SOMBOON ADVANCE TECHNOLOGY PUBLIC COMPANY LIMITED
SOMBOON FORGING TECHNOLOGY COMPANY LIMITED
SOMBOON MALLEABLE IRON INDUSTRIAL COMPANY LIMITED
INTERNATIONAL CASTING PRODUCTS COMPANY LIMITED
BANGKOK SPRING INDUSTRIAL COMPANY LIMITED
Head Office: 129 Moo 2 15th KM. Bangna-Trad Rd., Bangchalong, Bangplee, Samutprakarn 10540 Thailand Tel. (+66) 02 080 8123 www.satpcl.co.th

ประกาศที่ 019/2566
เรื่อง นโยบายด้านความมั่นคงปลอดภัยไซเบอร์และระบบเทคโนโลยีสารสนเทศ

หมวดที่ 1 บททั่วไป

1. วัตถุประสงค์

เพื่อให้การใช้งานระบบคอมพิวเตอร์เป็นไปอย่างเหมาะสมและมีประสิทธิภาพ รวมทั้งเพื่อป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานในลักษณะที่ไม่ถูกต้อง และเพื่อให้ผู้ใช้งานเข้าใจระเบียบปฏิบัติที่สอดคล้องกับนโยบายในเรื่องจริยธรรมธุรกิจและข้อพึงปฏิบัติในการทำงาน (Code of Conduct) รวมทั้งป้องกันการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ จึงขอประกาศนโยบายด้านความมั่นคงปลอดภัยไซเบอร์และระบบเทคโนโลยีสารสนเทศ ให้ผู้ใช้งานได้รับทราบและปฏิบัติตามโดยเคร่งครัด

2. ขอบเขตของนโยบายและความรับผิดชอบโดยรวมต่อความปลอดภัยของข้อมูลและระบบสารสนเทศ

นโยบายนี้ครอบคลุมถึงการใช้งานอุปกรณ์คอมพิวเตอร์ ข้อมูล และระบบเครือข่ายเทคโนโลยีสารสนเทศ ซึ่งถือเป็นทรัพย์สินของบริษัทฯ และไม่อนุญาตให้นำไปใช้เพื่อประโยชน์หรือธุรกิจส่วนตัว จึงเป็นความรับผิดชอบของผู้ใช้งานทุกท่านที่จะช่วยกันป้องกันความเสียหาย สูญเสีย และการใช้งานข้อมูลในทางที่ผิด หรือถูกเปิดเผยข้อมูลทางธุรกิจอย่างไม่เหมาะสมโดยไม่ได้รับอนุญาตจากบริษัทฯ รวมทั้งห้ามมีการทำซ้ำเปลี่ยนแปลง ลบทิ้ง หรือทำลายข้อมูลของบริษัทฯ โดยไม่ได้รับอนุญาต ทั้งนี้ผู้บริหารในระดับผู้จัดการขึ้นไปทุกคนจะต้องช่วยกันสอดส่องดูแลการใช้ข้อมูลของบริษัทฯ ในสายบังคับบัญชาอย่างเคร่งครัดโดยคำนึงถึงประโยชน์ของบริษัทฯ เป็นหลัก

3. คำนิยาม

3.1 บริษัทฯ หมายความว่า บริษัท สมบูรณ์ แอ็ดวานซ์ เทคโนโลยี จำกัด (มหาชน) และบริษัทย่อย

3.2 ฝ่ายเทคโนโลยีสารสนเทศ หมายความว่า หน่วยงานที่รับผิดชอบในการดำเนินงานด้านบริหารจัดการเทคโนโลยีสารสนเทศของบริษัท

3.3 ผู้ใช้งาน หมายความว่า ผู้ใช้งาน หรือบุคคลที่ได้รับอนุญาต (Authorized User) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศของบริษัทโดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (Role) ซึ่งบริษัทฯ กำหนดไว้

3.4 ระบบคอมพิวเตอร์ หมายความว่า อุปกรณ์ หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

3.5 ข้อมูลคอมพิวเตอร์ หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

3.6 ระบบเครือข่ายคอมพิวเตอร์ (Network System) หมายความว่า ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของบริษัทได้ เช่น ระบบ LAN ระบบ Intranet ระบบ Internet เป็นต้น

3.7 ระบบ LAN และระบบ Intranet หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานของบริษัทฯ เข้าด้วยกัน โดยมีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในบริษัทฯ

