ายคอมพิวเตอร์ให้มีความมั่นคงปลอดภัย และควบคุมให้มีการกำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัย ระดับของการให้บริการ และความต้องการด้านการบริหารจัดการของการให้บริการเครือข่ายในข้อตกลงหรือสัญญาการให้บริการด้านเครือข่ายต่าง ๆ ทั้งที่เป็นการให้บริการจากภายในหรือภายนอก รวมถึงจัดให้มีการแบ่งแยกระบบเครือข่ายคอมพิวเตอร์ตามความเหมาะสม โดยต้องพิจารณาถึงความต้องการเข้าถึงระบบเครือข่ายผลกระทบทางด้านความมั่นคงปลอดภัยสารสนเทศ และระดับความสำคัญของข้อมูลที่อยู่บนเครือข่ายนั้น

(ข) การควบคุมการรับส่งข้อมูลสารสนเทศ

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องจัดให้มีการควบคุมข้อมูลที่มีการแลกเปลี่ยนระหว่างหน่วยงานภายในบริษัท รวมทั้งบริษัทย่อย และระหว่างบริษัทกับหน่วยงานภายนอกโดยให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

- หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องควบคุม กำกับให้มีการข้อกำหนดสำหรับการปฏิบัติงานในการแลกเปลี่ยนข้อมูลสารสนเทศให้เหมาะสมสำหรับประเภทของการสื่อสารที่ใช้และประเภทของข้อมูลลำดับชั้นความลับของข้อมูล รวมถึงควบคุมให้มีข้อตกลงในการแลกเปลี่ยนข้อมูลสารสนเทศทั้งที่เป็นการแลกเปลี่ยนระหว่างหน่วยงานภายในบริษัท รวมทั้งบริษัทย่อย และระหว่างบริษัทกับหน่วยงานภายนอกอย่างเป็นลายลักษณ์อักษร
- หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องกำหนดมาตรการในการควบคุมการรับส่งข้อความทางอิเล็กทรอนิกส์ (Electronic Messaging) เช่น จดหมายอิเล็กทรอนิกส์ (E-Mail) หรือ EDI (Electronic Data Interchange) หรือ Instant Messaging เป็นต้น โดยข้อความทางอิเล็กทรอนิกส์ที่สำคัญจะต้องได้รับการป้องกันอย่าง



เหมาะสมจากการพยายามเข้าถึง การแก้ไข การรบกวนทำให้ระบบหยุดให้บริการจากผู้ไม่มีสิทธิ

- หัวหน้าหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องจัดให้บุคลากรและหน่วยงานภายนอกที่ปฏิบัติงานให้บริษัทมีการทำสัญญาการรักษาความลับหรือไม่เปิดเผยข้อมูลของบริษัท อย่างเป็นลายลักษณ์อักษร

6) การป้องกันภัยคุกคามต่อระบบสารสนเทศ

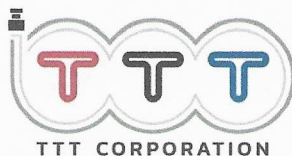
(ก) การป้องกันภัยคุกคามจากโปรแกรมไม่ประสงค์ดี

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องกำหนดมาตรการสำหรับการตรวจจับ การป้องกัน และการกู้คืนระบบเพื่อป้องกันทรัพย์สินจากซอฟต์แวร์ไม่ประสงค์ดี รวมทั้งต้องมีการสร้างความตระหนักที่เกี่ยวข้องให้กับผู้ใช้งานอย่างเหมาะสม

(ข) การบริหารจัดการช่องโหว่ทางเทคนิค

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องควบคุมให้ระบบสารสนเทศของบริษัท ได้รับการพิสูจน์ถึงช่องโหว่ทางเทคนิคซึ่งอาจเกิดขึ้นได้ โดยให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

- จัดให้มีการทดสอบการเจาะระบบ (Penetration Test) กับระบบงานที่มีความสำคัญที่เชื่อมต่อกับระบบเครือข่ายภายนอก (Untrusted Network) โดยบุคคลที่เป็นอิสระจากหน่วยงานที่รับผิดชอบด้านเทคโนโลยีสารสนเทศ และเป็นไปตามการวิเคราะห์ความเสี่ยงและผลกระทบทางธุรกิจ (Risk and Business Impact Analysis) ดังนี้
 - กรณีที่เป็นระบบงานสำคัญที่ประเมินแล้วมีความสำคัญสูง ต้องทดสอบอย่างน้อยทุก 3 ปี และเมื่อมีการเปลี่ยนแปลงระบบงานดังกล่าวอย่างมีนัยสำคัญ
 - กรณีที่เป็นระบบงานที่มีความสำคัญอื่น ๆ ต้องทดสอบอย่างน้อยทุก 5 ปี
- จัดให้มีการประเมินช่องโหว่ของระบบ (Vulnerability Assessment) กับระบบงานที่มีความสำคัญทุกระบบอย่างน้อยปีละ 1 ครั้งและเมื่อมีการเปลี่ยนแปลงระบบงานดังกล่าวอย่างมีนัยสำคัญ และรายงานผลไปยังหน่วยงานที่เกี่ยวข้องเพื่อให้รับทราบและหาแนวทางการแก้ไขและป้องกัน



