

นโยบายด้านเทคโนโลยีสารสนเทศ

บริษัท สิริซอฟต์ จำกัด (มหาชน) (“บริษัท”) มีนโยบายที่จะให้พนักงาน และผู้ปฏิบัติงานที่เกี่ยวข้องกับการใช้ระบบเทคโนโลยีสารสนเทศ อันประกอบด้วยวงจรเครือข่ายการสื่อสารข้อมูล ระบบซอฟต์แวร์ที่ใช้ในการปฏิบัติการและการประมวลผลข้อมูล เครื่องคอมพิวเตอร์ พร้อมอุปกรณ์ต่อพ่วง แฟ้มข้อมูล และข้อมูลของบริษัท อย่างมีประสิทธิภาพ ไม่ขัดต่อกฎหมาย หรือพระราชบัญญัติที่เกี่ยวข้อง โดยมีมาตรฐานความปลอดภัยที่เพียงพอ เพื่อประโยชน์และประสิทธิผลทางธุรกิจของบริษัท จึงกำหนดให้ถือปฏิบัติ ดังนี้

1. การรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

1.1 การตรวจสอบและประเมินความเสี่ยง

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องจัดให้มีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยให้ครอบคลุมถึงการระบุความเสี่ยง การประเมินความเสี่ยง และการควบคุมความเสี่ยงให้อยู่ในเกณฑ์ที่บริษัทยอมรับได้ รวมถึงจัดให้มีผู้รับผิดชอบในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม เพื่อให้มั่นใจว่าการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศถูกจัดการอย่างเหมาะสม

1.2 การบริหารจัดการทรัพยากรด้านเทคโนโลยีสารสนเทศ

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องจัดให้มีการบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับแผนกลยุทธ์ของบริษัท โดยให้ครอบคลุมถึงการบริหารทรัพยากรบุคคลและระบบเทคโนโลยีสารสนเทศที่เพียงพอต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ รวมถึงจัดให้มีการจัดการความเสี่ยงสำคัญในกรณีที่ไม่สามารถจัดสรรทรัพยากรได้เพียงพอต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ

1.3 การรักษาความปลอดภัยต่อทรัพย์สินสารสนเทศ

1.3.1 การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ

- (1) หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องกำหนดมาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ สำหรับการควบคุมเข้าถึงและการใช้งานระบบสารสนเทศของบริษัท ให้เหมาะสมกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูลรวมทั้งระดับขั้นการเข้าถึง เวลาที่ได้เข้าถึงและช่องทางการเข้าถึง และจัดให้มีการป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก รวมถึงจากโปรแกรมที่ไม่พึงประสงค์ที่จะสร้างความเสียหายให้แก่ข้อมูลของบริษัท
- (2) การใช้งานคอมพิวเตอร์และเทคโนโลยีสารสนเทศของบริษัท จะต้องเป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (และที่แก้ไขเพิ่มเติม) รวมถึงกฎหมายอื่นใดที่เกี่ยวข้อง
- (3) บริษัทจะจำกัดการเข้าถึงข้อมูลภายในโดยให้เฉพาะผู้บริหารที่เข้าถึงข้อมูลดังกล่าวได้ หรือผู้ที่มีหน้าที่โดยตรงในการบริหารงานต่าง ๆ ที่เกี่ยวข้องเท่านั้น ทั้งนี้ ให้รวมถึงการเปิดเผยข้อมูล

จำเป็นต่อพนักงานของบริษัท โดยบริษัทจะแจ้งให้พนักงานทราบว่าข้อมูลดังกล่าวนี้เป็นความลับ และไม่สามารถเปิดเผยให้แก่บุคคลภายนอกได้

- (4) บริษัทจะจัดระบบรักษาความปลอดภัยเพื่อป้องกันการเข้าถึงข้อมูล และเอกสารที่เป็นความลับอย่างเคร่งครัด
- (5) พนักงานที่ได้รับอนุญาตให้เข้าถึงข้อมูลที่เป็นความลับ จะต้องใช้ระบบเทคโนโลยีสารสนเทศให้ถูกต้องตามสิทธิที่ได้รับอนุญาต และจะต้องไม่ยินยอมให้ผู้อื่นใช้ หรือเข้าถึงรหัสผ่านสำหรับเข้าใช้งานระบบเทคโนโลยีสารสนเทศนั้น
- (6) ห้ามบุคคลใดใช้งานระบบเทคโนโลยีสารสนเทศเพื่อเข้าถึง หรือส่งข้อมูลส่วนตัว หรือข้อมูลที่มีเนื้อหาขัดต่อศีลธรรมอันดีเกี่ยวกับการพนัน การละเมิดสิทธิผู้อื่น หรือกระทบต่อความมั่นคงของประเทศชาติ
- (7) หากมีการสื่อสารผ่านสังคมออนไลน์ จะต้องดำเนินการอย่างเหมาะสม ถูกต้องตามความเป็นจริง โดยคำนึงถึงความเป็นธรรมต่อผู้มีส่วนเกี่ยวข้องทุกฝ่าย ไม่ก่อให้เกิดความเสียหายต่อบริษัท และจะไม่สื่อสารข้อมูลส่วนตัวในฐานะพนักงานของบริษัท ทั้งนี้ การดำเนินการใด ๆ ในฐานะตัวแทนของบริษัทผ่านสื่อสังคมออนไลน์ จะดำเนินการได้ต่อเมื่อได้รับอนุมัติจากบุคคลหรือฝ่ายที่รับผิดชอบในเรื่องที่เกี่ยวข้องนั้น ๆ รวมถึงได้ดำเนินการตามอำนาจและขั้นตอนการอนุมัติของบริษัทแล้วเท่านั้น