3.8 ระบบ Internet หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเตอร์เน็ตทั่วโลก

3.9 ระบบเทคโนโลยีสารสนเทศที่มีนัยสำคัญ หมายความว่า ระบบคอมพิวเตอร์และระบบเครือข่ายที่หากมีการหยุดชะงักจะส่งผลกระทบอย่างมีนัยสำคัญต่อการดำเนินงานหรือความต่อเนื่องในการดำเนินงาน ชื่อเสียง หรือฐานะของผู้ประกอบธุรกิจ หรือการใช้บริการของลูกค้า

3.10 รหัสผ่าน (Password) หมายความว่า ตัวอักษร หรืออักขระ หรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบ ยืนยันตัวบุคคลเพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

3.11 ความเสี่ยงด้านระบบข้อมูลสารสนเทศ หมายความว่า ความเสี่ยงที่เกิดขึ้นกับฐานข้อมูลต่างๆ ของระบบสารสนเทศภายในบริษัท เช่น ข้อมูลลูกค้า ข้อมูลผู้จัดจำหน่าย การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล เป็นต้น

3.12 บุคคลภายนอก (third party) บุคคลภายนอกที่มีความเกี่ยวข้องกับบริษัท ดังนี้

(1) ผู้ให้บริการงานด้านเทคโนโลยีสารสนเทศ เช่น บริษัทที่รับบริการดูแลศูนย์คอมพิวเตอร์ภายนอก, บริษัทที่ให้บริการดูแลและพัฒนาระบบเทคโนโลยีสารสนเทศ เป็นต้น

(2) ผู้ที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศ เช่น ผู้ให้บริการดูแลระบบ Firewall, ผู้ให้บริการเครื่องถ่ายเอกสาร, ผู้ให้บริการ Internet ที่มีความจำเป็นต้องกำหนดค่าในการเชื่อมต่อระบบภายในบริษัท เป็นต้น

(3) ผู้ที่สามารถเข้าถึงข้อมูลสำคัญของบริษัท หรือข้อมูลของลูกค้าของบริษัท เช่น ผู้ตรวจสอบบัญชีอิสระ เป็นต้น

3.13 ภัยคุกคามทางไซเบอร์ การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยการใช้คอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือโปรแกรมคอมพิวเตอร์ ซึ่งมุ่งหมายให้เกิดความเสียหายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง รวมถึงภยันตรายที่อาจจะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

3.14 เหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ (IT incident) หมายความว่า เหตุการณ์ด้านเทคโนโลยีสารสนเทศ ที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) เช่น

(1) ระบบเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจถูกบุกรุกหรือโจมตี

(2) ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศถูกคุกคาม

(3) ระบบเทคโนโลยีสารสนเทศหยุดชะงัก ไม่สามารถให้บริการได้

หมวดที่ 2 นโยบายการบริหารจัดการทรัพย์สิน (Asset) ของบริษัทฯ

4. ทรัพย์สินของบริษัทฯ

บริษัทฯ ได้จัดให้มีคอมพิวเตอร์ตั้งโต๊ะ และ Notebook เพื่อให้ผู้ใช้งานใช้ในทางการที่จ้างของบริษัทฯ ข้อมูลทั้งหมด โปรแกรมต่าง ๆ รวมถึง Software ที่ถูกบันทึกอยู่ในคอมพิวเตอร์ตั้งโต๊ะ และ Notebook ที่บริษัทฯ จัดให้ถือเป็นทรัพย์สินของบริษัทฯ ดังนั้น บริษัทฯ จึงไม่อนุญาตให้ผู้ใช้งานลงโปรแกรมใด ๆ เว้นแต่ได้รับการยินยอมจากฝ่ายเทคโนโลยีสารสนเทศ หากเครื่องคอมพิวเตอร์เกิดความเสียหาย ผู้ใช้งานเจ้าของเครื่องคอมพิวเตอร์ต้องรีบแจ้งฝ่ายเทคโนโลยีสารสนเทศโดยทันที และห้ามมิให้ทำการซ่อมแซม ปรับแต่ง หรือเปลี่ยนแปลงอุปกรณ์ใด ๆ ของเครื่องคอมพิวเตอร์โดยมิได้รับอนุญาต และเพื่อป้องกันการถูกลักลอบใช้งานโดยผู้อื่น ผู้ใช้งานจะต้องทำการล็อครหัสผ่านเครื่องคอมพิวเตอร์ทุกครั้งที่ไม่ได้ใช้งาน