- จัดให้มีการทดสอบขั้นตอนและกระบวนการในการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศอย่างน้อยปีละ 1 ครั้ง โดยอย่างน้อยต้องครอบคลุมถึงการบริหารจัดการความเสี่ยงไซเบอร์ (Cyber Security Drill)

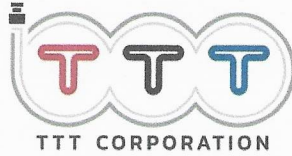
7) การจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องจัดให้มีข้อกำหนดในการจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศที่เหมาะสม เพื่อลดความผิดพลาดในการกำหนดความต้องการ การออกแบบ การพัฒนา และการทดสอบระบบสารสนเทศที่มีการพัฒนาขึ้นใหม่หรือปรับปรุงระบบงานเพิ่มเติม รวมถึงควบคุมให้ระบบงานที่พัฒนาหรือจัดหาเป็นไปตามข้อตกลงที่กำหนดไว้

(4) การกำหนดมาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องจัดให้มีมาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศของหน่วยงานที่สอดคล้องกับนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศที่ได้ประกาศใช้งาน และดำเนินการประกาศให้ผู้เกี่ยวข้องทั้งหมดทราบ เพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามมาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศได้ และต้องกำหนดผู้รับผิดชอบตามมาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศดังกล่าวให้ชัดเจน โดยมาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศของบริษัท แบ่งออกเป็น 14 ข้อ ได้แก่

- 1) มาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Standard)
- 2) การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ (Organization of Information Security)
- 3) การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร (Human Resource Security)
- 4) การบริหารจัดการทรัพย์สินสารสนเทศ (Asset Management)
- 5) การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ (Access Control)
- 6) การควบคุมการเข้ารหัสข้อมูล (Cryptographic Control)
- 7) การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (Physical and Environmental Security)
- 8) การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ (Operations Security)
- 9) การรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ (Communications Security)



- 10) การจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ (System Acquisition, Development and Maintenance)
- 11) การใช้บริการระบบสารสนเทศจากผู้ให้บริการภายนอก (IT Outsourcing)
- 12) การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Incident Management)
- 13) การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Aspects of Business Continuity Management)
- 14) การปฏิบัติตามข้อกำหนด (Compliance)

3. การรายงาน

ให้มีการรายงานการปฏิบัติตามนโยบายและมาตรการรักษาความปลอดภัยของระบบสารสนเทศ รวมถึงระเบียบและข้อกำหนดใดๆ ต่อคณะกรรมการบริษัท อย่างน้อยปีละ 1 ครั้ง หรือในกรณีที่มีเหตุการณ์ใด ๆ ซึ่งอาจส่งผลกระทบต่อ การปฏิบัติตามนโยบายและมาตรการรักษาความปลอดภัยของระบบสารสนเทศ รวมถึงระเบียบและข้อกำหนดอย่างมีนัยสำคัญ เช่น ระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่บริษัท หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและมาตรการรักษาความปลอดภัยของระบบสารสนเทศ รวมถึงระเบียบและข้อกำหนดที่บริษัทกำหนดไว้

4. บทบังคับใช้

นโยบายและมาตรการรักษาความปลอดภัยของระบบสารสนเทศนี้ให้ใช้บังคับกับ พนักงาน ลูกจ้างชั่วคราว ลูกจ้างประจำของบริษัท รวมถึงบุคคลภายนอกและหน่วยงานภายนอกที่ให้บริการแก่บริษัท

อนุมัติโดย

มติที่ประชุมคณะกรรมการบริษัท ครั้งที่ 4/2567 เมื่อวันที่ 14 สิงหาคม 2567 และมีผลบังคับใช้ในวันเดียวกัน

บริษัท ทีทีที คอร์ปอเรชั่น จำกัด

(นายอดิศศักดิ์ รักอริยะพงศ์)

ประธานกรรมการบริษัท