1.3.2 การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

- (1) หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องกำหนดมาตรการป้องกันควบคุมการใช้งาน และการบำรุงรักษาด้านกายภาพของทรัพย์สินสารสนเทศและอุปกรณ์สารสนเทศซึ่งเป็นโครงสร้างพื้นฐานที่สนับสนุนการทำงานของระบบสารสนเทศของบริษัท ให้อยู่ในสภาพที่มีความสมบูรณ์พร้อมใช้ รวมถึงป้องกันการเข้าถึงทรัพย์สินสารสนเทศหรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต
- (2) ห้ามบุคคลใดทำการเปลี่ยนแปลง ทำซ้ำ ลบทิ้ง หรือทำลายข้อมูลของบริษัท รวมทั้งห้ามมิให้เปิดเผยข้อมูลที่มีอยู่ในระบบสารสนเทศของบริษัท โดยไม่ได้รับอนุญาต

1.3.3 การจัดการข้อมูลสารสนเทศและการรักษาความลับ

- (1) การจำแนกประเภททรัพย์สินสารสนเทศ

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องกำหนดแนวทางการจัดหมวดหมู่ของทรัพย์สินสารสนเทศ และจัดลำดับชั้นความลับของสารสนเทศ โดยต้องกำหนดชั้นความลับให้สอดคล้องกับกฎหมายและข้อกำหนดที่เกี่ยวข้องกับบริษัท รวมถึงต้องดำเนินการบริหารจัดการลำดับชั้นความลับข้อมูลตามแนวทางการดำเนินงานที่กำหนดไว้

(2) การจัดทำระบบสำรองและแผนรองรับกรณีเกิดเหตุฉุกเฉิน

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องจัดทำระบบสารสนเทศสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานโดยคัดเลือกระบบสารสนเทศที่สำคัญ รวมทั้งจัดทำแผนรองรับกรณีเกิดเหตุฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามการดำเนินงาน พร้อมทั้งต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสารสนเทศสำรอง และการจัดทำแผนรองรับกรณีเกิดเหตุฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ และให้มีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และแผนรองรับกรณีเกิดเหตุฉุกเฉินอย่างสม่ำเสมอ

(3) การควบคุมการเข้าถึงข้อมูล

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องกำหนดมาตรการการเข้าถึงข้อมูลและแนวทางการเลือกมาตรฐานการเข้าถึงข้อมูล โดยให้มีความเหมาะสมกับความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลในแต่ละลำดับชั้นความลับที่กำหนดไว้ รวมทั้งติดตามให้มีการปฏิบัติให้เป็นไปตามนโยบายและวิธีการดังกล่าวอย่างสม่ำเสมอ

1.3.4 การควบคุมดูแลบุคลากรผู้ปฏิบัติงาน

(1) การควบคุมการใช้งานของผู้ใช้งาน

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องจัดให้มีการควบคุมการใช้งานทรัพยากรสารสนเทศและระบบสารสนเทศ ดังนี้

(1.1) กำหนดมาตรการป้องกันทรัพยากรสารสนเทศประเภทอุปกรณ์ระหว่างที่ไม่มีผู้ใช้งาน

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องกำหนดให้ผู้ใช้งานเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศโดยการใส่รหัสผ่าน และให้ออกจากระบบสารสนเทศ ระบบงานคอมพิวเตอร์ที่ใช้งาน และเครื่องคอมพิวเตอร์ โดยทันทีเมื่อไม่มีความจำเป็นต้องใช้งาน หรือเมื่อเสร็จสิ้นการปฏิบัติงาน รวมถึงให้มีการล็อกหน้าจอเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือเมื่อออกจากเครื่องคอมพิวเตอร์ตามเวลาที่กำหนดอย่างเหมาะสม