การเปลี่ยนแปลงผู้ถือครองทรัพย์สินที่เป็นคอมพิวเตอร์ Notebook รวมถึง Software ต่างๆ หน่วยงานของผู้ใช้งานที่เป็นเจ้าของทรัพย์สินจะต้องแจ้งเปลี่ยนแปลงต่อเจ้าหน้าที่ดูแลระบบเทคโนโลยีสารสนเทศภายในเดือนที่มีการเปลี่ยนแปลงข้อมูล เพื่อตรวจสอบและปรับปรุงทะเบียนทรัพย์สินให้ถูกต้องอย่างสม่ำเสมอ

การยกเลิกหรือหยุดใช้งานทรัพย์สินเนื่องจากสาเหตุใดๆ หน่วยงานของผู้ใช้งานที่เป็นเจ้าของทรัพย์สินควรนำทรัพย์สินส่งมอบคืนให้กับเจ้าหน้าที่ดูแลระบบเทคโนโลยีสารสนเทศภายในวันที่มีการยกเลิกการใช้งาน และเจ้าหน้าที่ดูแลระบบเทคโนโลยีสารสนเทศต้องทำการลบ ทำลายข้อมูลสำคัญ หรือปรับค่าข้อมูลของเครื่องคอมพิวเตอร์ให้กลับสู่ค่าตั้งต้น

5. การบริหารจัดการข้อมูลสารสนเทศ (Data/Information)

ผู้ใช้งานต้องตระหนักว่าข้อมูลคอมพิวเตอร์ ถือว่าเป็นทรัพย์สินของบริษัทฯ และต้องถูกนำไปใช้งานในทางการที่จ้างของบริษัทฯ เท่านั้น อีกทั้งผู้ใช้งานต้องไม่นำข้อมูลคอมพิวเตอร์ไปใช้เพื่อประโยชน์ส่วนตน การใช้งาน แก้ไข หรือเผยแพร่ข้อมูลคอมพิวเตอร์ต้องเป็นไปเพื่องานของบริษัทฯ ซึ่งตนเองรับผิดชอบ นอกจากนี้ข้อมูลคอมพิวเตอร์บางอย่างโดยเฉพาะอย่างยิ่งข้อมูลส่วนบุคคล ทรัพย์สินทางปัญญา และข้อมูลที่จำกัดสิทธิ เช่น Product Designs, Source Code, Pending Patent, Customer Lists, Pricing Cost and Sales Information, Third Party Contracts เป็นต้น เป็นข้อมูลที่มีความละเอียดอ่อน อาจมีกฎหมายที่เกี่ยวข้องและกำกับโดยเฉพาะ หรือมีมูลค่าของข้อมูลสูง อ้างอิงประกาศระเบียบปฏิบัติ เกี่ยวกับการแบ่งประเภทข้อมูลและการปกป้องข้อมูล ตามประกาศที่ 020/2566 ผู้ใช้งานต้องปฏิบัติตามประกาศและระเบียบดังกล่าวอย่างเคร่งครัด

6. การติดตั้งซอฟต์แวร์ (Software)

ห้ามผู้ใช้งานติดตั้งซอฟต์แวร์ทุกประเภทในเครื่องคอมพิวเตอร์ของบริษัทฯ รวมถึงห้ามคัดลอกซอฟต์แวร์ลิขสิทธิ์ และนำซอฟต์แวร์ไปติดตั้งที่อื่น ไม่ว่าจากการดาวน์โหลด หรือจากแผ่นโปรแกรม ในกรณีที่ลักษณะงานมีความจำเป็นต้องใช้ซอฟต์แวร์อื่นเป็นพิเศษ ผู้ใช้งานต้องติดต่อให้ฝ่ายเทคโนโลยีสารสนเทศเป็นผู้ดำเนินการ หากผู้ใช้งานทำการติดตั้งซอฟต์แวร์โดยมิได้รับอนุญาตให้ถือเป็นความผิดทางวินัย

7. การเข้าถึงระบบเทคโนโลยีสารสนเทศ (Accessing Information System)

การเข้าถึงระบบเทคโนโลยีสารสนเทศของบริษัทฯ : บริษัทฯ อนุญาตให้ผู้ใช้งานเข้าถึงระบบต่างๆ ในบริษัทฯ ผ่านอุปกรณ์ของบริษัทที่ได้รับอนุมัติจากผู้บริหารระดับสูงของหน่วยงานเท่านั้น ซึ่งสิทธิที่ผู้ใช้งานได้รับอนุญาต จำเป็นจะต้องมีการทบทวนสิทธิให้เหมาะสมในการใช้งานระบบต่างๆ ของบริษัทอย่างสม่ำเสมอ

การใช้ระบบ e-mail : ระบบ e-mail และระบบสื่อสารทางอิเล็กทรอนิกส์ถือเป็นทรัพย์สินของบริษัทฯ ซึ่งสงวนสิทธิให้ผู้ใช้งานใช้เพื่อประโยชน์ทางธุรกิจของบริษัทฯ เท่านั้น ห้ามผู้ใช้งานส่งข้อมูลที่ผิดกฎหมาย ข้อความกล่าวร้าย ทำให้เสื่อมเสียหยาบคาย ส่อเสียดอนาจาร หรือเป็นการให้ร้ายบุคคลอื่น โดยใช้ระบบ e-mail หรือระบบสื่อสารทางอิเล็กทรอนิกส์ใด ๆ ทั้งนี้ บริษัทฯ สงวนสิทธิในการตรวจสอบ e-mail ของผู้ใช้งานได้ทุกเมื่อ โดยไม่จำเป็นต้องแจ้งให้ผู้ใช้งานทราบล่วงหน้า

การใช้งานระบบ Internet : บริษัทฯ อนุญาตให้ผู้ใช้งานใช้อินเทอร์เนต (Internet) ในการแสวงหาข้อมูล ความรู้ที่เป็นประโยชน์ต่อการปฏิบัติงาน หรือใช้เป็นแหล่งอ้างอิงข้อมูลในการทำงาน รวมถึงข่าวสารทั่วไป ทั้งนี้ บริษัทได้ติดตั้งระบบจำแนกหมวดหมู่ Website และกำหนดหมวดหมู่ที่อนุญาตและไม่อนุญาตให้ใช้งาน และบริษัทสงวนสิทธิในการตรวจสอบการใช้งานอินเทอร์เนต โดยไม่จำเป็นต้องแจ้งให้ผู้ใช้งานทราบล่วงหน้า

การใช้งานระบบ File Sharing อนุญาตให้ใช้ข้อมูลที่จัดเก็บอยู่ใน File Sharing ได้เฉพาะผู้ที่ได้รับอนุญาตจากผู้บริหารระดับสูงของหน่วยงานนั้นๆ ที่เป็นเจ้าของข้อมูลเท่านั้น ข้อมูลใน File Sharing ซึ่งถือเป็นข้อมูลความลับสูงสุดของหน่วยงานนั้นๆ จำเป็นจะต้องกำหนดชั้นความลับเพื่อควบคุมการใช้ข้อมูลให้เหมาะสมและป้องกันการรั่วไหลของข้อมูล รวมถึงผู้บริหารระดับสูงของหน่วยงานต้องมีการทบทวนสิทธิการใช้ข้อมูล File Sharing ของหน่วยงานอย่างสม่ำเสมอ

การเข้าถึงข้อมูลบนระบบคลาวด์ (Share point หรือ One drive) อนุญาตให้เข้าถึงข้อมูลได้เฉพาะการเข้าผ่านอุปกรณ์ของบริษัทฯ ที่ได้รับอนุญาตแล้วเท่านั้น

การใช้งานระบบ IT ที่มีนัยสำคัญ เช่น ระบบ SAP หรือที่คณะกรรมการด้านความมั่นคงปลอดภัยไซเบอร์ฯ เห็นชอบ บริษัทฯ อนุญาตให้ผู้ใช้งานที่ได้รับอนุมัติจากผู้บริหารระดับสูงของหน่วยงานดังกล่าวในการขออนุมัติเพื่อการเข้าใช้งานระบบ และฝ่ายเทคโนโลยีสารสนเทศมีหน้าที่ควบคุมการเข้าใช้งานระบบให้เหมาะสม และสามารถเปลี่ยนแปลงแก้ไขสิทธิในการเข้าใช้งานที่ไม่เหมาะสมได้ โดยมีการทบทวนปรับปรุงสิทธิให้เหมาะสมอย่างสม่ำเสมอ สอดคล้องกับหน้าที่ความรับผิดชอบของผู้ใช้งาน และทำการลบสิทธิการใช้งานระบบออกเมื่อสิ้นสุดความจำเป็นในการใช้งาน รวมถึงมีกระบวนการยืนยันตัวตนของผู้ใช้งาน (Authentication) ที่เหมาะสมเป็นประจำทุกปี