(1.2) กำหนดการใช้งานอุปกรณ์เคลื่อนที่และการปฏิบัติงานจากเครือข่ายภายนอกบริษัท

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องกำหนดให้มีมาตรการที่เหมาะสมควบคุมความมั่นคงปลอดภัยของอุปกรณ์สื่อสารประเภทพกพา โดยพิจารณาจากความเสี่ยงที่มีการนำอุปกรณ์เข้ามา

เชื่อมต่อกับเครือข่ายคอมพิวเตอร์ของบริษัท รวมถึงกำหนดมาตรการควบคุมสำหรับการนำอุปกรณ์ออกไปใช้งานภายนอกบริษัท

(1.3) กำหนดการควบคุมการติดตั้งซอฟต์แวร์บนระบบงาน

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องจัดทำขั้นตอนปฏิบัติงานและมาตรการควบคุมการติดตั้งซอฟต์แวร์บนระบบที่ให้บริการจริง เพื่อจำกัดการติดตั้งซอฟต์แวร์โดยผู้ใช้งานและป้องกันการติดตั้งซอฟต์แวร์ที่ไม่ได้รับอนุญาตให้ใช้งาน และกำหนดรายการซอฟต์แวร์มาตรฐาน (Software Standard) ที่อนุญาตให้ติดตั้งบนเครื่องคอมพิวเตอร์ของบริษัท อย่างเป็นลายลักษณ์อักษร และปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในบริษัททราบและปฏิบัติตาม

(2) การควบคุมดูแลผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ (IT Outsourcing)

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องจัดทำข้อกำหนดและกรอบการปฏิบัติงานของผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ มีความมั่นคงปลอดภัย โดยข้อกำหนดและกรอบการปฏิบัติงานต้องครอบคลุมกรณีที่ผู้รับดำเนินการมีการให้บริการภายนอกรายอื่น (Sub-Contract) รับช่วงจัดการงานด้านเทคโนโลยีสารสนเทศ

1.3.5 การจัดการระบบเครือข่ายคอมพิวเตอร์และการรับส่งข้อมูลสารสนเทศ

(1) การรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องควบคุม กำกับให้มีการบริหารจัดการการควบคุมเครือข่ายคอมพิวเตอร์ให้มีความมั่นคงปลอดภัย และควบคุมให้มีการกำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัย ระดับของการให้บริการ และความต้องการด้านการบริหารจัดการของการให้บริการเครือข่ายในข้อตกลงหรือสัญญาการให้บริการด้านเครือข่ายต่าง ๆ ทั้งที่เป็นการให้บริการจากภายในหรือภายนอก รวมถึงจัดให้มีการแบ่งแยกระบบเครือข่ายคอมพิวเตอร์ตามความเหมาะสม โดยต้องพิจารณาถึงความต้องการเข้าถึงระบบเครือข่าย ผลกระทบทางด้านความมั่นคงปลอดภัยสารสนเทศ และระดับความสำคัญของข้อมูลที่อยู่บนเครื่อข่ายนั้น

(2) การควบคุมการรับส่งข้อมูลสารสนเทศ

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องจัดให้มีการควบคุมข้อมูลที่มีการแลกเปลี่ยนระหว่างหน่วยงานภายในบริษัท รวมทั้งบริษัทย่อย และระหว่างบริษัทกับหน่วยงานภายนอกโดยให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

(2.1) แผนกเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับให้มีข้อกำหนดสำหรับการปฏิบัติงานในการแลกเปลี่ยนข้อมูลสารสนเทศให้เหมาะสมสำหรับประเภทของการสื่อสารที่ใช้ และประเภทของข้อมูลลำดับชั้นความลับของข้อมูล รวมถึงควบคุมให้มีข้อตกลงในการ

แลกเปลี่ยนข้อมูลสารสนเทศทั้งที่เป็นการแลกเปลี่ยนระหว่างหน่วยงานภายในบริษัท รวมทั้งบริษัทย่อย และระหว่างบริษัทกับหน่วยงานภายนอกอย่างเป็นลายลักษณ์อักษร

- (2.2) แผนกเทคโนโลยีสารสนเทศ ต้องกำหนดมาตรการในการควบคุมการรับส่งข้อความทางอิเล็กทรอนิกส์ (Electronic Messaging) เช่น จดหมายอิเล็กทรอนิกส์ (E-Mail) หรือ EDI (Electronic Data Interchange) หรือ Instant Messaging เป็นต้น โดยข้อความทางอิเล็กทรอนิกส์ที่สำคัญจะต้องได้รับการป้องกันอย่างเหมาะสมจากการพยายามเข้าถึง การแก้ไข การรบกวนทำให้ระบบหยุดให้บริการจากผู้ไม่มีสิทธิ
- (2.3) หัวหน้าแผนกเทคโนโลยีสารสนเทศต้องจัดให้บุคลากรและหน่วยงานภายนอกที่ปฏิบัติงานให้บริษัทมีการทำสัญญารักษาความลับหรือไม่เปิดเผยข้อมูลของบริษัทอย่างเป็นลายลักษณ์อักษร