8. ความเสี่ยงด้านระบบข้อมูลสารสนเทศ

ปัจจุบันฝ่ายเทคโนโลยีสารสนเทศ มีการติดตามและประเมินความเสี่ยงในกิจกรรมที่สำคัญผ่านคณะกรรมการด้านความเสี่ยงระดับองค์กรอย่างต่อเนื่อง ซึ่งการส่งข้อมูล สำเนาเอกสาร หรือรูปต่างๆ ภายในบริษัทฯ ผู้ใช้งานต้องระมัดระวังไม่ให้มีรูปภายในอาคารโรงงาน เครื่องจักร สินค้า หรือรูปอื่นใดทางสื่อออนไลน์ที่อาจทำให้เกิดมีการเผยแพร่ออกไปในวงกว้างและบริษัทฯ อาจได้รับความเสียหาย หรือการใช้ระบบคอมพิวเตอร์จากภายนอกบริษัทฯ ต้องใช้ความระมัดระวังมิให้ข้อมูลของบริษัทฯ ถูกเผยแพร่จนบริษัทฯ อาจได้รับความเสียหาย ผู้ใช้งานมีหน้าที่รับผิดชอบ หากนำเครื่องคอมพิวเตอร์และอุปกรณ์จัดเก็บข้อมูลไปใช้ภายนอกบริษัท และเกิดการสูญหาย หรือความเสียหาย อันเนื่องมาจากการบกพร่องละเลย ประมาทเลินเล่อหรือฝ่าฝืนการปฏิบัติตามนโยบายระบบเทคโนโลยีสารสนเทศ จนเป็นเหตุให้ข้อมูลของบริษัทถูกเผยแพร่ออกไปจนบริษัทฯ อาจได้รับความเสียหาย ซึ่งถือเป็นความเสี่ยงระดับองค์กรอย่างหนึ่ง ทั้งนี้ บริษัทฯ ถือว่าการฝ่าฝืนข้อพึงระมัดระวังดังกล่าวข้างต้นมีโทษทางวินัย

หมวดที่ 3 การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

9. การบริหารจัดการที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบคอมพิวเตอร์

9.1 ห้ามมิให้ผู้ใช้งานเข้าถึง (Access) โดยมิชอบ[1] ซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ เช่น กรณีที่มีการกำหนดรหัสผ่านเพื่อป้องกันมิให้บุคคลอื่นใช้เครื่องคอมพิวเตอร์ และผู้กระทำผิดดำเนินการด้วยวิธีใดวิธีหนึ่งเพื่อให้ได้รหัสผ่านนั้นมาและสามารถใช้เครื่องคอมพิวเตอร์นั้นได้โดยนั่งอยู่หน้าเครื่องคอมพิวเตอร์ และให้หมายความรวมถึงการเข้าถึงระบบคอมพิวเตอร์หรือเข้าถึงข้อมูลคอมพิวเตอร์ แม้ตัวบุคคลที่เข้าถึงจะอยู่ห่างโดยระยะทางกับเครื่องคอมพิวเตอร์ แต่สามารถเจาะเข้าไปในระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่ตนต้องการได้

9.2 ห้ามมิให้ผู้ใช้งานเปิดเผย[2] มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่มีไว้สำหรับตนแก่ผู้หนึ่งผู้ใดหรือหลายคน หากว่าระบบคอมพิวเตอร์นั้นมีมาตรการการเข้าถึง เช่น มีการลงทะเบียน Username และรหัสผ่าน หรือมีวิธีการอื่นใดที่จัดขึ้นเป็นการเฉพาะ

9.3 ห้ามมิให้ผู้ใช้งานเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบซึ่งข้อมูลนั้นได้มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน

9.4 ห้ามมิให้ผู้ใช้งานกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้

9.5 ห้ามมิให้ผู้ใช้งานทำการรบกวนข้อมูลและอุปกรณ์คอมพิวเตอร์ของผู้อื่นโดยการทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ

9.6 ห้ามมิให้ผู้ใช้งานกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนระบบคอมพิวเตอร์นั้นไม่สามารถทำงานได้

9.7 ห้ามมิให้ผู้ใช้งานส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว เช่น การปกปิดหรือปลอมแปลง IP Address และให้หมายความรวมถึงการกระทำที่ทำให้ไม่สามารถตรวจสอบถึงแหล่งที่มาของการส่งข้อมูลและส่งผลให้ไม่อาจตรวจสอบได้ทางระบบข้อมูลจราจรทางคอมพิวเตอร์ อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่น

9.8 ห้ามมิให้ผู้ใช้งานส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นอันมีลักษณะเป็นการก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับข้อมูลคอมพิวเตอร์ หรือจดหมายอิเล็กทรอนิกส์ โดยไม่เปิดโอกาสให้ผู้รับสามารถบอกเลิกหรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับได้โดยง่าย

9.9 ฝ่ายเทคโนโลยีสารสนเทศ มีสิทธิในการตรวจสอบ และติดตามทรัพย์สินที่ผู้ใช้งานถือครองอยู่เป็นประจำ หากทรัพย์สินเริ่มมีสัญญาณส่งผลกระทบที่ทำให้การใช้งานไม่ต่อเนื่อง หรือไม่พร้อมใช้งาน หน่วยงานเจ้าของทรัพย์สินต้องรีบรายงานการใช้ทรัพย์สินดังกล่าว ต่อเจ้าหน้าที่ดูแลระบบเทคโนโลยีสารสนเทศที่รับผิดชอบเพื่อดำเนินการแก้ไขโดยทันที เพื่อป้องกันมิให้ธุรกิจต้องหยุดชะงักในการดำเนินงาน

---

[1] "การเข้าถึง" ในที่นี้ หมายถึง การเข้าถึงโดยปราศจากสิทธิโดยชอบธรรม (Without Right)

[2] "โดยเปิดเผย" ในที่นี้ หมายถึง แค่นำมาตราการนั้นเปิดเผยต่อผู้ใดผู้หนึ่งหรือหลายคน เมื่อเปิดเผยแล้วผู้ใดจะทราบหรือนำไปใช้หรือไม่ ไม่สำคัญ

9.10 การเข้าศูนย์คอมพิวเตอร์ภายใน (Server Room) บริษัทฯ ต้องมีการยืนยันตัวตนของผู้เข้า-ออก บันทึกข้อมูลการเข้า-ออก และผู้ขอเข้าศูนย์คอมพิวเตอร์ต้องได้รับอนุมัติจากผู้บริหารระดับสูงของฝ่ายเทคโนโลยีสารสนเทศ อ้างอิง คู่มือวิธีการปฏิบัติ : การเข้าใช้งานห้อง Server

หมวดที่ 4 การเข้าถึงระบบเทคโนโลยีสารสนเทศของบุคคลภายนอก (third party)

10. การใช้บริการจากบุคคลภายนอก

การใช้บริการงานด้านระบบเทคโนโลยีสารสนเทศจากบุคคลภายนอก จะต้องผ่านหลักเกณฑ์การคัดเลือก สรรหา อ้างอิงตามคู่มือการจัดซื้อ / จัดจ้าง มีการระบุหน้าที่และขอบเขตความรับผิดชอบของบุคคลภายนอกตามข้อตกลงหรือสัญญาการให้บริการอย่างชัดเจนและเป็นลายลักษณ์ โดยบริษัทฯ มีมาตรการในการตรวจสอบและติดตามการดำเนินงานที่มีนัยสำคัญ ที่มีผลกระทบต่อการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลได้

รวมถึงบุคคลภายนอกควรใช้ความระมัดระวังมิให้ข้อมูลของบริษัทฯ ถูกเผยแพร่ต่อภายนอกโดยไม่ได้รับอนุญาต หรือต้องรักษาความลับของบริษัทฯ หากข้อมูลดังกล่าวถูกเผยแพร่ต่อสาธารณะ และส่งผลกระทบที่ก่อให้เกิดความเสียหายต่อบริษัทฯ บุคคลภายนอกต้องรับผิดชอบต่อผลดังกล่าว

หมวดที่ 5 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT (IT operation security)