1.3.6 การป้องกันภัยคุกคามต่อระบบสารสนเทศ

- (1) การป้องกันภัยคุกคามจากโปรแกรมไม่ประสงค์ดี

หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องกำหนดมาตรการสำหรับการตรวจจับ การป้องกัน และการกู้คืนระบบเพื่อป้องกันทรัพย์สินจากซอฟต์แวร์ไม่ประสงค์ดี รวมทั้งต้องมีการสร้างความตระหนักที่เกี่ยวข้องให้กับผู้ใช้งานอย่างเหมาะสม

- (2) การบริหารจัดการช่องโหว่ทางเทคนิค

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องควบคุมให้ระบบสารสนเทศของบริษัท ได้รับการพิสูจน์ถึงช่องโหว่ทางเทคนิคซึ่งอาจเกิดขึ้นได้ โดยให้เป็นไปตามหลักเกณฑ์ดังต่อไปนี้

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

ดังกล่าวอย่างมีนัยสำคัญ และรายงานผลไปยังหน่วยงานที่เกี่ยวข้องเพื่อให้รับทราบ และหาแนวทางการแก้ไขและป้องกัน

- (2.3) จัดให้มีการทดสอบขั้นตอนและกระบวนการในการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศอย่างน้อยปีละ 1 ครั้ง โดยอย่างน้อยต้องครอบคลุมถึงการบริหารจัดการความเสี่ยงไซเบอร์ (Cyber Security Drill)

1.3.7 การจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ

หน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของบริษัท ต้องจัดให้มีข้อกำหนดในการจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศที่เหมาะสม เพื่อลดความผิดพลาดในการกำหนดความต้องการ การออกแบบ การพัฒนา และการทดสอบระบบสารสนเทศที่มีการพัฒนาขึ้นใหม่หรือปรับปรุงระบบงานเพิ่มเติม รวมถึงควบคุมให้ระบบงานที่พัฒนาหรือจัดหาเป็นไปตามข้อตกลงที่กำหนดไว้

1.4 การกำหนดมาตรฐานการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

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

- 1.4.1 มาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Standard)
- 1.4.2 การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ (Organization of Information Security)
- 1.4.3 การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร (Human Resource Security)
- 1.4.4 การบริหารจัดการทรัพย์สินสารสนเทศ (Asset Management)
- 1.4.5 การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ (Access Control)
- 1.4.6 การควบคุมการเข้ารหัสข้อมูล (Cryptographic Control)
- 1.4.7 การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (Physical and Environmental Security)
- 1.4.8 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ (Operations Security)
- 1.4.9 การรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ (Communications Security)

- 1.4.10 การจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ (System Acquisition, Development and Maintenance)
- 1.4.11 การใช้บริการระบบสารสนเทศจากผู้ให้บริการภายนอก (IT Outsourcing)
- 1.4.12 การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Incident Management)
- 1.4.13 การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Aspects of Business Continuity Management)
- 1.4.14 การปฏิบัติตามข้อกำหนด (Compliance)

2. การรายงาน

กำหนดให้มีการรายงานการปฏิบัติตามนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมถึงระเบียบและข้อกำหนดใด ๆ ต่อคณะกรรมการบริษัท อย่างน้อยปีละ 1 ครั้ง หรือในกรณีที่มีเหตุการณ์ใด ๆ ซึ่งอาจส่งผลกระทบต่อการปฏิบัติตามนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมถึงระเบียบและข้อกำหนดอย่างมีนัยสำคัญ เช่น ระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่บริษัท หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมถึงระเบียบและข้อกำหนดที่บริษัทกำหนดไว้ ทั้งนี้ ผู้บริหารระดับสูงสุดของหน่วยงาน (ประธานเจ้าหน้าที่บริหาร : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

3. บทบังคับใช้

นโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศนี้ให้ใช้บังคับกับ พนักงาน ลูกจ้างชั่วคราว ลูกจ้างประจำของบริษัท รวมถึงบุคคลภายนอก และหน่วยงานภายนอกที่ให้บริการแก่บริษัท

นโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศฉบับนี้ ได้รับการอนุมัติจากที่ประชุมคณะกรรมการบริษัท ครั้งที่ 1/2566 เมื่อวันที่ 28 มีนาคม 2566 และให้มีผลใช้บังคับตั้งแต่วันที่ 29 มีนาคม 2566 เป็นต้นไป