11. การปฏิบัติงานของเจ้าหน้าที่ดูแลระบบเทคโนโลยีสารสนเทศ

อ้างอิงตามคู่มือวิธีการปฏิบัติ : IT OPERATION PROCESS สำหรับแนวทางปฏิบัติงานของเจ้าหน้าที่ดูแลระบบเทคโนโลยีสารสนเทศ เพื่อดูแลระบบ Network ภายในบริษัท การแก้ไขปัญหาต่างๆ ของระบบคอมพิวเตอร์ รวมถึงดูแลและบำรุงรักษา Hardware และ Software ของอุปกรณ์ต่าง ภายในบริษัท ให้มีประสิทธิภาพดีและพร้อมใช้งานอยู่ตลอดเวลา และเพิ่มความเชื่อมั่นระบบความปลอดภัยของข้อมูลให้แก่ผู้ใช้งาน

ซึ่งคู่มือวิธีการปฏิบัติที่มีการบังคับใช้ในปัจจุบัน ที่เกี่ยวข้องได้แก่

คู่มือวิธีการปฏิบัติ : การสำรองข้อมูลระบบ File Server

คู่มือวิธีการปฏิบัติ : การกู้คืนข้อมูลระบบ File Server

คู่มือวิธีการปฏิบัติ : การสร้างบัญชีผู้ใช้ระบบ File Server

คู่มือวิธีการปฏิบัติ : การสร้างบัญชีผู้ใช้ระบบ Email

คู่มือวิธีการปฏิบัติ : การขึ้นทะเบียนเครื่องลูกข่าย

คู่มือวิธีการปฏิบัติ : การบันทึกคำร้องผ่าน Helpdesk

คู่มือวิธีการปฏิบัติ : การสร้างบัญชีผู้ใช้ระบบ File Server

คู่มือวิธีการปฏิบัติ : การสร้างบัญชีผู้ใช้งานระบบคอมพิวเตอร์

คู่มือวิธีการปฏิบัติ : การร้องขอใช้งานระบบจากภายนอกผ่าน VPN

คู่มือวิธีการปฏิบัติ : การสร้างบัญชีผู้ใช้ระบบ File Server

หมวดที่ 6 การรักษาความมั่นคงปลอดภัยเกี่ยวกับระบบเครือข่ายสื่อสาร (communication system security)

12. ระบบเครือข่ายสื่อสาร

ระบบเทคโนโลยีสารสนเทศต่างๆ ที่ใช้งานในบริษัท มีการควบคุมการเชื่อมต่อของระบบงานต่าง ๆ (Application system) ที่สำคัญของบริษัทได้อย่างเหมาะสม โดยแบ่งแยกเครือข่ายของระบบเทคโนโลยีที่มีนัยสำคัญ ออกจากเครือข่ายของระบบการปฏิบัติงานทั่วไป หรือเครือข่ายสำหรับบุคคลภายนอก (guest network)

มีการติดตั้งอุปกรณ์ป้องกันความเสี่ยงและรักษาความปลอดภัยให้กับเครือข่ายที่มีความสำคัญ เพื่อป้องกันและตรวจจับการบุกรุกทางด้านไซเบอร์ และควบคุมการใช้งานเฉพาะอุปกรณ์ที่ได้รับอนุมัติให้เชื่อมต่อกับระบบภายในได้เท่านั้น

หมวดที่ 7 การบริหารจัดการโครงการด้านระบบเทคโนโลยีสารสนเทศ (IT project management)

13. การจัดหา พัฒนา และแก้ไขเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศ

กำหนดกรอบการบริหารจัดการโครงการ (Project management framework) เริ่มตั้งแต่

(1) การจัดหาระบบเทคโนโลยีสารสนเทศ ที่สามารถตอบสนองความต้องการทางธุรกิจและความมั่นคงปลอดภัยไซเบอร์

(2) การพัฒนาระบบเทคโนโลยีสารสนเทศ โดยมีการควบคุมเกี่ยวกับการออกแบบ พัฒนา ทดสอบระบบ และนำระบบขึ้นใช้งานจริง มีความถูกต้องพร้อมใช้งาน และสอดคล้องกับแผนการดำเนินธุรกิจ กรณีมอบหมายให้บุคคลภายนอกเป็นผู้พัฒนาหรือแก้ไข ต้องมีการติดตามและควบคุมการดำเนินการให้เป็นไปตามข้อตกลงหรือสัญญา

(3) การแก้ไขเปลี่ยนแปลงระบบ ต้องได้รับอนุมัติจากผู้ช่วยผู้จัดการทั่วไปของหน่วยงานในการอนุมัติเพื่อแก้ไขเปลี่ยนแปลงระบบ มีการทดสอบและการอนุมัติเพื่อนำระบบขึ้นใช้งานจริง

หมวดที่ 8 เหตุการณ์ผิดปกติและแผนฉุกเฉินด้านระบบเทคโนโลยีสารสนเทศ

(IT incident & contingency plan)

ในกรณีที่พบเหตุการณ์ผิดปกติเกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์และระบบเทคโนโลยีสารสนเทศ ที่ส่งผลกระทบก่อให้เกิดความเสียหายต่อทรัพย์สินของผู้ใช้งานหรือผู้ที่เกี่ยวข้อง ผู้ที่พบเหตุการณ์ต้องรีบแจ้งเหตุการณ์ดังกล่าวต่อฝ่ายเทคโนโลยีสารสนเทศ เพื่อจัดการเหตุการณ์ผิดปกติ ค้นหาสาเหตุที่แท้จริง มีการบันทึกข้อมูลและรายงานเหตุการณ์ผิดปกติต่อคณะทำงานด้านความมั่นคงปลอดภัยไซเบอร์และระบบเทคโนโลยีสารสนเทศ โดยต้องสามารถกู้คืนระบบให้กลับสู่สภาพปกติภายในระยะเวลาที่กำหนด

กำหนดให้มีการประเมินความเสี่ยงของเหตุการณ์ที่ส่งผลกระทบต่อองค์กรและขอความเห็นชอบจากคณะกรรมการฯ ในการจัดทำแผนฉุกเฉินด้านระบบเทคโนโลยีสารสนเทศ เพื่อรองรับเหตุการณ์ผิดปกติ มีการสื่อสารให้ผู้ใช้งานเข้าใจและปฏิบัติตามแผนฉุกเฉินได้ ซึ่งแผนฉุกเฉินต้องทบทวนและทดสอบอย่างน้อยปีละ 1 ครั้ง

หมวดที่ 9 การบังคับใช้และการทบทวนนโยบาย

14. การปฏิบัติตามนโยบาย กฎหมาย และข้อกำหนดที่เกี่ยวข้อง

ผู้ใช้งานต้องรับทราบ ทำความเข้าใจ และปฏิบัติตามนโยบายความปลอดภัยของระบบเทคโนโลยีสารสนเทศและป้องกันภัยทางไซเบอร์ ฉบับนี้ รวมถึง กฎ ระเบียบ ข้อบังคับ และกฎหมาย ที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารอย่างเคร่งครัด ซึ่งรวมถึงแต่ไม่จำกัดเฉพาะ

- พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560
- พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 4) พ.ศ. 2562

ฝ่ายเทคโนโลยีสารสนเทศ และฝ่ายที่เกี่ยวข้องต้องร่วมกับฝ่ายกำกับและตรวจสอบในการติดตาม และรวบรวมกฎหมาย กฎ ระเบียบ หลักเกณฑ์ และข้อกำหนดต่างๆ ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยจัดทำเป็นเอกสารเพื่อใช้เป็นข้อกำหนดในการปฏิบัติงาน และปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

15. บทกำหนดโทษ

ผู้ใช้งานที่ฝ่าฝืนนโยบายนโยบายความปลอดภัยของระบบเทคโนโลยีสารสนเทศและป้องกันภัยทางไซเบอร์ ฉบับนี้ บริษัทฯ จะพิจารณาลงโทษทางวินัยตามข้อบังคับการทำงานของบริษัทฯ ที่กำหนดไว้ รวมทั้ง ผู้ใช้งานดังกล่าวอาจต้องรับผิดทั้งทางอาญาและทางแพ่ง ตามที่กฎหมายกำหนด

16. การทบทวนนโยบาย

ฝ่ายเทคโนโลยีสารสนเทศและฝ่ายที่เกี่ยวข้องต้องดำเนินการทบทวนนโยบายความปลอดภัยของระบบเทคโนโลยีสารสนเทศและป้องกันภัยทางไซเบอร์เป็นประจำ อย่างน้อยปีละ 1 ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงแก้ไขกฎหมาย เพื่อปรับปรุงแก้ไขนโยบายของบริษัทฯ ให้เหมาะสม และถูกต้องตามกฎหมายต่อไป

ทั้งนี้มีผลตั้งแต่วันที่ 15 มีนาคม 2566 เป็นต้นไป

จึงประกาศมาให้ทราบโดยทั่วกัน

(นภัสร กิตะพาณิชย์)
กรรมการผู้อำนวยการ

CC : All Executives , Managers.